

Oracle® Secure Backup Reference



Release 12.2

E85992-02

January 2018

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Secure Backup Reference, Release 12.2

E85992-02

Copyright © 2006, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Kathy Rich

Contributing Authors: Padmaja Potineni, Lance Ashdown, Aishwarya Minocha, Antonio Romero

Contributors: Anand Agrawal, George Claborn, Michael Chamberlain, Sumit Chougule, Donna Cooksey, Senad Dizdar, Tony Dziedzic, Judy Ferstenberg, Steven Fried, Geoff Hickey, Ashok Joshi, Cris Pedregal-Martin, Chris Plakyda, George Stabler, Radhika Vullikanti, Joe Wadleigh, Steve Wertheimer

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, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	xxix
Documentation Accessibility	xxix
Related Documents	xxix
Conventions	xxx

Changes in This Release for Oracle Secure Backup Reference

Changes in Oracle Secure Backup 12c Release 2 (12.2.0.1)	xxxii
Deprecated Features	xxxii

1 About obtool

1.1 obtool Invocation	1-1
1.1.1 obtool Login	1-1
1.1.1.1 Login and Preauthorization	1-2
1.1.2 obtool Interactive Mode	1-3
1.1.2.1 obtool Syntax for Interactive Mode	1-3
1.1.2.2 Command Execution in Interactive Mode	1-3
1.1.2.3 Input Redirection in Interactive Mode	1-4
1.1.2.4 Exiting obtool	1-4
1.1.3 obtool Noninteractive Mode	1-4
1.1.3.1 Escaping Special Characters in obtool Command Line	1-5
1.1.3.2 Running Multiple obtool Commands Non-Interactively	1-5
1.1.3.3 Redirecting obtool Commands From an Input File	1-5
1.1.4 Exiting obtool	1-6
1.1.5 Logging Out of obtool	1-6
1.1.6 Starting obtool as a Specific User: obtool -u	1-6
1.1.7 obtool Domain Authentication	1-6
1.1.8 obtool Version Number	1-7
1.1.9 obtool Date and Time Information	1-7
1.2 obtool Online Help	1-7
1.2.1 obtool Topics	1-8

1.2.2	obtool Command Syntax	1-9
1.2.3	obtool Glossary	1-9
1.3	obtool Command Categories	1-9
1.3.1	Backup Commands	1-10
1.3.2	Backup Image Commands	1-11
1.3.3	Backup Image Instance Management	1-11
1.3.4	Backup Piece Commands	1-11
1.3.5	Backup Window Commands	1-11
1.3.6	Browser Commands	1-12
1.3.7	Checkpoint Commands	1-12
1.3.8	Class Commands	1-13
1.3.9	Daemon Commands	1-13
1.3.10	Database Backup Storage Selector Commands	1-14
1.3.11	Dataset Commands	1-14
1.3.12	Device Commands	1-15
1.3.13	Duplication on Demand Commands	1-15
1.3.14	Duplication Window Commands	1-15
1.3.15	File-System Command	1-16
1.3.16	Host Commands	1-16
1.3.17	Job Commands	1-16
1.3.18	Library Commands	1-16
1.3.19	Location Commands	1-17
1.3.20	Media Family Commands	1-17
1.3.21	Miscellaneous Commands	1-18
1.3.22	Policy Commands	1-18
1.3.23	Preferred Network Interface Commands	1-19
1.3.24	Reports Commands	1-19
1.3.25	Restore Commands	1-19
1.3.26	Rotation Policy Commands	1-20
1.3.27	Schedule Commands	1-20
1.3.28	Section Commands	1-20
1.3.29	Snapshot Commands	1-21
1.3.30	Staging Commands	1-21
1.3.31	Summary Commands	1-21
1.3.32	User Commands	1-22
1.3.33	Volume Rotation Commands	1-22
1.3.34	Volume Duplication Commands	1-22
1.4	obtool Lexical Conventions	1-23
1.4.1	Conventions in Syntax Diagrams	1-23
1.4.2	Conventions in Code Examples	1-24

2 obtool Commands: addbw to lsvol

2.1.1	addbw	2-1
2.1.2	adddw	2-2
2.1.3	addp	2-3
2.1.4	backup	2-4
2.1.5	borrowdev	2-12
2.1.6	canceljob	2-14
2.1.7	catalog	2-15
2.1.8	catds	2-19
2.1.9	catrpt	2-20
2.1.10	catxcr	2-22
2.1.11	cd	2-25
2.1.12	cdds	2-26
2.1.13	cdp	2-27
2.1.14	chclass	2-28
2.1.15	chdev	2-30
2.1.16	chdup	2-41
2.1.17	chhost	2-43
2.1.18	chinstance	2-47
2.1.19	chkbw	2-48
2.1.20	chkds	2-49
2.1.21	chkdw	2-50
2.1.22	chloc	2-50
2.1.23	chmf	2-52
2.1.24	chpni	2-54
2.1.25	chrot	2-56
2.1.26	chsched	2-58
2.1.27	chssel	2-65
2.1.28	chstage	2-69
2.1.29	chsum	2-70
2.1.30	chuser	2-72
2.1.31	chvol	2-75
2.1.32	clean	2-79
2.1.33	closedoor	2-80
2.1.34	cpinstance	2-80
2.1.35	ctldaemon	2-83
2.1.36	discoverdev	2-85
2.1.37	dumpdev	2-88

2.1.38	dupvol	2-90
2.1.39	edds	2-92
2.1.40	exit	2-93
2.1.41	exportvol	2-94
2.1.42	extractvol	2-96
2.1.43	find	2-97
2.1.44	id	2-100
2.1.45	identifyvol	2-100
2.1.46	importvol	2-102
2.1.47	insertvol	2-105
2.1.48	inventory	2-108
2.1.49	labelvol	2-110
2.1.50	loadvol	2-112
2.1.51	logout	2-113
2.1.52	ls	2-114
2.1.53	lsbackup	2-117
2.1.54	lsbkup	2-119
2.1.55	lsbu	2-122
2.1.56	lsbw	2-125
2.1.57	lscheckpoint	2-126
2.1.58	lsclass	2-128
2.1.59	lsdaemon	2-131
2.1.60	lsdev	2-133
2.1.61	lsds	2-139
2.1.62	lsdup	2-140
2.1.63	lsdw	2-141
2.1.64	lsfs	2-141
2.1.65	lshost	2-143
2.1.66	lsinstance	2-146
2.1.67	lsjob	2-149
2.1.68	lsloc	2-155
2.1.69	lsmf	2-156
2.1.70	lsp	2-157
2.1.71	lspiece	2-160
2.1.72	lspni	2-162
2.1.73	lsrestore	2-164
2.1.74	lsrot	2-166
2.1.75	lsrpt	2-166
2.1.76	lssched	2-167
2.1.77	lssection	2-170
2.1.78	lssnap	2-173

2.1.79	lsssel	2-175
2.1.80	lsstage	2-177
2.1.81	lssum	2-178
2.1.82	lsuser	2-180
2.1.83	lsvol	2-182

3 obtool Commands: managedev to vfylibs

3.1.1	managedev	3-1
3.1.2	mkclass	3-2
3.1.3	mkdev	3-6
3.1.4	mkds	3-21
3.1.5	mkdup	3-24
3.1.6	mkhost	3-26
3.1.7	mkloc	3-34
3.1.8	mkmf	3-36
3.1.9	mkpni	3-40
3.1.10	mkrot	3-42
3.1.11	mksched	3-44
3.1.12	mksnap	3-53
3.1.13	mkssel	3-54
3.1.14	mkstage	3-57
3.1.15	mksum	3-61
3.1.16	mkuser	3-64
3.1.17	mountdev	3-69
3.1.18	movevol	3-71
3.1.19	opendoor	3-72
3.1.20	pingdev	3-73
3.1.21	pinghost	3-75
3.1.22	pwd	3-76
3.1.23	pwdds	3-77
3.1.24	pwdp	3-77
3.1.25	quit	3-79
3.1.26	recallvol	3-79
3.1.27	releasevol	3-80
3.1.28	renbkup	3-81
3.1.29	renclass	3-83
3.1.30	rendev	3-84
3.1.31	rends	3-85
3.1.32	rendup	3-86
3.1.33	renhost	3-87

3.1.34	renloc	3-88
3.1.35	renmf	3-88
3.1.36	renrot	3-89
3.1.37	rensched	3-90
3.1.38	rensnap	3-91
3.1.39	renssel	3-93
3.1.40	renstage	3-94
3.1.41	rensum	3-94
3.1.42	renuser	3-95
3.1.43	resdev	3-96
3.1.44	resetp	3-97
3.1.45	restore	3-99
3.1.46	returndev	3-105
3.1.47	reusevol	3-106
3.1.48	revhost	3-108
3.1.49	rmbbackup	3-108
3.1.50	rmbw	3-110
3.1.51	rmcheckpoint	3-110
3.1.52	rmclass	3-111
3.1.53	rmdev	3-112
3.1.54	rmids	3-114
3.1.55	rmdup	3-115
3.1.56	rmidw	3-116
3.1.57	rmhost	3-117
3.1.58	rminstance	3-118
3.1.59	rmjob	3-119
3.1.60	rmloc	3-120
3.1.61	rmmf	3-121
3.1.62	rmpr	3-122
3.1.63	rmprc	3-123
3.1.64	rmprni	3-124
3.1.65	rmrestore	3-127
3.1.66	rmrot	3-127
3.1.67	rmsched	3-128
3.1.68	rmsection	3-129
3.1.69	rmsnap	3-130
3.1.70	rmssel	3-132
3.1.71	rmstage	3-133
3.1.72	rmsum	3-133
3.1.73	rmuser	3-134
3.1.74	rmvol	3-135

3.1.75	rpyjob	3-137
3.1.76	runjob	3-138
3.1.77	set	3-140
3.1.78	setbw	3-140
3.1.79	setdw	3-141
3.1.80	setp	3-142
3.1.81	show	3-144
3.1.82	stagescan	3-145
3.1.83	unlabelvol	3-146
3.1.84	unloadvol	3-148
3.1.85	unmountdev	3-149
3.1.86	unresdev	3-150
3.1.87	unrmsection	3-151
3.1.88	unset	3-153
3.1.89	updatehost	3-153
3.1.90	vault	3-155
3.1.91	vfylibs	3-156

4 obtool Placeholders

4.1.1	aspec	4-1
4.1.2	authtype	4-3
4.1.3	backup-container	4-4
4.1.4	backup-level	4-4
4.1.5	concjobs	4-5
4.1.6	content	4-5
4.1.7	data-selector	4-6
4.1.8	dataset-dir-name	4-7
4.1.9	dataset-file-name	4-7
4.1.10	dataset-name	4-8
4.1.11	date-range	4-8
4.1.12	date-time	4-9
4.1.13	day-date	4-9
4.1.14	day-specifier	4-12
4.1.15	devicename	4-12
4.1.16	dupevent	4-12
4.1.17	duplicationrule	4-13
4.1.18	duration	4-14
4.1.19	element-spec	4-14
4.1.20	event	4-15
4.1.21	filenumber	4-16

4.1.22	filenumber-list	4-16
4.1.23	iee-range	4-16
4.1.24	iee-spec	4-17
4.1.25	job-type	4-17
4.1.26	name-format	4-19
4.1.27	ndmp-backup-type	4-20
4.1.28	numberformat	4-21
4.1.29	oid	4-21
4.1.30	oid-list	4-22
4.1.31	policyname	4-22
4.1.32	preauth-spec	4-23
4.1.33	produce-days	4-24
4.1.34	protover	4-24
4.1.35	restriction	4-25
4.1.36	role	4-25
4.1.37	rotationrule	4-26
4.1.38	schedule-priority	4-26
4.1.39	se-range	4-27
4.1.40	se-spec	4-27
4.1.41	size-spec	4-28
4.1.42	summary-start-day	4-28
4.1.43	time	4-29
4.1.44	time-range	4-29
4.1.45	vid	4-30
4.1.46	vol-range	4-30
4.1.47	vol-spec	4-31
4.1.48	vol-status	4-31
4.1.49	wwn	4-32

5 obtool Variables

5.1.1	browsemode	5-1
5.1.2	drive	5-1
5.1.3	errors	5-2
5.1.4	escape	5-2
5.1.5	fs	5-2
5.1.6	host	5-3
5.1.7	level	5-3
5.1.8	library	5-3
5.1.9	maxlevel	5-3
5.1.10	namewidth	5-4

5.1.11	numberformat	5-4
5.1.12	snapshot	5-4
5.1.13	verbose	5-4
5.1.14	viewmode	5-5
5.1.15	width	5-5

6 Dataset Language

6.1	Overview of the Dataset Language	6-1
6.2	Dataset File Examples	6-2
6.2.1	Backing Up Multiple Paths on Multiple Hosts	6-2
6.2.2	Including Dataset Files Within Dataset Files	6-2
6.2.3	Defining the Scope of a Backup	6-3
6.3	Backward Compatibility	6-4
6.4.1	Dataset Statements	6-4
6.4.1.1	after backup	6-5
6.4.1.2	before backup	6-6
6.4.1.3	cross all mountpoints	6-7
6.4.1.4	cross local mountpoints	6-8
6.4.1.5	cross remote mountpoints	6-9
6.4.1.6	exclude dir	6-10
6.4.1.7	exclude file	6-11
6.4.1.8	exclude name	6-11
6.4.1.9	exclude oracle database files	6-13
6.4.1.10	exclude path	6-14
6.4.1.11	include catalog	6-15
6.4.1.12	include dataset	6-16
6.4.1.13	include host	6-16
6.4.1.14	include path	6-17
6.4.1.15	setenv NDMP	6-19

7 Defaults and Policies

7.1	Backup Compression Policies	7-1
7.1.1	option	7-2
7.1.2	buffersize	7-2
7.1.3	excludeformats	7-3
7.2	Backup Encryption Policies	7-3
7.2.1	algorithm	7-3
7.2.2	enablehardwareencryption	7-4
7.2.3	encryption	7-5

7.2.4	keytype	7-5
7.2.5	rekeyfrequency	7-6
7.2.6	requireencryptablemedia	7-6
7.3	Copy Backup Image Instance Policies	7-7
7.3.1	defaultjobpriority	7-7
7.3.2	encryption	7-7
7.3.3	copyoptions	7-8
7.4	Cloud Storage Device Policies	7-8
7.4.1	proxyserver	7-8
7.4.2	proxyuser	7-8
7.4.3	proxypassword	7-9
7.4.4	segmentsize	7-9
7.4.5	streamsperjob	7-9
7.4.6	transfertimeout	7-9
7.4.7	usepersistentcon	7-9
7.5	Daemon Policies	7-9
7.5.1	auditlogins	7-10
7.5.2	obhttpdwindowslogon	7-10
7.5.3	obhttpdwindowspassword	7-10
7.5.4	obixdmaxupdaters	7-10
7.5.5	obixdrechecklevel	7-11
7.5.6	obixdupdaternicevalue	7-11
7.5.7	webautostart	7-11
7.5.8	webpass	7-12
7.5.9	windowscontrolcertificateservice	7-13
7.6	Device Policies	7-13
7.6.1	checkserialnumbers	7-13
7.6.2	deletediskorphans	7-14
7.6.3	disableasyncio	7-15
7.6.4	discovereddevicestate	7-15
7.6.5	errorrate	7-15
7.6.6	maxdriveidletime	7-15
7.6.7	maxacsejectwaittime	7-16
7.6.8	poolfreespacegoal	7-17
7.6.9	returntoservicecheck	7-17
7.7	Duplication Policies	7-17
7.7.1	duplicateovernetwork	7-17
7.7.2	duplicationjobpriority	7-18
7.7.3	duplicationoptions	7-18
7.8	Index Policies	7-19
7.8.1	asciiindexrepository	7-19

7.8.2	autoindex	7-19
7.8.3	earliestindexcleanuptime	7-19
7.8.4	generatendmpindexdata	7-20
7.8.5	indexcleanupfrequency	7-20
7.8.6	latestindexcleanuptime	7-20
7.8.7	maxindexbuffer	7-20
7.8.8	positiondatainterval	7-21
7.8.9	saveasciiindexfiles	7-21
7.9	Log Policies	7-22
7.9.1	adminlogevents	7-22
7.9.2	adminlogfile	7-22
7.9.3	clientlogevents	7-23
7.9.4	jobretaintime	7-23
7.9.5	logretaintime	7-23
7.9.6	transcriptlocation	7-23
7.9.7	transcriptretaintime	7-24
7.9.8	unixclientlogfile	7-24
7.9.9	windowsclientlogfile	7-24
7.10	Media Policies	7-24
7.10.1	barcodesrequired	7-25
7.10.2	blockingfactor	7-25
7.10.3	freedstucktapethreshold	7-25
7.10.4	maxblockingfactor	7-26
7.10.5	overwriteblanktape	7-26
7.10.6	overwriteforeigntape	7-26
7.10.7	overwriteunreadabletape	7-27
7.10.8	volumeretaintime	7-27
7.10.9	writewindowtime	7-27
7.11	Naming Policies	7-27
7.11.1	winsserver	7-27
7.12	NDMP Policies	7-28
7.12.1	authenticationtype	7-28
7.12.2	backupev	7-28
7.12.3	backuptype	7-29
7.12.4	dmahosts	7-29
7.12.5	password	7-29
7.12.6	port	7-30
7.12.7	protocolversion	7-30
7.12.8	restoreev	7-30
7.12.9	username	7-31
7.13	Operations Policies	7-31

7.13.1	autohistory	7-32
7.13.2	autolabel	7-32
7.13.3	backupimagerechecklevel	7-32
7.13.4	backupoptions	7-33
7.13.5	databuffersize	7-33
7.13.6	disablerds	7-34
7.13.7	fullbackupcheckpointfrequency	7-34
7.13.8	incrbackupcheckpointfrequency	7-34
7.13.9	overwritecheckfrequency	7-35
7.13.10	mailport	7-35
7.13.11	mailserver	7-35
7.13.12	mailfrom	7-35
7.13.13	maxcheckpointrestarts	7-36
7.13.14	maxentriesrestoreoperation	7-36
7.13.15	progressupdatefrequency	7-36
7.13.16	restartablebackups	7-36
7.13.17	restoreoptions	7-37
7.13.18	rmanpriority	7-37
7.13.19	rmanresourcewaittime	7-38
7.13.20	rmanrestorestartdelay	7-38
7.13.21	tcpbufsize	7-38
7.13.22	useloadbalance	7-38
7.13.23	windowsskipcdfs	7-39
7.13.24	windowsskiplockedfiles	7-39
7.14	Scheduler Policies	7-39
7.14.1	applybackupsfrequency	7-40
7.14.2	cachealljobs	7-40
7.14.3	defaultstarttime	7-40
7.14.4	maxdataretries	7-41
7.14.5	pollfrequency	7-41
7.14.6	recyclejobthreshold	7-41
7.14.7	retainbackupmetrics	7-41
7.15	Security Policies	7-42
7.15.1	autocertissue	7-42
7.15.2	certkeysize	7-43
7.15.3	certlifetime	7-43
7.15.4	certwarning	7-43
7.15.5	encryptdataintransit	7-44
7.15.6	loginduration	7-44
7.15.7	minuserpasswordlen	7-44
7.15.8	passwordgracetime	7-44

7.15.9	passwordlifetime	7-45
7.15.10	passwordreusetime	7-45
7.15.11	securecomms	7-45
7.15.12	trustedhosts	7-45
7.15.13	untrustedhostjobs	7-46
7.15.14	webinactivitytimeout	7-46
7.15.15	websessiontimeout	7-46
7.16	Staging Policies	7-46
7.16.1	defaultscanjobpriority	7-46
7.16.2	obstagescandebuglevel	7-47
7.17	Vaulting Policies	7-47
7.17.1	autorunmmjobs	7-47
7.17.2	autovolumerelease	7-48
7.17.3	invretrydelay	7-48
7.17.4	maxinvretrytime	7-48
7.17.5	minwritablevolumes	7-49
7.17.6	offsitecustomerid	7-49
7.17.7	reportretaintime	7-49

8 Classes and Rights

8.1	Class Rights	8-2
8.1.1	access file system backups	8-2
8.1.2	access Oracle database backups	8-3
8.1.3	browse backup catalogs with this access	8-3
8.1.4	display administrative domain's configuration	8-4
8.1.5	modify administrative domain's configuration	8-4
8.1.6	list any backup, regardless of its owner	8-4
8.1.7	list any backups owned by user	8-4
8.1.8	list any job, regardless of its owner	8-5
8.1.9	list any jobs owned by user	8-5
8.1.10	manage devices and change device state	8-5
8.1.11	modify any backup, regardless of its owner	8-5
8.1.12	modify any backups owned by user	8-5
8.1.13	modify any job, regardless of its owner	8-5
8.1.14	modify any jobs owned by user	8-5
8.1.15	modify catalog	8-6
8.1.16	modify own name and password	8-6
8.1.17	perform file system backups as privileged user	8-6
8.1.18	perform file system backups as self	8-6
8.1.19	perform Oracle database backups and restores	8-6

8.1.20	perform file system restores as privileged user	8-6
8.1.21	perform file system restores as self	8-7
8.1.22	query and display information about devices	8-7
8.1.23	receive email describing internal errors	8-7
8.1.24	receive email regarding expired passphrase keys	8-7
8.1.25	receive email requesting operator assistance	8-7

A Miscellaneous Programs

A.1.1	makedev	A-1
A.1.2	obcleanup	A-3
A.1.3	obcm	A-5
A.1.4	uninstallob	A-9

B obtar

B.1	obtar Overview	B-1
B.2	Optimizing Your Use of obtar	B-2
B.2.1	Using tar with Backup Images Created by obtar	B-2
B.2.2	Backing Up and Restoring Raw File Systems	B-3
B.2.2.1	Backing Up Raw Partitions	B-4
B.2.2.2	Restoring Raw Partitions	B-4
B.2.3	Changing Criteria for Incremental Backups	B-4
B.2.4	Backing Up Across Mount Points	B-5
B.3.1	obtar -c	B-6
B.3.2	obtar -x	B-8
B.3.3	obtar -t	B-11
B.3.4	obtar -zz	B-14
B.3.5	obtar Options	B-14

C RMAN Media Management Parameters

C.1	Database Backup Storage Selectors and RMAN Media Management Parameters	C-1
C.2	About Setting the Job Priority for RMAN Operations	C-2
C.3.1	OB_BACKUP_NAME	C-2
C.3.2	OB_DEVICE	C-3
C.3.3	OB_ENCRYPTION	C-4
C.3.4	OB_IGNORE_NUMA	C-6
C.3.5	OB_MEDIA_FAMILY	C-6
C.3.6	OB_PRIORITY	C-7
C.3.7	OB_RESOURCE_WAIT_TIME	C-8

D Oracle Secure Backup Support for Extended Attributes and Access Control Lists

D.1	Overview of Extended Attributes and Access Control Lists	D-1
D.2	Supported Platforms	D-2
D.3	Requirements	D-2
D.4	Security Practices	D-3
D.5	Performing Backup and Recovery with Extended Attributes and Access Control Lists on Linux and Unix	D-3

E Startup and Shutdown of Oracle Secure Backup Services

Glossary

Index

List of Examples

2-1	Adding Backup Windows	2-1
2-2	Adding Duplication Windows	2-2
2-3	Enabling Verbose Output from the NDMP Data Service	2-3
2-4	Making a Full Backup	2-10
2-5	Restricting Backups to Different Devices	2-10
2-6	Backing Up to a Disk Pool	2-11
2-7	Backing Up to a Cloud Storage Device	2-11
2-8	Transferring Backup Ownership to Another User	2-12
2-9	Displaying the Transcript for a Hanging Backup	2-13
2-10	Borrowing a Tape Drive	2-13
2-11	Resuming a Job After Borrowing a Device	2-13
2-12	Cancelling a Backup Job	2-14
2-13	Cataloging a Volume	2-17
2-14	Cataloging a Disk Pool	2-18
2-15	Displaying the Contents of a Dataset	2-19
2-16	Listing Media Movement Reports	2-22
2-17	Displaying a Job Transcript	2-24
2-18	Displaying the Transcript for a Hanging Backup	2-24
2-19	Displaying a Job Continuously	2-25
2-20	Displaying Warnings for a Job	2-25
2-21	Changing Directories	2-26
2-22	Making a Dataset Directory	2-27
2-23	Browsing Policy Information	2-28
2-24	Changing Classes	2-29
2-25	Reconfiguring a Tape Drive	2-38
2-26	Reconfiguring a Tape Library	2-39
2-27	Reconfiguring a Disk Pool	2-40
2-28	Reconfiguring a Cloud Storage Device	2-40
2-29	Modifying a Duplication Policy	2-42
2-30	Changing a Host	2-47
2-31	Checking for the Existence of Backup Windows	2-48
2-32	Checking a File for Syntax	2-49
2-33	Checking Files for Syntax	2-49
2-34	Modifying a Location Object	2-52
2-35	Changing Properties of a Media Family	2-53

2-36	Adding a PNI for a Host	2-55
2-37	Adding a PNI for Outbound Connections for a Host	2-55
2-38	Changing a Rule in a Rotation Policy	2-57
2-39	Changing a Backup Schedule	2-64
2-40	Adding Content Types to a Database Backup Storage Selector	2-68
2-41	Changing a Job Summary Schedule	2-71
2-42	Changing an Oracle Secure Backup User	2-74
2-43	Changing Password Settings for an Oracle Secure Backup User	2-75
2-44	Changing Volume Attributes	2-78
2-45	Cleaning a Tape Drive	2-79
2-46	Closing a Library Door	2-80
2-47	Suspending the obscheduled Daemon	2-84
2-48	Discovering Devices Attached to an Oracle Secure Backup Host	2-88
2-49	Dumping the Error Log for a Tape Drive	2-89
2-50	Duplicating a Volume	2-91
2-51	Checking a File for Syntax	2-92
2-52	Exiting obtool	2-93
2-53	Exporting a Volume	2-95
2-54	Extracting a Volume	2-97
2-55	Finding Backup Entries on a Host	2-99
2-56	Finding a Type of Entry on a Host	2-99
2-57	Finding Backups Using the Hostname	2-99
2-58	Displaying the Current User	2-100
2-59	Identifying Volumes	2-102
2-60	Displaying Backup Image Labels	2-102
2-61	Importing Volumes	2-104
2-62	Notifying Oracle Secure Backup of a Manually Inserted Volume	2-107
2-63	Taking an Inventory of a Tape Library	2-109
2-64	Taking an Inventory of a Tape Library that Does not Contain a Barcode Reader	2-110
2-65	Manually Labeling a Volume	2-112
2-66	Loading a Volume in a Tape Drive	2-113
2-67	Displaying the Current User	2-114
2-68	Displaying Information About a File	2-116
2-69	Listing a Backup in Long Form	2-118
2-70	Specifying Backup Image Instances for a Specified Host	2-121
2-71	Displaying Backup Image Details in Long Format	2-121
2-72	Displaying the Contents of Backup Images	2-121

2-73	Listing Cataloged Backups	2-124
2-74	Listing Cataloged Backups for a Specific Instance	2-125
2-75	Listing Backup Windows	2-126
2-76	Listing Checkpoint Information	2-127
2-77	Displaying Information About a Class	2-130
2-78	Listing Daemons in Short Form	2-132
2-79	Listing Daemons in Long Form	2-132
2-80	Listing Daemons in Default Form	2-132
2-81	Listing Details for a Library	2-137
2-82	Displaying Space Consumption Details for a Disk Pool	2-138
2-83	Listing Details for a Cloud Storage Device	2-138
2-84	Displaying the Contents of a Dataset Directory	2-140
2-85	Listing Information About Duplication Policies	2-140
2-86	Listing File Systems on an NDMP Host	2-142
2-87	Displaying Host Information	2-145
2-88	Listing Duplicate Volumes for Backup Image Instances	2-147
2-89	Displaying Backup Image Instance Details in Long Format	2-147
2-90	Displaying Backup Sections for a Backup Image Instance	2-147
2-91	Displaying Staging Information in Long Format	2-148
2-92	Filtering Jobs by State	2-154
2-93	Filtering Jobs by Time	2-154
2-94	Filtering Jobs by Host	2-154
2-95	Filtering Jobs by User	2-154
2-96	Displaying Job Data in Long Format	2-154
2-97	Displaying All Time-Related Data	2-155
2-98	Displaying Subjob Data in Long Format	2-155
2-99	Listing Media Family Information	2-157
2-100	Listing Log Policies	2-159
2-101	Listing Policies by Type	2-159
2-102	Listing a Security Password Policy	2-159
2-103	Displaying Backup Pieces	2-161
2-104	Displaying Volume ID Used by Backup Pieces	2-162
2-105	Listing PNIs	2-163
2-106	Listing Restore Requests	2-165
2-107	Listing Media Management Reports	2-167
2-108	Displaying Backup	2-169
2-109	Displaying Backup for the Stage Scan Type	2-170

2-110	Listing Backup Sections	2-172
2-111	Displaying Snapshots	2-175
2-112	Displaying a Database Backup Storage Selector	2-177
2-113	Listing Stage Rules in Short Format	2-177
2-114	Listing Stage Rules in Long Format	2-178
2-115	Displaying Job Summary Schedules	2-179
2-116	Displaying Oracle Secure Backup User Information	2-182
2-117	Displaying the Volumes in a Library	2-186
2-118	Displaying the Contents of a Volume	2-187
2-119	Displaying the Volumes that Can be Recycled	2-187
3-1	Deleting Expired Backup Image Instances for a Specified Host	3-2
3-2	Making a Class	3-6
3-3	Configuring a Tape Drive	3-19
3-4	Configuring a Tape Library	3-20
3-5	Configuring a Disk Pool	3-20
3-6	Configuring a Tape Library with Device File on Linux	3-20
3-7	Configuring a Cloud Storage Device	3-20
3-8	Creating a Dataset	3-23
3-9	Creating a Dataset Subdirectory	3-23
3-10	Creating a Dataset for a Windows Host	3-23
3-11	Creating a Volume Duplication Policy	3-25
3-12	Adding a Host Running Oracle Secure Backup Locally	3-33
3-13	Adding a Host with a Large Key Size	3-33
3-14	Adding an NDMP Host	3-33
3-15	Creating a Location Object	3-35
3-16	Creating a Time-Managed Media Family	3-39
3-17	Creating a Content-Managed Media Family	3-39
3-18	Defining a PNI	3-41
3-19	Configuring a Single Interface for Outbound Connections	3-41
3-20	Configuring a Network for Outbound Connections	3-42
3-21	Using Any Network to Establish and Outbound Connection	3-42
3-22	Scheduling a Weekly Backup	3-52
3-23	Creating a Snapshot	3-54
3-24	Creating a Database Backup Storage Selector	3-57
3-25	Generating Stage Rules That Match RMAN Backup Images	3-60
3-26	Generating Stage Rules That Match RMAN Backup Images of a Specified Age	3-60
3-27	Staging File-system Backups for Two Hosts	3-60

3-28	Staging File-system Backups for a Single Host That Are at Least 4TB Size Total	3-60
3-29	Copying Backup Image Instances With Any Media Family Containing Database Pieces	3-61
3-30	Scheduling a Job Summary	3-63
3-31	Sample Job Summary	3-64
3-32	Creating an Oracle Secure Backup User	3-67
3-33	Creating an Oracle Backup User with Specific Password Settings	3-68
3-34	Creating an Oracle Secure Backup User with a Windows Domain	3-68
3-35	Manually Mounting a Tape Volume	3-70
3-36	Moving a Volume	3-72
3-37	Opening an Import/Export Door	3-73
3-38	Pinging a Tape Drive with Multiple Attachments	3-74
3-39	Pinging a Host	3-75
3-40	Displaying the Current Directory	3-76
3-41	Displaying the Current Directory	3-77
3-42	Displaying the Current Directory in the Policy Tree	3-78
3-43	Quitting obtool	3-79
3-44	Renaming Backup Images	3-82
3-45	Renaming a Class	3-83
3-46	Renaming a Device	3-84
3-47	Renaming a Dataset	3-85
3-48	Renaming a Volume Duplication Policy	3-86
3-49	Renaming a Host	3-87
3-50	Renaming a Media Family	3-89
3-51	Renaming a Backup Schedule	3-91
3-52	Renaming a Snapshot	3-92
3-53	Renaming a Database Backup Storage Selector	3-93
3-54	Renaming a Stage Rule	3-94
3-55	Renaming a Job Summary Schedule	3-95
3-56	Renaming an Oracle Secure Backup User	3-96
3-57	Reserving a Device	3-97
3-58	Resetting Policies to Their Default Values	3-98
3-59	Resetting Password Policies to Their Default Values	3-98
3-60	Performing a Raw Restore Operation Based on the Oracle Secure Backup Catalog	3-105
3-61	Performing a Raw Restore Operation	3-105
3-62	Performing a Catalog Based Restore using Oracle Secure Backup Wildcard Pattern Matching	3-105
3-63	Returning Borrowed Devices	3-106

3-64	Reusing a Volume	3-107
3-65	Deleting a Backup Request	3-109
3-66	Removing Backup Windows	3-110
3-67	Removing Checkpoints	3-111
3-68	Removing a Class	3-112
3-69	Removing a Tape Drive	3-114
3-70	Removing a Disk Pool and Its Contents	3-114
3-71	Removing a Dataset	3-115
3-72	Removing a Duplication Policy	3-116
3-73	Removing a Duplication Window	3-117
3-74	Removing a Host	3-118
3-75	Removing a Job	3-120
3-76	Removing Media Families	3-122
3-77	Enabling Verbose Output from the NDMP Data Service	3-123
3-78	Removing Backup Pieces	3-124
3-79	Removing All PNI Definitions for a Host	3-125
3-80	Removing a Client from All PNI Definitions	3-126
3-81	Removing All PNI Definitions That Use a Specified Interface	3-126
3-82	Removing Clients from a PNI Definition	3-126
3-83	Removing a Restore Request	3-127
3-84	Removing a Backup Schedule	3-129
3-85	Removing Backup Sections	3-130
3-86	Removing a Snapshot	3-131
3-87	Removing a Snapshot	3-131
3-88	Deleting a Database Backup Storage Selector	3-133
3-89	Example Title	3-133
3-90	Removing a Job Summary Schedule	3-134
3-91	Removing an Oracle Secure Backup User	3-135
3-92	Displaying Information About a Job Requesting Assistance	3-137
3-93	Displaying Information About a Job Requesting Assistance	3-138
3-94	Running a Job Now	3-139
3-95	Setting a Variable	3-140
3-96	Changing Backup Windows	3-141
3-97	Setting a Duplication Window	3-142
3-98	Setting Policy Values	3-143
3-99	Setting the Port Number for NDMP Daemons	3-143
3-100	Setting the Password Lifetime Security Policy	3-144

3-101	Setting the Policy to Cross Mount Points During a File-System Backup	3-144
3-102	Setting the Certificate Lifetime and Warning Policies	3-144
3-103	Showing the Value of a Variable	3-145
3-104	Running an On-Demand Stagescan Job	3-146
3-105	Unlabeling a Volume	3-147
3-106	Unloading a Volume from a Tape Drive	3-148
3-107	Unmounting a Tape Volume	3-150
3-108	Unreserving a Device	3-151
3-109	Undoing the Deletion of Backup Sections	3-152
3-110	Undefining a Variable	3-153
3-111	Updating a Host	3-154
3-112	Recertifying a Host	3-155
3-113	Scheduling an On-Demand Vaulting Scan	3-156
3-114	Checking the Configuration of a Tape Library	3-158
3-115	Running vftlibs When a Robot Process Is Active	3-158
3-116	Running vfylibs When IDs Do Not Match	3-158
4-1	aspec	4-3
4-2	date-time	4-9
4-3	day-date	4-11
4-4	duration	4-14
4-5	iee-range	4-17
4-6	oid-list	4-22
4-7	preauth-spec	4-24
4-8	se-range	4-27
4-9	time	4-29
4-10	time-range	4-30
4-11	vol-range	4-31
6-1	Sample Dataset	6-2
6-2	Backing Up Multiple Paths on Multiple Hosts	6-2
6-3	common-exclusions.ds	6-3
6-4	Including a Dataset File	6-3
6-5	Applying Exclusions to a Path	6-3
6-6	Using Braces to Limit Scope	6-3
6-7	Refining the Scope of a Set of Rules	6-3
6-8	after backup Statement	6-6
6-9	before backup Statement	6-7
6-10	Global Host Inclusion	6-8

6-11	Global Path Inclusion	6-8
6-12	Local Path Inclusion	6-8
6-13	Global Host Inclusion	6-9
6-14	Global Path Inclusion	6-9
6-15	Local Path Inclusion	6-9
6-16	Global Host Inclusion	6-10
6-17	Global Path Inclusion	6-10
6-18	Local Path Inclusion	6-10
6-19	exclude name Statement	6-12
6-20	exclude oracle database files Statement	6-13
6-21	exclude path Statement	6-14
6-22	include catalog Directive with Extra Files	6-16
6-23	include dataset Statement	6-16
6-24	include path Statement	6-17
6-25	include path Statement on Windows	6-18
6-26	include path Statement on Linux/UNIX	6-18
6-27	include host Statements	6-18
6-28	Dataset File with include host and include path Statements	6-19
6-29	Dataset File with include host and include path Statements	6-19
6-30	Dataset File for backing up Obfuscated Wallets in Unencrypted Backups	6-19
6-31	Adding NDMP Values to a Dataset	6-20
A-1	Creating a Device Special File for a Tape Drive	A-3
A-2	Sample Output from obcleanup	A-4
A-3	Exporting a Signed Certificate Chain	A-8
A-4	Importing a Signed Certificate Chain	A-8
A-5	Creating a Cloud Wallet Containing Trust Points Using Certificate Files	A-8
A-6	Uninstalling Oracle Secure Backup	A-9
B-1	Backing Up to a Volume	B-7
B-2	Backing Up Multiple Files	B-7
B-3	Changing Directory Information	B-7
B-4	Changing Directory Information	B-8
B-5	Extracting Files from a Backup Image	B-10
B-6	Displaying the Contents of a Backup Image	B-10
B-7	Displaying the Volume Label	B-10
B-8	Extracting Data to a Different Location	B-10
B-9	Preventing obtar from Overwriting Files	B-10
B-10	Restoring a Raw File-System Partition	B-10

B-11	Displaying the Contents of a Backup Image	B-12
B-12	Displaying the Contents of a Backup Image on a Volume Set	B-12
B-13	Displaying Additional Information About a Backup Image	B-12
B-14	Displaying Information About a File in an Image	B-12
B-15	Displaying Information About Multiple Directories	B-12
B-16	Cataloging a File-System Backup Image	B-13
B-17	Cataloging an RMAN Backup Image	B-13
B-18	Displaying the Labels of All Backup Images on a Volume	B-14
C-1	Backup Name with SEND Command	C-3
C-2	SBT Backup with SEND Command	C-4
C-3	SBT Backup with ENV Parameter	C-4
C-4	Encrypted Backup with SEND Command	C-5
C-5	Persistent Encryption Configuration	C-5
C-6	Disabling NUMA-awareness	C-6
C-7	SBT Backup with SEND Command	C-7
C-8	SBT Backup with ENV Parameter	C-7
C-9	Setting Priority with SEND command	C-8
C-10	Setting Priority with ENV Parameter	C-8
C-11	SBT Restore with SEND Command	C-9
C-12	SBT Restore with ENV Parameter	C-9
C-13	Restore with Device Name Specified	C-11

List of Tables

1-1	Priority of Preauthorization Matching	1-3
1-2	cl-option	1-3
1-3	Values for Confirmation Message	1-4
1-4	Online Help Options	1-7
1-5	Command Topics for Oracle Secure Backup	1-7
2-1	Message Levels	2-23
2-2	Values for --command	2-84
2-3	Output of the lsbackup command	2-118
2-4	Output of the lsbu command	2-124
2-5	Ischeckpoint Output	2-127
2-6	Isclass Output	2-129
2-7	Isdaemon Output	2-132
2-8	Isdev Output	2-135
2-9	Isfs Output	2-142
2-10	Ishost Output	2-144
2-11	Isjob Output	2-153
2-12	Ismf Output	2-157
2-13	Ispiece Output	2-161
2-14	Ispni Output	2-163
2-15	Isrestore Output	2-165
2-16	Issched Output	2-168
2-17	Issection Output	2-171
2-18	Issnap Output	2-174
2-19	Isssel Output	2-176
2-20	Issum Output	2-179
2-21	Isuser Output	2-181
2-22	Isvol Output	2-186
4-1	Raw Device Names for Popular Systems	4-2
8-1	Classes and Rights	8-1
A-1	Default SCSI Bus Designations	A-2
B-1	obtar Modes	B-1
B-2	obtar Options	B-15
B-3	mask Values	B-21
C-1	Determining Media Family and Device Settings	C-2
D-1	Supporting Platforms for Extended Attributes and Access Control Lists	D-2

Preface

This document provides information on Oracle Secure Backup command syntax and semantics.

Audience

This book is intended for system administrators and database administrators who install, configure or use Oracle Secure Backup. To use this document, you must be familiar with the operating system environment on which you plan to use Oracle Secure Backup.

 **Note:**

To perform Oracle database backup and restore operations, you should also be familiar with Oracle backup and recovery concepts, including Recovery Manager (RMAN).

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 that have purchased support 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 on Oracle Secure Backup, see the following Oracle resources:

- *Oracle Secure Backup Administrator's Guide*
This book describes how to use Oracle Secure Backup to perform backup and restore operations. The book is oriented to the Oracle Secure Backup Web tool, which is a Web-based GUI interface.
- *Oracle Secure Backup Installation and Configuration Guide*

This book describes how to install Oracle Secure Backup, and how to manage your administrative domain. The book is relevant for both file-system and database backup and restore operations.

- *Oracle Database Backup and Recovery User's Guide*

This book provides an overview of backup and recovery and discusses backup and recovery strategies. It provides instructions for basic backup and recovery of your database using Recovery Manager (RMAN). It also covers more advanced database backup and recovery topics, including performing user-managed backup and recovery for users who choose not to use RMAN.

You can access the Oracle Secure Backup product download site from the Oracle Secure Backup product Web site, which is located at the following URL:

<http://www.oracle.com/technetwork/database/database-technologies/secure-backup/documentation/securebackup-094467.html>

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 Secure Backup Reference

This preface contains information about new and changed features for Oracle Secure Backup 12c Release 2 (12.2).

Changes in Oracle Secure Backup 12c Release 2 (12.2.0.1)

The following are the changes in *Oracle Secure Backup Reference* for Oracle Database 12c Release 2 (12.2.0.1).

New Features

- New staging commands let you temporarily store one or more backup image instances in a disk pool storage container in preparation for automatically copying or moving the backup image instances to another container. For example, a backup instance can be moved from a disk pool to a tape volume or a cloud container.
See [Staging Commands](#) (page 1-21)
- Oracle Secure Backup now supports backup to Oracle Cloud Infrastructure Object Storage Classic. Backup data can be written to either Oracle Cloud Object Storage or Archive Storage. Oracle Cloud storage is accessed and managed using Oracle Secure Backup cloud storage devices in a manner similar to other Oracle Secure Backup devices.

All backup data is securely written to cloud storage devices by encrypting the backup data at the client host, with encryption keys being managed by the Oracle Secure Backup administrative server.

Cloud storage devices can also be used as targets for staging, which allows you to back up your data to a faster disk pool and then move it to the cloud.

You can also copy backup instances from Oracle Cloud Infrastructure Object Storage Classic to Oracle Cloud Infrastructure Archive Storage Classic for long-term retention.

- Oracle Secure Backup software compression is now supported on Windows systems, as well as on UNIX systems. Additionally, multiple levels of compression are now available: `low`, `medium`, `basic`, and `high`. These new options are more efficient, in terms of compression ratio and speed, than the existing compression method using the `obtar -z` option (which is available only on UNIX systems).

See the `--compression` option of the [backup](#) (page 2-4) command. Also see [Backup Compression Policies](#) (page 7-1).

Deprecated Features

The following feature was deprecated as of Oracle Secure Backup 12c Release 2 (12.2.0.1), and may be desupported in a future release:

- `obtar -z` option

Compresses data (when backing up) or keeps data compressed (when restoring).

As of Oracle Secure Backup 12c Release 2 (12.2.0.1), new backups are not allowed to compress data using the `-Z` option. The `-Z` option is retained only for use in restoring older compressed legacy backups with the `restore` command.

The following feature was deprecated as of Oracle Secure Backup 12c Release 1 (12.1.0.3), and may be desupported in a future release:

- `obcopy` utility

The `obcopy` utility copies one tape volume to another. This utility is deprecated.

It is recommended that you use the [dupvol](#) (page 2-90) command to duplicate a tape volume.

1

About obtool

This chapter explains how to use the [obtool](#) command-line interface. It contains the following topics:

- [obtool Invocation](#) (page 1-1)
- [obtool Online Help](#) (page 1-7)
- [obtool Command Categories](#) (page 1-9)
- [obtool Lexical Conventions](#) (page 1-23)
- [obtool Exit Codes](#) (page 1-24)

1.1 obtool Invocation

This section explains how to invoke the obtool utility, which is a command-line interface to Oracle Secure Backup. You can obtain online help about obtool invocation options by running the following command at the operating system prompt:

```
% obtool help invocation
```

The obtool utility displays the following output:

```
obtool invocation:
Usage: To enter interactive mode:
      obtool [<cl-option>]...
Usage: To execute one command and exit:
      obtool [<cl-option>]... <command> [<option>]... [<argument>]...
Usage: To display program version number and exit:
      obtool --version/-V
```

The following sections explain the obtool invocation options in more detail.

1.1.1 obtool Login

The first time you invoke the obtool utility, you are required to establish your identity as an [Oracle Secure Backup user](#). If you have not yet established an Oracle Secure Backup user identity, then obtool prompts you for a user name and password, as shown in the following example:

```
% obtool
Oracle Secure Backup 12.2.0.1.0
login:
```

Oracle Secure Backup creates the `admin` user automatically at installation and prompts you for the password.

 **Note:**

The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the Oracle Secure Backup user be prompted for the password.

 **See Also:**

- "[User Commands](#) (page 1-22)" for information on setting up Oracle Secure Backup user identities
- "[Policy Commands](#) (page 1-18)" for more information about the `security/loginduration` policy

1.1.1.1 Login and Preauthorization

After you have logged into obtool, Oracle Secure Backup stores your identity in a login token located in the `/admin/config/user` subdirectory. The information for each Oracle Secure Backup user is stored in a separate file. The lifetime of the login token is controlled by the [loginduration](#) (page 7-44) security policy.

Oracle Secure Backup command-line tools authenticate users either with an explicit login or with a [preauthorization](#). In the latter case, access is authorized only for the specified operating system user on the specified host. You can create a preauthorization by specifying `--preauth` on the [mkuser](#) (page 3-64) command.

When you invoke an Oracle Secure Backup command-line tool, it finds the user ID according to the following rules of precedence:

1. If you specify an explicit user ID, then the user ID is used for the operation. You must specify the correct password for this user ID.
2. If you do not specify a user ID, and if an applicable login token exists that indicates that this user has a persistent explicit login, then Oracle Secure Backup uses the user ID associated with this token for the operation. Note that persistent tokens are never created for sessions that have been preauthorized.
3. If you do not specify a user ID, and if no applicable persistent login token exists, then Oracle Secure Backup attempts to find a matching preauthorization. If no preauthorization exists, then some command-line tools prompt for a user ID, whereas others fail and exit.

The rules for locating a matching preauthorization are the same for both command-line operations and [Recovery Manager \(RMAN\)](#) backup and restore operations. If two or more preauthorizations could match, then Oracle Secure Backup prioritizes matches as shown in [Table 1-1](#) (page 1-3).

Table 1-1 Priority of Preauthorization Matching

priority	host name	userid	domain
1	explicitly specified	explicitly specified	explicitly specified
2	*	explicitly specified	explicitly specified
3	*	explicitly specified	unspecified
4	*	unspecified	unspecified

1.1.2 obtool Interactive Mode

To use obtool in interactive mode, enter `obtool` at the operating system command line.

1.1.2.1 obtool Syntax for Interactive Mode

Use the following syntax when invoking obtool in interactive mode:

```
obtool [ cl-option ]...
```

[Table 1-2](#) (page 1-3) describes the legal substitutions for the *cl-option* placeholder.

Table 1-2 cl-option

Option	Meaning
<code>--longerrors/-E</code>	Shows error messages in long form. See also " errors (page 5-2)".
<code>--norc/-n</code>	Does not run commands from <code>.obtoolrc</code> . You can put a sequence of <code>obtool</code> commands in this file for obtool to run whenever it is invoked. By default, obtool automatically searches for <code>.obtoolrc</code> in the current directory. If this file is not found and if the HOME environment variable is defined, then obtool searches for the file in the HOME directory. When the file is located, obtool reads the file before it enters interactive mode.
<code>--verbose/-v</code>	Displays extra informational messages. See also " verbose (page 5-4)".

1.1.2.2 Command Execution in Interactive Mode

After a successful login to obtool, the following prompt is displayed:

```
ob>
```

You can enter the commands described in [obtool Commands: addbw to lsvol](#) (page 2-1) at the obtool prompt. Note that some commands provide an `--nq` option, which specifies that no confirmation message should be displayed after you run the command. If you do not include the `--nq` option for these commands, then obtool prompts you for confirmation. You must enter a value from [Table 1-3](#) (page 1-4) at the confirmation prompt.

Table 1-3 Values for Confirmation Message

Value	Meaning
y	Perform the operation on the object named in the query.
n	Do not perform the operation on the object named in the query and proceed to the next selection (if any).
q	Do not perform the operation on the object named in the query and stop processing this command immediately. Note that objects for which you have answered y have been affected.
a	Perform the operation on the object named in the query and on all objects that the command has not yet included in a query. Note that objects for which you have answered n are not affected.
?	Display brief help text and then redisplay the prompt.

In the prompt, the item in brackets ([. . .]) indicates the default if you do not reply to the prompt.

1.1.2.3 Input Redirection in Interactive Mode

In interactive mode, you can redirect input to a script containing multiple obtool commands. This technique is useful if you must run the same series of obtool commands on a regular basis. The syntax is as follows, where *pathname* is the path name of a file containing obtool commands:

```
ob> pathname
```

For example, you can create a file called `mycommands.txt` with the following content:

```
# begin mycommands.txt
lsdev --long
lshost --long
# end
```

You can redirect the obtool input to this script as follows:

```
ob> < /home/mycommands.txt
```

1.1.2.4 Exiting obtool

Use the [exit](#) (page 2-93) command to exit obtool, as shown in the following example:

```
ob> exit
```

1.1.3 obtool Noninteractive Mode

To pass a command to obtool on the command line, use the following syntax:

```
obtool [ cl-option ]... command-name [ option ]... [ argument ]...
```

The following example runs the obtool [lsdev](#) (page 2-133) command and then returns to the operating system prompt:

```
% obtool lsdev
library      libl          in service
```

```
drive 1  tape1          in service
library  lib2           in service
drive 1  tape2          in service
```

1.1.3.1 Escaping Special Characters in obtool Command Line

As with any command line, it might be necessary to quote characters that are significant to the command line interpreter or shell from which obtool is invoked. For example:

- When running obtool commands from the command line that include a semicolon, quotes might be required to prevent the semicolon from being interpreted by the shell. See "[Running Multiple obtool Commands Non-Interactively](#) (page 1-5)" for details on the use of the semicolon in command lines.
- If the obtool escape character is set to the ampersand (&) character (see "[escape](#) (page 5-2)"), and if you specify & as part of a file name when running obtool commands noninteractively, then enclose the file name within single quotes. For example:

```
obtool cd -h phred '/home/markb&patti'
```

Because the ampersand character is within single quotes, it is not interpreted and is considered part of the file name.

1.1.3.2 Running Multiple obtool Commands Non-Interactively

To run multiple obtool commands in non-interactive mode, separate the commands with a semicolon. When used in this manner, the output of each obtool command is preceded by a line of text that displays the command processed. The following example illustrates the use of two commands in a Linux bash shell:

```
oblin1$ obtool lsmf -s ';' lsh -s
Output of command : lsmf -s
RMAN-DEFAULT

Output of command : lsh -s
brhost2
brhost3
stacb40
```

Each command returns `Output of command :` and the command name even if the command does not give any other output.

1.1.3.3 Redirecting obtool Commands From an Input File

You can redirect input to obtool when in noninteractive mode. For example, you can create a file called `mycommands.txt` with the following content:

```
# begin mycommands.txt
lsdev --long
lshost --long
# end
```

You can redirect the obtool input to this script as follows:

```
obtool < /home/mycommands.txt
```

You can also nest redirection files. For example, you can create a second command file called `mycommands2.txt` and then edit `mycommands.txt` as follows to redirect input from `mycommands2.txt`:

```
# begin mycommands.txt
lsdev --long
lshost --long
# redirect input to second command file
< /home/mycommands2.txt
# end
```

1.1.4 Exiting obtool

You can end an obtool session by using either the `exit` or `quit` commands, or the `logout` command.

The `exit` command ends the obtool session, but a login token preserves the user's credentials, so that the next time you start obtool you are not prompted for a user name or password. The `quit` command is a synonym for `exit`.

1.1.5 Logging Out of obtool

The `logout` command destroys the login token, so that the user is prompted for credentials during the next obtool session.

For example:

```
[root@osblin1 ~]# obtool
Oracle Secure Backup 12.2.0.1.0
login: admin
Password:
ob> quit
[root@osblin1 ~]# obtool
ob> logout
[root@osblin1 ~]# obtool
Oracle Secure Backup 12.2.0.1.0
login:
```

You can also use the `logout` command in obtool when invoking it in non-interactive mode. For example:

```
[root@osblin1 ~]# obtool -logout
[root@osblin1 ~]# obtool
Oracle Secure Backup 12.2.0.1.0
login:
```

1.1.6 Starting obtool as a Specific User: obtool -u

You can force obtool to use different credentials when starting, destroying any existing login token. To do so, use the `-u` option with `obtool`, specifying the name of the [Oracle Secure Backup user](#) for the session. For example:

```
[root@osblin1 ~]# obtool -u admin
Password:
ob>
```

1.1.7 obtool Domain Authentication

You can force obtool to use request credentials, regardless of whether there is an existing login token. To do so, use the following syntax:

```
obtool --authenticate
```

1.1.8 obtool Version Number

To display program version number and exit, use the following syntax:

```
obtool --version/-V
```

1.1.9 obtool Date and Time Information

If a date reported by an obtool command is more than six months earlier or more than two months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier or less than two months in the future, then it is reported in a `mm/dd.hh:mm` format.

1.2 obtool Online Help

[Table 1-4](#) (page 1-7) displays the online help options for the obtool utility.

Table 1-4 Online Help Options

Help topic	Command
A list of help topics	<code>help topics</code>
Help for a specific topic	<code>help topic-name</code>
Usage for a specific command	<code>help command-name</code>
Usage for all commands related to a topic	<code>help topic-name usage</code>
Single glossary term	<code>help term</code>
Glossary of all terms used for a topic	<code>help topic-name glossary</code>

For example, enter the following command to view help topics:

```
ob> help topics
```

Online help is available for the topics listed in [Table 1-5](#) (page 1-7).

Table 1-5 Command Topics for Oracle Secure Backup

Topic	Description
advanced	Advanced and seldom-used commands
backups	Data backup operations
backupwindow	Backup window definition
browser	File-system browser
checkpoint	Checkpoint management

Table 1-5 (Cont.) Command Topics for Oracle Secure Backup

Topic	Description
class	User class rights
daemon	Daemon (service) display and control
dataset	Dataset descriptions
device	Device configuration
duplication	Volume duplication operations
fs	File-system operations for Network Attached Storage (NAS) devices
host	Host configuration
images	Backup image and backup image instance management
invocation	obtool invocation options
job	Scheduler job management
library	Tape library and volume management operations
location	Location configuration
mediafamily	Media family configuration
miscellany	Miscellaneous commands
piece	Backup piece display
policy	Defaults and policies configuration
ssel	Database backup storage selector
reports	Media management reports
restores	Data restore operations
rotation	Rotation policy configuration
schedule	Schedule configuration
section	Backup section database commands
snapshot	Snapshot management for Network Attached Storage (NAS) devices
staging	Staging of disk backup image instances
summary	Summary report scheduling configuration
user	User configuration
variables	Variables that affect obtool operations

1.2.1 obtool Topics

For a list of commands on a particular topic, enter `help` followed by the topic name. For example, run the following command to display help about the `class` commands:

```
ob> help class
```

The command displays the following output:

```
Class definition commands:
chclass      change the attributes of a user class
lsclass     list the names and attributes of one or more user classes
mkclass     define a user class
```

```
renclass          assign a new name to a user class
rmclass          remove a user class from the administrative domain
```

1.2.2 obtool Command Syntax

For the syntax of a particular command, enter `help` followed by the command name. For example, enter the following command to display help for the [lssection](#) (page 2-170) command:

```
ob> help lssection
```

The command displays the following output:

```
Usage: lssection [ --long | --short ] [ --noheader/-H ] [ --incomplete/-i ]
               [ --oid/-o oid-list ]...
               [ { --vid/-v vid-list } | { --void/-V oid-list } }
               [ --file/-f filename-list ]...
```

You can also display help for placeholders in the syntax. For example, you can display the help for the `vid-list` placeholder as follows:

```
ob> help vid-list
```

The command displays the following output:

```
vid-list          one or more volume IDs (vids), each separated by a comma
```

1.2.3 obtool Glossary

For a glossary of terms for a topic, enter the keyword `help`, the topic name, and then the keyword `glossary`. For example, the following command displays the keyword glossary for the [snapshot](#) commands:

```
ob> help snapshot glossary
```

The command displays the following output:

```
<filesystem-name>  the logical or physical name of a file system that is
                   logically connected to a host
<hostname>        a name of a host assigned by the user via mkhost or renhost
<numberformat>    the format in which to display large numbers, one of:
                   friendly    displays large values in "KB", "MB", ...
                   precise     shows precise values (with commas)
                   plain       like precise, but eschews commas
                   (unspecified) uses "numberformat" variable or, if
                   unset, "friendly"
```

The remaining sections describe the obtool commands.

1.3 obtool Command Categories

obtool Commands: [addbw to lsvol](#) (page 2-1) organizes obtool commands alphabetically. This section categorizes commands into the following categories:

- [Backup Commands](#) (page 1-10)
- [Backup Image Commands](#) (page 1-11)
- [Backup Image Instance Management](#) (page 1-11)

- [Backup Piece Commands](#) (page 1-11)
- [Backup Window Commands](#) (page 1-11)
- [Browser Commands](#) (page 1-12)
- [Checkpoint Commands](#) (page 1-12)
- [Class Commands](#) (page 1-13)
- [Daemon Commands](#) (page 1-13)
- [Database Backup Storage Selector Commands](#) (page 1-14)
- [Dataset Commands](#) (page 1-14)
- [Device Commands](#) (page 1-15)
- [Duplication on Demand Commands](#) (page 1-15)
- [Duplication Window Commands](#) (page 1-15)
- [File-System Command](#) (page 1-16)
- [Host Commands](#) (page 1-16)
- [Job Commands](#) (page 1-16)
- [Library Commands](#) (page 1-16)
- [Location Commands](#) (page 1-17)
- [Media Family Commands](#) (page 1-17)
- [Miscellaneous Commands](#) (page 1-18)
- [Policy Commands](#) (page 1-18)
- [Preferred Network Interface Commands](#) (page 1-19)
- [Reports Commands](#) (page 1-19)
- [Restore Commands](#) (page 1-19)
- [Rotation Policy Commands](#) (page 1-20)
- [Schedule Commands](#) (page 1-20)
- [Section Commands](#) (page 1-20)
- [Snapshot Commands](#) (page 1-21)
- [Staging Commands](#) (page 1-21)
- [Summary Commands](#) (page 1-21)
- [User Commands](#) (page 1-22)
- [Volume Rotation Commands](#) (page 1-22)
- [Volume Duplication Commands](#) (page 1-22)

1.3.1 Backup Commands

Commands in this category enable you to create, display, and delete a file-system backup request.

The obtool utility includes the following commands for [file-system backup](#):

- [backup](#) (page 2-4)

- [lsbackup](#) (page 2-117)
- [rmbbackup](#) (page 3-108)

1.3.2 Backup Image Commands

Commands in this category enable you to list and manage backup images.

The obtool utility includes the following commands for backup images:

- [lsbkup](#) (page 2-119)
- [renbkup](#) (page 3-81)

1.3.3 Backup Image Instance Management

Commands in this category enable you to create, display, remove, and move backup image instances. A backup image instance is a complete representation of a backup image that exists on a storage location.

The obtool utility includes the following commands for managing backup image instances:

- [lsinstance](#) (page 2-146)
- [chinstance](#) (page 2-47)
- [cpinstance](#) (page 2-80)
- [rminstance](#) (page 3-118)

1.3.4 Backup Piece Commands

Commands in this category enable you to list and remove [Recovery Manager \(RMAN\)](#) backup pieces. A [backup piece](#) is a physical file in an Oracle proprietary format. An RMAN backup piece is created on tape as a [backup image](#).

These commands enable advanced users to correct any synchronization errors between RMAN backups and Oracle Secure Backup backups. The obtool utility includes the following backup piece commands:

- [lspiece](#) (page 2-160)
- [rmpiece](#) (page 3-123)

1.3.5 Backup Window Commands

Commands in this category enables you to configure backup windows. A [backup window](#) defines the times during which a [scheduled backup](#) runs. You can identify a single backup window that applies to all days of the week (a default backup window), or fine-tune backup windows based on specific days or dates.

 **Note:**

If no backup windows are identified, then scheduled backups do not run. The default backup window is daily 00:00-24:00.

The obtool utility includes the following backup window commands:

- [addbw](#) (page 2-1)
- [chkbw](#) (page 2-48)
- [lsbw](#) (page 2-125)
- [rmbw](#) (page 3-110)
- [setbw](#) (page 3-140)

1.3.6 Browser Commands

Commands in this category enable you to browse the Oracle Secure Backup [catalog](#). Each time Oracle Secure Backup performs a scheduled or [on-demand backup](#), it records the name and attributes of each file-system object it backs up. It writes this data to a repository — an Oracle Secure Backup catalog — stored on the [administrative server](#) file system. Oracle Secure Backup maintains a discrete backup catalog for each [client](#) in your [administrative domain](#).

When you browse a backup catalog, Oracle Secure Backup presents the data in the form of a file-system tree as it appeared on the [client](#) from which the data was saved. For example, if you backed up the `/home/myfile.f` file located on myhost, then the backup catalog for myhost represents the contents of the [backup image](#) as `/home/myfile.f`.

At the root of the backup catalog file system appears the [super-directory](#), which contains all files and directories saved from the top-most file-system level. The super-directory provides you with a starting point from which to access every top-level file-system object stored in the backup catalog.

The obtool utility includes the following browser commands:

- [cd](#) (page 2-25)
- [find](#) (page 2-97)
- [ls](#) (page 2-114)
- [lsbu](#) (page 2-122)
- [pwd](#) (page 3-76)

1.3.7 Checkpoint Commands

Commands in this category enable you to list and remove checkpoints. Checkpoints are position markers created periodically during restartable [Network Attached Storage \(NAS\)](#) backups to provide a location on the tape to which an interrupted backup can return and resume.

A backup is restartable if it meets the following conditions:

- The backup [client](#) is a Network Appliance [filer](#) running Data ONTAP 6.4 or later.
- The [backup image](#) is saved to a [tape drive](#) controlled by an [Network Data Management Protocol \(NDMP\)](#) server version 3 or later.
- The [restartablebackups](#) (page 7-36) operations policy is enabled.
- The backup has reached a point from which it can be restarted.

At the beginning of each [backup job](#), Oracle Secure Backup automatically determines whether the backup can be restarted from a mid-point. If it can be restarted, then Oracle Secure Backup periodically establishes a checkpoint that it can later use to restart the backup. When each additional checkpoint is recorded, the previous checkpoint is discarded. You can control checkpoint behavior with the [fullbackupcheckpointfrequency](#) (page 7-34), [incrbackupcheckpointfrequency](#) (page 7-34), and [maxcheckpointrestarts](#) (page 7-36) operations policies.

 **Note:**

If you use the restartable backups feature, then ensure that the `/tmp` directory on the [administrative server](#) is on a partition that maintains at least 1 GB of free space.

The obtool utility includes the following checkpoint commands:

- [lscheckpoint](#) (page 2-126)
- [rmcheckpoint](#) (page 3-110)

1.3.8 Class Commands

Commands in this category enable you to configure classes. A [class](#) defines a set of [rights](#) that are granted to an [Oracle Secure Backup user](#). You can assign multiple users to a class, each of whom is a member of exactly one class. A class is similar to a UNIX group, but it defines a finer granularity of access rights tailored to the needs of Oracle Secure Backup.

Oracle Secure Backup automatically predefines several classes, which are described in [Classes and Rights](#) (page 8-1). You can perform the same operations on these classes as on user-defined classes.

The obtool utility includes the following class commands:

- [chclass](#) (page 2-28)
- [lsclass](#) (page 2-128)
- [mkclass](#) (page 3-2)
- [renclass](#) (page 3-83)
- [rmclass](#) (page 3-111)

1.3.9 Daemon Commands

Commands in this category enable you to configure Oracle Secure Backup [daemons](#). A daemon is a process or service that runs in the background and performs a specified operation at predefined times or in response to certain events.

The obtool utility includes the following daemon commands:

- [ctldaemon](#) (page 2-83)
- [lsdaemon](#) (page 2-131)

1.3.10 Database Backup Storage Selector Commands

Commands in this category enable you to manage Oracle configuration data.

Oracle configuration data is stored in a [database backup storage selector](#). Storage selectors are created, named, and modified by an [Oracle Secure Backup user](#) belonging to a [class](#) with the modify configuration right. As with other configuration objects such as hosts, tape devices, and users, storage selectors are stored on the [administrative server](#).

Storage selectors give Oracle Secure Backup users fine-grained control over database backup operations. Oracle Secure Backup uses the information encapsulated in storage selectors when interacting with [Recovery Manager \(RMAN\)](#). As explained in [RMAN Media Management Parameters](#) (page C-1), you can override storage selectors by specifying media management parameters in RMAN.

The obtool utility includes the following Oracle configuration commands:

- [chssel](#) (page 2-65)
- [lsssel](#) (page 2-175)
- [mkssel](#) (page 3-54)
- [renssel](#) (page 3-93)
- [rmssel](#) (page 3-132)

1.3.11 Dataset Commands

Commands in this category enable you to create and configure an Oracle Secure Backup [dataset](#). A [dataset file](#) is an editable file that describes which hosts and paths that Oracle Secure Backup should back up.

Oracle Secure Backup stores and manages dataset files on the [administrative server](#) file system. Like Windows and UNIX file systems, Oracle Secure Backup datasets are organized in a naming tree. You can optionally create dataset directories to help you organize your data definitions. You can nest directories 10 levels deep.

The [samples](#) subdirectory of the [Oracle Secure Backup home](#) contains sample dataset files. Before you begin to define datasets, you can view these dataset files to get an idea of how to define a strategy for constructing your own.

For more details about datasets, see *Oracle Secure Backup Administrator's Guide*.

The obtool utility includes the following dataset commands:

- [catds](#) (page 2-19)
- [cdds](#) (page 2-26)
- [chkds](#) (page 2-49)
- [edds](#) (page 2-92)
- [lsds](#) (page 2-139)
- [mkds](#) (page 3-21)
- [pwdds](#) (page 3-77)
- [rends](#) (page 3-85)

- [rmds](#) (page 3-114)

1.3.12 Device Commands

Commands in this category enable you to configure a [tape device](#) for use with Oracle Secure Backup. A tape device is a [tape drive](#) or [tape library](#) identified by a user-defined device name.

The obtool utility includes the following device commands:

- [borrowdev](#) (page 2-12)
- [chdev](#) (page 2-30)
- [discoverdev](#) (page 2-85)
- [dumpdev](#) (page 2-88)
- [lsdev](#) (page 2-133)
- [managedev](#) (page 3-1)
- [mkdev](#) (page 3-6)
- [mountdev](#) (page 3-69)
- [pingdev](#) (page 3-73)
- [rendev](#) (page 3-84)
- [resdev](#) (page 3-96)
- [returndev](#) (page 3-105)
- [rmdev](#) (page 3-112)
- [unmountdev](#) (page 3-149)
- [unresdev](#) (page 3-150)
- [vfylibs](#) (page 3-156)

1.3.13 Duplication on Demand Commands

Commands in this category enable you to duplicate volumes on demand.

The obtool utility includes the following duplication on demand commands:

- [dupvol](#) (page 2-90)

1.3.14 Duplication Window Commands

Commands in this category enable you to manage duplication windows, which are time and day ranges.

The obtool utility includes the following duplication window commands:

- [adddw](#) (page 2-2)
- [chkdw](#) (page 2-50)
- [lsdw](#) (page 2-141)
- [rmdw](#) (page 3-116)

- [setdw](#) (page 3-141)

1.3.15 File-System Command

The [lsfs](#) (page 2-141) command enables you to list file systems on a [Network Attached Storage \(NAS\)](#) device accessed through [Network Data Management Protocol \(NDMP\)](#).

1.3.16 Host Commands

Commands in this category enable you to configure one or more hosts. A host is a computer that is accessible through [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#) in the Oracle Secure Backup [administrative server](#) network; a host is identified by a host name paired with an IP address.

The obtool utility includes the following host commands:

- [chhost](#) (page 2-43)
- [lshost](#) (page 2-143)
- [mkhost](#) (page 3-26)
- [pinghost](#) (page 3-75)
- [renhost](#) (page 3-87)
- [revhost](#) (page 3-108)
- [rmhost](#) (page 3-117)
- [updatehost](#) (page 3-153)

1.3.17 Job Commands

Commands in this category enable you to manage jobs, which are backup or restore operations that you have defined with the [backup](#) (page 2-4) or [restore](#) (page 3-99) commands.

The obtool utility includes the following job commands:

- [canceljob](#) (page 2-14)
- [catxcr](#) (page 2-22)
- [lsjob](#) (page 2-149)
- [rmjob](#) (page 3-119)
- [rpyjob](#) (page 3-137)
- [runjob](#) (page 3-138)

1.3.18 Library Commands

Commands in this category enable you to manage the contents of a [tape library](#). A tape library is a medium changer that accepts [Small Computer System Interface \(SCSI\)](#) commands to move media between a [storage location](#) and a [tape drive](#).

Most tape library commands accept either the `--library/-L` or `--drive/-D` option, depending on the operation requested. These options interact in the following ways:

- If a command requires a tape library, then you can specify either a tape library or a tape drive because the identity of a tape drive uniquely identifies a tape library.
- If a command requires a tape drive, then you must specify a tape drive because a tape library name is sometimes insufficient to uniquely identify a tape drive.

If you specify neither a tape library nor a tape drive, then obtool uses the tape library and tape drive variables (see [obtool Variables](#) (page 5-1)).

The obtool utility includes the following tape library commands:

- [catalog](#) (page 2-15)
- [clean](#) (page 2-79)
- [closeddoor](#) (page 2-80)
- [exportvol](#) (page 2-94)
- [extractvol](#) (page 2-96)
- [identifyvol](#) (page 2-100)
- [importvol](#) (page 2-102)
- [insertvol](#) (page 2-105)
- [inventory](#) (page 2-108)
- [labelvol](#) (page 2-110)
- [loadvol](#) (page 2-112)
- [lsvol](#) (page 2-182)
- [movevol](#) (page 3-71)
- [opendoor](#) (page 3-72)
- [reusevol](#) (page 3-106)
- [unlabelvol](#) (page 3-146)
- [unloadvol](#) (page 3-148)

1.3.19 Location Commands

Commands in this category enable you to manage locations.

The obtool utility includes the following location commands:

- [chloc](#) (page 2-50)
- [lsloc](#) (page 2-155)
- [mkloc](#) (page 3-34)
- [renloc](#) (page 3-88)
- [rmloc](#) (page 3-120)

1.3.20 Media Family Commands

Commands in this category enable you to configure media families. A [media family](#) is a named classification of backup volumes that share the following characteristics:

- [volume ID](#) sequence

- Expiration policy
- Write-allowed time period, which is called the [volume write window](#)

Write windows and expiration policies give you control over tape recycling. The default for both settings is to allow tapes to be written to indefinitely and kept forever. Setting limits enables you to [overwrite](#) tapes automatically at predetermined intervals.

Oracle Secure Backup is installed with a default content-managed media family named `RMAN-DEFAULT`. If no media family specified in a [Recovery Manager \(RMAN\)](#) job and if no matching backup storage selector exists, then RMAN uses `RMAN-DEFAULT`. You cannot delete or rename this default media family, although you can change specified attributes with `chmf`.

The obtool utility includes the following media family commands:

- [chmf](#) (page 2-52)
- [lsmf](#) (page 2-156)
- [mkmf](#) (page 3-36)
- [renmf](#) (page 3-88)
- [rmmf](#) (page 3-121)

1.3.21 Miscellaneous Commands

The obtool utility includes the following miscellaneous commands:

- [exit](#) (page 2-93)
- [id](#) (page 2-100)
- [logout](#) (page 2-113)
- [set](#) (page 3-140)
- [unset](#) (page 3-153)
- [show](#) (page 3-144)
- [quit](#) (page 3-79)

1.3.22 Policy Commands

Commands in this category enable you to create and manage policies. Oracle Secure Backup [defaults and policies](#) are configuration data that control how Oracle Secure Backup operates within an [administrative domain](#). You can use policies to tailor many characteristics of Oracle Secure Backup. [Defaults and Policies](#) (page 7-1) contains a complete list of policies and policy classes.

Policies are grouped into policy classes. Each class contains policies that describe a particular area of Oracle Secure Backup operation. Use the [lsp](#) (page 2-157) command display a list of classes and policies.

The obtool utility includes the following policy commands:

- [addp](#) (page 2-3)
- [cdp](#) (page 2-27)
- [lsp](#) (page 2-157)

- [pwdp](#) (page 3-77)
- [resetp](#) (page 3-97)
- [rmp](#) (page 3-122)
- [setp](#) (page 3-142)

1.3.23 Preferred Network Interface Commands

Commands in this category enable you to configure a [PNI \(Preferred Network Interface\)](#). A network can have multiple physical connections between a client and the server performing an operation on behalf of the client. For example, a pair of hosts can maintain both Ethernet and [Fiber Distributed Data Interface \(FDDI\)](#) connections. The PNI commands enable you to specify which of the server's network interfaces should transmit data for each client.

Network load balancing ensures optimal utilization of network interfaces by distributing the data transfer load across all available network interfaces. When a PNI is configured, then load balancing is disabled and PNI takes precedence.

See Also:

Oracle Secure Backup Installation and Configuration Guide for more information about network load balancing

The obtool utility includes the following PNI commands:

- [chpni](#) (page 2-54)
- [lspni](#) (page 2-162)
- [mkpni](#) (page 3-40)
- [rmpni](#) (page 3-124)

1.3.24 Reports Commands

Commands in this category enable you to display and list media management reports.

The obtool utility includes the following reports commands:

- [catrpt](#) (page 2-20)
- [lsrpt](#) (page 2-166)

1.3.25 Restore Commands

Commands in this category enable you to manage restore jobs.

The obtool utility includes the following restore commands:

- [lsrestore](#) (page 2-164)
- [restore](#) (page 3-99)
- [rmrestore](#) (page 3-127)

1.3.26 Rotation Policy Commands

Commands in this category enable you to manage rotation policies

The obtool utility includes the following [rotation policy](#) commands:

- [chrot](#) (page 2-56)
- [lsrot](#) (page 2-166)
- [mkrot](#) (page 3-42)
- [renrot](#) (page 3-89)
- [rmrot](#) (page 3-127)

1.3.27 Schedule Commands

Commands in this category enable you to configure a [backup schedule](#) to tell Oracle Secure Backup when to back up file-system data. In the backup schedule you describe the following:

- Triggers that indicate when the backups should occur. You can specify the days of the week, month, quarter, or year on which you want the backup to occur and the time in each day that a backup should begin.
- Name of each [dataset file](#) describing the data to back up. Oracle Secure Backup uses the host and path names, exclusion rules, and other information from each dataset file.
- Name of a [media family](#) to use. Oracle Secure Backup uses media families to assign selected characteristics to the backup.

The obtool utility includes the following schedule commands:

- [chsched](#) (page 2-58)
- [lssched](#) (page 2-167)
- [mksched](#) (page 3-44)
- [rensched](#) (page 3-90)
- [rmsched](#) (page 3-128)

1.3.28 Section Commands

Commands in this category enable you to manage backup sections. When Oracle Secure Backup performs a backup (either file-system or database), it creates a [backup image](#) on one or more tapes. A [backup section](#) is the portion of a backup image instance that occupies one physical [volume](#). A backup image instance that fits on a single volume consists of one backup section.

The obtool utility includes the following schedule commands:

- [lssection](#) (page 2-170)
- [rmsection](#) (page 3-129)
- [unrmsection](#) (page 3-151)

1.3.29 Snapshot Commands

Commands in this category enable you to manage snapshots. A [snapshot](#) is a consistent copy of a volume or a file system. Snapshots are supported only for a Network Appliance [filer](#) running Data ONTAP 6.4 or later.

The obtool utility includes the following snapshot commands:

- [lssnap](#) (page 2-173)
- [mksnap](#) (page 3-53)
- [rensnap](#) (page 3-91)
- [rmsnap](#) (page 3-130)

1.3.30 Staging Commands

The staging commands allow you to create stage rules that control which backup images are copied, and when they are copied. Stage rules can also be used to control the minimum time a backup image is guaranteed to remain on a stage device.

The obtool utility includes the following staging commands:

- [chstage](#) (page 2-69)
- [lsstage](#) (page 2-177)
- [mkstage](#) (page 3-57)
- [renstage](#) (page 3-94)
- [rmstage](#) (page 3-133)

1.3.31 Summary Commands

Commands in this category enable you to configure job summaries. A [job summary](#) is a generated text file report that indicates whether backup and restore operations were successful. A [job summary schedule](#) is the user-defined schedule according to which Oracle Secure Backup generates job summaries.

Oracle Secure Backup can generate and email job summaries detailing the status of backup and restore jobs. You can configure Oracle Secure Backup to generate one or more of these summaries. For each summary, you can choose the following:

- The schedule according to which Oracle Secure Backup produces the summary
- The start of the time period the summary spans (the end time is always the summary generation time)
- The [Oracle Secure Backup user](#) to whom the summary is emailed

Each job summary contains the following sections:

- Pending jobs
- Ready and running jobs
- Successful jobs
- Unsuccessful jobs

The obtool utility includes the following job summary commands:

- [chsum](#) (page 2-70)
- [lssum](#) (page 2-178)
- [mksum](#) (page 3-61)
- [rensum](#) (page 3-94)
- [rmsum](#) (page 3-133)

1.3.32 User Commands

Commands in this category enable you to configure [Oracle Secure Backup user](#) accounts for logging into and using Oracle Secure Backup. To configure Oracle Secure Backup users, you must be belong to a [class](#) with the [modify administrative domain's configuration](#) (page 8-4) right.

The obtool utility includes the following user commands:

- [chuser](#) (page 2-72)
- [lsuser](#) (page 2-180)
- [mkuser](#) (page 3-64)
- [renuser](#) (page 3-95)
- [rmuser](#) (page 3-134)

1.3.33 Volume Rotation Commands

Commands in this category enable you to control [volume](#) rotation as part of media lifecycle management.

The obtool utility includes the following volume rotation commands:

- [chvol](#) (page 2-75)
- [recallvol](#) (page 3-79)
- [releasevol](#) (page 3-80)
- [rmvol](#) (page 3-135)
- [vault](#) (page 3-155)

1.3.34 Volume Duplication Commands

Commands in this category enable you to control [volume](#) duplication as part of media lifecycle management.

The obtool utility includes the following volume duplication commands:

- [chdup](#) (page 2-41)
- [lsdup](#) (page 2-140)
- [mkdup](#) (page 3-24)
- [rendup](#) (page 3-86)
- [rmdup](#) (page 3-115)

1.4 obtool Lexical Conventions

This section describes the conventions used in the obtool command syntax diagrams and code examples of this manual. It describes:

- [Conventions in Syntax Diagrams](#) (page 1-23)
- [Conventions in Code Examples](#) (page 1-24)

1.4.1 Conventions in Syntax Diagrams

Syntax diagrams indicate legal syntax for Oracle Secure Backup commands. Syntax diagrams are displayed in a monospace (fixed-width) font and are preceded with a heading as shown in the following example:

clean::=

```
clean [ --drive/-D drivename ] [ --force/-f ] [ --use/-u element-spec ]
```

The following table describes typographic conventions used in syntax diagrams.

Convention	Meaning	Example
[]	Brackets enclose optional items from which you can choose one or none. A space is included after a beginning bracket and before a closing bracket for improved readability. Note that a comma-delimited list of tokens following a command option cannot be separated by spaces unless the entire string is enclosed within quotes.	<code>cancel•job [--quiet/-q --verbose/-v] [--tag/-t <i>tag[,tag]...</i>]</code>
{ }	Braces are required items for which you must select one of the enclosed values. Each value is separated by a vertical bar (). A space is included after a beginning brace and before a closing brace for improved readability. Note that a comma-delimited list of tokens following a command option cannot be separated by spaces unless the entire string is enclosed within quotes.	<code>disc•overdev { --host/-h <i>hostname</i> }... { * <i>dbname[,dbname]...</i> }</code>
	A vertical bar represents a choice of two or more options within brackets or braces. Enter exactly one of the options.	<code>ls [--long/-l --short/-s]</code>
--text/-text	A slash separating two flags, each preceded by one or two dashes, indicates an either-or choice between semantically equivalent options. For example, --in/-i represents a choice between the --in and -i flags.	<code>[--level/-l <i>backup-level</i>]</code>
...	Horizontal ellipsis points indicate that the preceding syntax item can be repeated. Note that spaces are not permitted between comma-delimited items.	<code>sho•w [<i>variable-name</i>]...</code>

Convention	Meaning	Example
.	A bullet within command syntax indicates that the characters between the bullet and the terminating whitespace can be omitted for convenience.	inv•entory
<i>Italics</i>	Italicized text indicates placeholders or variables for which you must supply particular values.	chkds <i>dataset-file-name</i> ...

1.4.2 Conventions in Code Examples

Code examples illustrate Oracle Secure Backup command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
ob> backup --dataset homedir.ds --go
```

The following table describes typographic conventions used in examples.

Convention	Meaning	Example
courier	Courier typeface indicates command line entries, system output display, options and arguments that you enter, executables, filenames, and directory names.	ob> cdds /mydatasets
Bold	Bold typeface distinguishes user input from command output in examples in cases where the two could be confused.	ob> mkds --nq --input mydataset.ds Input the new dataset contents. Terminate with an EOF or a line containing just a dot ("."). include host brhost2 include path /home .
.	Vertical ellipsis points in an example mean that information not directly related to the example has been omitted.	ob> lsvol --library lib1 Inventory of library lib1: . . . in dte: vacant

1.5 obtool Exit Codes

When obtool encounters an error, it reports an exit code with a brief description. The exit code file `obexit.h` is in `/usr/local/oracle/backup/samples`. It lists and describes all obtool exit codes. You might find it useful to anticipate errors and branch accordingly when building obtool scripts.

2

obtool Commands: addbw to lsvol

This chapter describes the [obtool](#) commands in alphabetical order. "[obtool Command Categories](#) (page 1-9)" organizes the obtool commands into various categories.

2.1.1 addbw

Purpose

Use the `addbw` command to add a [backup window](#), which is a time and day range, to an existing list of backup windows.



See Also:

"[Backup Window Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `addbw` command.

Syntax

```
addbw::=
```

```
addbw { --times/-t time-range[,time-range]... }  
day-specifier[,day-specifier]...
```

Semantics

--times/-t *time-range*

Defines a time-of-day range. Refer to "[time-range](#) (page 4-29)" for a description of the *time-range* placeholder.

day-specifier

Defines the day ranges for the backup window. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example

Example 2-1 Adding Backup Windows

This example creates backup windows so that backups can run from 8 a.m. to 8 p.m. on weekends and any time other than 8 a.m. to 8 p.m. on weekdays.

```
ob> addbw --times 08:00-20:00 weekend  
ob> addbw --times 00:00-08:00 mon-fri  
ob> addbw --times 20:00-24:00 mon-fri  
ob> lsbw
```

```
weekend 08:00-24:00
weekday 00:00-08:00,20:00-24:00
```

2.1.2 addw

Purpose

Use the `addw` command to add a duplication window, which is a time and day range, to an existing list of duplication windows.



See Also:

"[Duplication Window Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `addw` command.

Syntax

```
addw::=
```

```
addw { --times/-t time-range[,time-range]... } day-specifier[,day-specifier]...
```

Semantics

--times/-t *time-range*

Defines a time-of-day range for the duplication window. Refer to "[time-range](#) (page 4-29)" for a description of the *time-range* placeholder.

day-specifier

Defines the day ranges for the duplication window. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example

Example 2-2 Adding Duplication Windows

This example shows that a daily duplication window exists, that runs between 10 a.m. to 8 p.m. The `addw` command creates two other duplication windows, one that extends the window on weekends to 9 p.m., and another that is created for a specific date and time.

```
ob> lsdw
daily 10:00-20:00
ob> addw -t 20:00:00-21:00:00 weekend
ob> lsdw
weekend 10:00-21:00
weekday 10:00-20:00
ob> addw -t 15:30-16:30:30 09/30
ob> lsdw
09/30 15:30-16:30:30
weekend 10:00-21:00
weekday 10:00-20:00
```

2.1.3 addp

Purpose

Use the `addp` command to add a variable name-value pair to a policy.

See Also:

- ["Policy Commands \(page 1-18\)"](#) for related commands
- [Defaults and Policies \(page 7-1\)](#) for a complete list of policies and policy classes

Prerequisites

You must have the [modify administrative domain's configuration \(page 8-4\)](#) right to use the `addp` command.

Syntax

`addp::=`

```
addp policy-name { member-name member-value }...
```

Semantics

policy-name

Specifies the name of a policy or a class of policies.

member-name

Specifies the user-assigned name of a policy, usually an environment variable name.

member-value

Specifies the user-assigned value of a policy, usually an environment variable value.

Example

Example 2-3 Enabling Verbose Output from the NDMP Data Service

This example uses the `addp` command to set the `VERBOSE` environment variable for the [backupev \(page 7-28\)](#) policy in the `ndmp` class.

```
ob> pwdp
/
ob> lsp ndmp
authenticationtype      negotiated                [default]
backupev                (none)                  [default]
backuptype              (host type specific)    [default]
password                (not set)               [default]
port                    10000                   [default]
protocolversion         (as proposed by server) [default]
restoreev               (none)                  [default]
username                root                    [default]
ob> addp ndmp/backupev VERBOSE y
```

```
ob> lsp ndmp/backupdev
backupdev VERBOSE y
```

2.1.4 backup

Purpose

Use the `backup` command to create a file-system [backup request](#). A [file-system backup](#) is distinct from a database backup, which is initiated by [Recovery Manager \(RMAN\)](#).

Backup requests are held locally in `obtool` until you run the `backup` command with the `--go` option. Oracle Secure Backup forwards the requests to the [scheduler](#), at which time the requests become jobs and are eligible to run.

A backup made with the `backup` command is called an [on-demand backup](#). On-demand backups run just once, either immediately or at a specified time in the future. In contrast, a [scheduled backup](#) runs according to a user-specified schedule, which you create with the [mksched](#) (page 3-44) command.

Each time Oracle Secure Backup performs a backup, it records the name and attributes of each file-system object that it backs up. It writes this data to the Oracle Secure Backup [catalog](#), which is stored on the [administrative server](#). Oracle Secure Backup maintains a discrete backup catalog for each [client](#) in the [administrative domain](#).

Whether backups are encrypted and whether the encryption algorithm and keys are used depends upon the current global backup policies described in [Backup Encryption Policies](#) (page 7-3), client backup policies set with the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands, and the value of the `--encryption` option, if specified.

Client side software encryption is automatically forced on when backup data is written to Oracle Cloud Infrastructure. Encryption is not forced on when Oracle Secure Backup catalog backup data is written to Oracle Cloud Infrastructure.

Whether backups are compressed and whether the compression option is used, depends upon the current global backup policies described in [Backup Compression Policies](#) (page 7-1), client backup policies set with the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands, and the value of the `--compression` option, if specified.

 **See Also:**

- ["Backup Commands \(page 1-10\)"](#) for commands relating to on-demand backups
- [Backup Image Commands \(page 1-11\)](#) for commands relating to backup images
- [Backup Image Instance Commands \(page 1-11\)](#) for commands relating to backup image instances
- ["Schedule Commands \(page 1-20\)"](#) for commands relating to scheduled backups
- ["Browser Commands \(page 1-12\)"](#) for commands that enable you to browse the contents of the backup catalog of any client
- ["Dataset Commands \(page 1-14\)"](#) to learn how to create and manage dataset files and directories
- ["Job Commands \(page 1-16\)"](#) to learn how to display and manage backup jobs
- ["Media Family Commands \(page 1-17\)"](#) to learn how to create and manage media families

Prerequisites

You must have the [perform file system backups as privileged user \(page 8-6\)](#) right if you specify the `--privileged` option. Otherwise, you must have the [perform file system backups as self \(page 8-6\)](#) right.

To use the `--user` option, you must have the following rights: Perform file system backups as privileged user, Modify any backup, regardless of its owner, and Modify any job, regardless of its owner.

Usage Notes

If a disk pool runs out of space when a backup operation is in progress, the pool manager daemon tries to free space by deleting expired backup image instances. If the space freed is also not sufficient, then the backup job is paused. The administrator may need to increase the size of the disk pool. The administrator can also choose to cancel the backup job while it is paused.

Syntax

`backup::=`

```
backup [--level/-l backup-level] [--priority/-p schedule-priority]
      [--at/-a date-time] [--family/-f media-family-name]
      [--restrict/-r restriction[,restriction]...]
      [--privileged/-g | --unprivileged/-G] [--storekey/-s]
      [--encryption/-e encryption] [--algorithm/-L enc-algorithm]
      [ {--passphrase/-P passphrase} | --querypassphrase/-Q ]
      [--disablehwencryption/-d] [--expires/-x duration]
      [--dataset/-D dataset-name...] [--disablestorecatalog/-C]
      [--name/-n name-format] [--quiet/-q] [--waitfor/-W duration]
      [--user/-u user-name]
```

```
[ --compression/-K {off | low | medium | basic | high} ]  
[--go]
```

Semantics

--level/-l *backup-level*

Identifies a [backup level](#). The default level is 0. Refer to "[backup-level](#) (page 4-4)" for a description of the *backup-level* placeholder.

--priority/-p *schedule-priority*

Assigns a schedule priority to a backup. The default priority is 100. Refer to "[schedule-priority](#) (page 4-26)" for a description of the *schedule-priority* placeholder.

--at/-a *date-time*

Specifies the date and optional time to perform the backup. By default the backup is eligible to run immediately. If you specify a future date, then the backup is eligible to run at the date and time specified rather than immediately. Refer to "[date-time](#) (page 4-9)" for a description of the *date-time* placeholder.

--family/-f *media-family-name*

Defines the [media family](#) to be used for the backup. If you do not specify a media family, then Oracle Secure Backup defaults to the `null` media family. In this case, the [volume](#) has no expiration time and its [write window](#) remains open forever. By default, `VOL` is used for the [volume ID](#) prefix, as in the volume ID `VOL000002`.

--restrict/-r *restriction*

Defines a [tape device](#), disk pool, host, tape device/host pair, or cloud storage device in the administrative domain that identifies one or more acceptable devices for the backup. Refer to "[restriction](#) (page 4-25)" for a description of the *restriction* placeholder.

In the absence of a device restriction, the backup runs on the first available tape device. You can specify the restriction as a device name (as assigned by [mkdev](#) (page 3-6) or [chdev](#) (page 2-30)) or as an [attachment](#).

If the backup target is a cloud storage device, then the device must be specified because Oracle Secure Backup never backs up to a cloud storage device by default.

--privileged/-g

Requests that the backup run in privileged mode.

On Linux and UNIX hosts, a [privileged backup](#) runs under the `root` operating system identity. For example, [Oracle Secure Backup user](#) `joeblogg` runs under operating system account `root`. On Windows systems, the backup runs under the same account as the Oracle Secure Backup service on the Windows client.

--unprivileged/-G

Requests that the backup run in unprivileged mode (default).

When you create an Oracle Secure Backup user with the [mkuser](#) (page 3-64) command, or modify a user with the [chuser](#) (page 2-72) command, you associate an operating system user with the Oracle Secure Backup user. When an Oracle Secure Backup user makes an [unprivileged backup](#) or restore of a host, the host is accessed with the operating system user identity associated with the Oracle Secure Backup user. For example, assume Linux user `jblogg` is associated with Oracle Secure Backup user `joeblogg`. If you log on to `obtool` as `joeblogg` and initiate an unprivileged backup of a Linux host, then the backup runs under operating system account `jblogg` and backs up only those files accessible to `jblogg`.

--encryption/-e {yes | no | forcedoff | transient}

Specifies whether to use encryption for this [backup job](#). Values are:

- `yes`
Use encryption for this backup job. The encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `no`
Do not use encryption for this backup job. This is the default.
Note that if the global backup policy or client backup policy is set to `required`, then those policies supersede this value and encryption is used. If encryption is used, then the encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `forcedoff`
Do not use encryption for this backup job, regardless of global or client backup policy.
- `transient`
Encrypt the backups created with this job using a transient passphrase (supplied with the `--passphrase` or `--querypassphrase` options to `backup`), and the encryption algorithm specified by the global encryption policy setting.
This option is intended for use when creating backup files for a restore operation at another location where the Oracle [wallet](#) is not available.

 **See Also:**

Oracle Secure Backup Administrator's Guide for more information on transient backups

--algorithm/-L

Specifies the encryption algorithm to use with this backup. Values include `AES128`, `AES192` and `AES256`. The default is `AES192`.

--passphrase/-p *string*

Specifies the transient passphrase for use with the `--encryption transient` option. Value specified is a user-supplied string, in quotes.

--querypassphrase/-Q

Specifies that the [operator](#) must be prompted for the transient passphrase for use with the `--encryption transient` option.

--storekey/-s

Specifies that the transient passphrase for this backup should be added to the appropriate key stores. The default behavior is that transient passphrases are not stored in any key store.

--disablehwencryption /-d

Disables hardware-based encryption. If encryption is specified, then Oracle Secure Backup uses software-based encryption even if the backup occurs on a tape drive capable of hardware-based encryption.

--disablestoredcatalog/-C

Specifies that the backup image instance created by this backup will not have an attached catalog. Use this option only for backups stored on tape volume.

--expires/-x *duration*

Deletes the backup job if it is not processed within the specified *duration* after the job first becomes eligible to run. If you specify the `--at` option, then the time period begins at the date and time specified by `--at`; if you do not specify the `--at` option, then the time period begins when you run the `backup` command.

Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

--quiet/-q

Does not display job ID or status information when a backup job is dispatched to the scheduler. Use this option with the `--go` option.

--name /-n *name-format*

Specifies the name assigned to the backup image created by this backup job. You can explicitly specify a name, specify one or more name format variables, or use a combination of name format variable and static values that you specify.

See "[name-format](#) (page 4-19)" for a description of the *name-format* placeholder.

Each backup image name must be unique within the Oracle Secure Backup catalog. If you do not specify a date in the name, then a six-digit date in the `-yyymmdd` format is automatically appended to the backup image name. If you do not include a time in the name, a six-digit time in the `-hhmmss` format is automatically appended to the backup image name. If you do not add a date or time in the name, then both values in the `-yyymmdd-hhmmss` format are automatically appended to the backup image name.

--waitfor/-W *duration*

Specifies the amount of time that Oracle Secure Backup waits for the backup job to complete. After the specified time duration is exceeded, Oracle Secure Backup exits from `obtool`.

See "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

--dataset/-D *dataset-name*

Identifies the [dataset file](#), which is a file that defines the data to be backed up, or the [dataset directory](#). If you specify the name of a dataset directory, then it is equivalent to naming all of the dataset files contained within the directory tree. The `--dataset` and `--go` options are not mutually exclusive.

By default, file-system backups initiated by `obtool` do not cross mount points.

However, you can use mount point statements in your dataset files to cross mount points.

 **See Also:**

- "[cross all mountpoints](#) (page 6-7)"
- "[cross local mountpoints](#) (page 6-8)"
- "[cross remote mountpoints](#) (page 6-9)"

Another way to cross remote mount points is to use the [setp](#) (page 3-142) command and set the `operations policy backupoptions` as described in [Example 3-101](#) (page 3-144).

--user/-u *username*

Specifies the name of the Oracle Secure Backup user who owns the created backup job.

--compression/-K {*off* | *low* | *medium* | *basic* | *high*}

Specifies a compression option for the on-demand backup job that overrides any global and client-level compression options already set.

The possible values are as follows:

off

Software compression is not used for the backup regardless of global and client level policy

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the `medium` option. It is slower than the `low` and `medium` options, but faster than the `high` option.

high

Compresses data as much as possible, making extensive use of CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

The default value is that no compression option is set.

If compression is not specified as part of the `backup` command, then the client host setting for compression is used. If the client host compression setting is not set, then the domain-level policy is used. If the domain-level policy is also not set, then no software compression is performed for this job.

 **Note:**

- There is no one best compression level. The best level to use depends on your specific environment and compression requirements, as well as network traffic characteristics (workload), backup speed, and the content of the data set being compressed.
- Oracle Secure Backup compression options are not applicable to database backups performed using RMAN.

For database backups, similar compression options can be specified as part of RMAN commands.

- Oracle Secure Backup compression options are not applicable to NDMP hosts (`--access ndmp`).
- If Oracle Secure Backup finds hardware capable of doing hardware compression, then it disables any software compression option that may be set, with appropriate warning messages as part of the job.

--go

Sends all backup requests that are queued in the request queue to the Oracle Secure Backup scheduler. Backup requests are held locally in `obtool` until you run `backup` with the `--go` option or exit `obtool`. If you exit `obtool` without specifying `--go`, then all queued backup requests are discarded. `obtool` warns you before deleting the requests.

If two users log in to `obtool` as the same Oracle Secure Backup user, and if one user creates backup requests (but not does not specify `--go`), then the other user does not see the requests when issuing `lsbackup` (page 2-117).

When backup requests are forwarded to the scheduler, the scheduler creates a job for each backup request and adds it to the [job list](#). At this time, the jobs are eligible for execution. If the `--at` option was specified for a job, then this job is not eligible for execution until the specified time arrives.

Oracle Secure Backup assigns each on-demand backup job an identifier consisting of the username of the logged in user, a slash, and a unique numeric identifier. An example of a job identifier for an on-demand backup is `sbt/233`.

Examples**Example 2-4 Making a Full Backup**

This example illustrates a privileged backup with a priority 10. The data to be backed up is defined by the `home.ds` file. Assume that this file contains the following entries, which specify that the `/home` directory on `brhost2` should be backed up:

```
include host brhost2
include path /home
```

The backup is scheduled to run at 10 p.m. on June 14.

```
ob> backup --level full --at 2013/06/14.22:00 --priority 10 --privileged
--dataset home.ds --go
Info: backup request 1 (dataset home.ds) submitted; job id is admin/6.
```

Example 2-5 Restricting Backups to Different Devices

This example creates two on-demand backup requests, one for dataset `datadir.ds` and the other for dataset `datadir2.ds`, and restricts each to a different tape drive. The

backup --go command forwards the requests to the scheduler. The `lsjob` (page 2-149) command displays information about the jobs.

```
ob> backup --level 0 --restrict tape1 --dataset datadir.ds
ob> backup --level 0 --restrict tape2 --dataset datadir2.ds
ob> backup --go
Info: backup request 1 (dataset datadir.ds) submitted; job id is admin/8.
Info: backup request 2 (dataset datadir2.ds) submitted; job id is admin/9.
ob> lsjob --long admin/8 admin/9
admin/8:
  Type:                dataset datadir.ds
  Level:               full
  Family:              (null)
  Scheduled time:      none
  State:               completed successfully at 2012/03/17.16:30
  Priority:             100
  Privileged op:      no
  Run on host:         (administrative server)
  Attempts:            1
admin/9:
  Type:                dataset datadir2.ds
  Level:               full
  Family:              (null)
  Scheduled time:      none
  State:               completed successfully at 2013/03/17.16:30
  Priority:             100
  Privileged op:      no
  Run on host:         (administrative server)
  Attempts:            1
```

Example 2-6 Backing Up to a Disk Pool

This example creates a file-system backup that is immediately forwarded to the scheduler. Because a priority was not specified, the default value of 100 is used. The data to be backed up is stored in the dataset `my_datasets/bk_fs_sun.ds`. The `--restrict` option indicates that the backup is restricted to use the disk pool `dp2` or `dp3`.

```
ob> backup --dataset my_datasets/bk_fs_sun.ds --restrict dp2,dp3 --go
Info: backup request 1 (dataset my_datasets/bk_fs_sun.ds) submitted; job id is
admin/7.

ob> lsjob --long admin/7
admin/7:
  Type:                dataset my_datasets/bk_fs_sun.ds
  Level:               full
  Family:              (null)
  Encryption:         off
  Scheduled time:      none
  State:               completed successfully at 2013/04/23.03:54
  Priority:             100
  Privileged op:      no
  Run on host:         (administrative server)
  Attempts:            1
```

Example 2-7 Backing Up to a Cloud Storage Device

```
ob> backup --dataset my_datasets/bk_fs_sun.ds -encryption on --restrict clodev --go
Info: backup request 1 (dataset tbrset/entire_backup) submitted; job id is admin/9.

ob> lsjob --long admin/9
admin/9:
```

```

Type:                dataset my_datasets/bk_fs_sun.ds
Level:              full
Backup name format: (system default)
Family:            (null)
Encryption:        on
Disable h/w encryption: no
Store catalog on media: yes
Scheduled time:    none
State:             completed successfully at 2017/10/31.11:36
Priority:          100
Privileged op:    no
Run on host:      (administrative server)
Attempts:         1
ob>

```

Example 2-8 Transferring Backup Ownership to Another User

This example creates an on-demand file-system backup and transfers the ownership to the Oracle Secure Backup user `bkup_usr1`. The data to be backed up is stored in the dataset `my_datasets/bk_fs_week`.

```

ob> backup -D my_datasets/bk_fs_week -u bkup_usr1 -go
Info: backup request 1 (dataset my_datasets/bk_fs_week) submitted; job id is
bkup_usr1/3.

```

2.1.5 borrowdev

Purpose

Use the `borrowdev` command to borrow a [tape drive](#).

You use the `borrowdev` command if a backup or restore job is requesting assistance. You can reply to the input request by using the [rpyjob](#) (page 3-137) command, but this technique can be cumbersome for multiple commands because `obtool` issues a prompt after each command. The `borrowdev` command temporarily overrides the [tape device](#) reservation made by the requesting job and enables you to run arbitrary [tape library](#) or [tape drive](#) commands. You can use the [returndev](#) (page 3-105) command to release the tape drive and use the [catxcr](#) (page 2-22) or [rpyjob](#) (page 3-137) commands to resume the job.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `borrowdev` command.

Syntax

```
borrowdev::=
```

```
borrowdev drive-name...
```

Semantics

drive-name

Specifies the name of the tape drive to borrow.

Examples

Example 2-9 Displaying the Transcript for a Hanging Backup

In this example, `backup job admin/6` is not proceeding. Running the `catxcr` (page 2-22) command reveals that Oracle Secure Backup cannot find a usable tape for the backup.

```
End of tape has been reached. Please wait while I rewind and unload the tape. The Volume ID of the
next tape to be written is VOL000007. The tape has been unloaded.
```

```
obtar: couldn't perform auto-swap - can't find usable volume in library (OB device mgr)
Enter a command from the following list:
load <n>      .. load the tape from element <n> into the drive
unload <n>    .. unload the tape from the drive into element <n>
help         .. display other commands to modify drive's database
go           .. to use the tape you selected
quit         .. to give up and abort this backup or restore
:
```

Example 2-10 Borrowing a Tape Drive

Assume that you press the Enter key to return to the `obtool` prompt. In this example, you insert a tape into slot 2 of the tape library, borrow the tape drive, load the `volume` from slot 2 into the tape drive, and then release the tape drive with the `returndev` (page 3-105) command.

```
ob> lsvol --long
Inventory of library lib1:
   in  mte:      vacant
   in  1:        volume VOL000006, barcode ADE201, oid 116, full
   in  2:        vacant
   in  3:        vacant
   in  4:        vacant
   in  dte:      vacant
ob> insertvol unlabeled 2
ob> borrowdev tapel
ob> loadvol 2
ob> returndev tapel
```

Example 2-11 Resuming a Job After Borrowing a Device

This example runs the `catxcr` (page 2-22) command for the job and then enters `go` at the prompt to resume the backup.

```
ob> catxcr admin/6.1
admin/6.1: 2013/04/11.18:36:44 _____
admin/6.1: 2013/04/11.18:36:44
admin/6.1: 2013/04/11.18:36:44      Transcript for job admin/6.1 running on brhost2
.
.
.
admin/6.1: Backup started on Mon Apr 11 2013 at 18:36:44
admin/6.1: Volume label:
admin/6.1: Enter a command from the following list:
```

```

admin/6.1:      load <n>      .. load the tape from element <n> into the drive
admin/6.1:      unload <n>     .. unload the tape from the drive into element <n>
admin/6.1:      help        .. display other commands to modify drive's database
admin/6.1:      go          .. to use the tape you selected
admin/6.1:      quit        .. to give up and abort this backup or restore
admin/6.1: :
admin/6.1: : go

```

2.1.6 canceljob

Purpose

Use the `canceljob` command to cancel a pending or running job. You can display these jobs by specifying the `--pending` or `--active` options on the [lsjob](#) (page 2-149) command.

Canceling a job terminates the job if it is running, then marks its job record as `canceled`. Oracle Secure Backup considers canceled jobs as no longer eligible to be run. If you cancel a job that has subordinates, then each of its subordinate jobs is also canceled.



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to cancel another user's jobs, then you must have the right to [modify any job, regardless of its owner](#) (page 8-5). If you are attempting to cancel your own jobs, then you must have the right to [modify any jobs owned by user](#) (page 8-5).

Syntax

```
canceljob::=
```

```
canceljob [ --quiet/-q | --verbose/-v ] job-id...
```

Semantics

--quiet/-q

Suppresses output.

--verbose/-v

Displays verbose output.

job-id

Specifies the job identifier of the job to be canceled. You can display job identifiers with the [lsjob](#) (page 2-149) command.

Example

Example 2-12 Cancelling a Backup Job

This example displays a pending job and then cancels it.

```
ob> lsjob --pending
Job ID          Sched time  Contents                               State
-----
sbt/8           03/21.18:00 dataset fullbackup.ds                 future work
ob> canceljob sbt/8
Info: canceled job sbt/8.
ob> lsjob --pending
ob>
```

2.1.7 catalog

Purpose

Imports stored backup catalog data from the specified backup container in the administrative domain into the backup catalog.

Use the `catalog` command in the following scenarios:

- During disaster recovery
If the Oracle Secure Backup catalog is damaged and no backup copy of the catalog is available, then you can use the `catalog` command to recreate the catalog.
- When a disk pool is replicated to a different storage system
You can import the backup image instances in the replicated copy into a backup catalog that belongs to a different administrative domain.
- Importing a volume set
You can import backup catalog data while importing a volume set in a new administrative domain.

Prerequisites

The volume set that is being cataloged must be a part of the Oracle Secure Backup volumes database. Use the `identifyvol` command or `importvol` command with the `--identity` option to include the volume set in the volumes database.

Usage Notes

When you run the `catalog` command, Oracle Secure Backup creates a catalog import job. Oracle Secure Backup scans the contents of the volume set, disk pool device, or cloud storage device and identifies the backup image instances that are not currently stored in the backup catalog. When the catalog import job is processed, the backup catalog is updated with the instances identified during the scan. If the catalog operation detects a backup image from a client that does not exist in the current administrative domain, it creates a dummy host with the same name and the UUID as that backup image. This host is solely maintains relevant logs and cannot be used for backup and restore operations.

When cataloging a disk pool or cloud storage device, use the `--device` option before specifying the name of the device. If you don't use this option, then the `catalog` command automatically assumes the backup container is a tape volume and displays an error.

After a catalog import job completes, use the `catxcr` command to display the transcript associated with this catalog import job.

Syntax

catalog::=

```
catalog
[--firstfullimage/-f] [--quiet/-q | --verbose/-V] [--forcecatimport/-F]
[--debug/-e...] [--fastcatalogonly/-Y] [--foreground/-g]
[--priority/-p schedule-priority] [--waitfor/-W duration]
{[--vid/-v vid] | [--barcode/-b tag] | [--void/-o void] |
[--backupsectionoid/-B oid]}
{[--device/-d devicename] | [--drive/-D drivename]}
```

Semantics

--firstfullimage/-f

Specifies that the catalog import job on tape will begin from the backup image instance that begins with the first backup section. All existing archive sections will be skipped and all subsequent backup image instances are imported.

--quiet/-q

Specifies that details of the import operation must not be displayed. Only a simplified version of the volume label and archive label is displayed.

--verbose/-V

Specifies that additional details about the catalog import operation such as backup catalog data, volume labels, and archive labels must be displayed. If this option is omitted, a simplified version of the volume labels and archive labels is displayed. If neither the `--quiet` nor the `--verbose` option is specified, then Oracle Secure Backup displays basic information about the catalog import job.

--forcecatimport/-F

Enables you to import backup catalog data, even if some volumes in a volume set are not present in the volumes database. Oracle Secure Backup imports catalog data from the existing volumes into the backup catalog.

This option is useful when one or more volumes in a volume set is missing. It also recatalogs existing backups in the backup catalog using information from the backup container.

However, if the catalog spans multiple tape volumes and any of these volumes containing catalog data is missing, the information will not be imported.

--debug/-e

Specifies that additional debugging information must be written to the log files. This information is useful in debugging errors that may be caused during the catalog import job. Specifying this option multiple times increases the amount of debug information written to the log files.

--fastcatalogonly/-Y

Specifies that only backup image instances that have the associated backup catalog data must be imported.

--foreground/-g

Specifies that the catalog operation will be performed directly, without creating a prior catalog import job. Use this option only for tape volumes.

--priority/-p *schedule-priority*

Specifies the priority associated with this catalog import job.

--waitfor/-W duration

Specifies the amount of time that Oracle Secure Backup waits for the catalog job to complete. After this specified duration is exceeded, Oracle Secure Backup either displays a new `obtool` command prompt or exits from `obtool` if the `catalog` command was invoked directly from a system command prompt.

See "duration (page 4-14)" for a description of the `duration` placeholder.

--vid/-v vid

Specifies the unique volume ID of the tape volume or volume set whose data must be imported into the backup catalog. Oracle Secure Backup imports catalog data starting with the first volume in the volume set. Typically, this involves loading a previous tape volume. If the `--firstfullimage` option is specified, then the cataloging process begins with the backup image instance that begins on this volume. Use the `lsvol` command to obtain the volume ID of tape volumes.

See "vid (page 4-30)" for a description of the `vid` placeholder.

--barcode/-b tag

Specifies the barcode of the tape volume whose data must be imported into the backup catalog. Use the `lsvol` command to obtain the barcode of volumes.

--void/-o void

Specifies the catalog identifier of the volume whose data must be imported into the backup catalog. Use the `lsvol` command to obtain the volume ID, `lsbu` command to display the backup ID, and `lspiece` command to display the piece OID for this volume.

--backupsectionoid/-B

Specifies the backup section ID of the backup section that must be imported into the backup catalog. Use the `lssection` command to determine the backup section ID (BSOID) of backup sections.

--device/-d devicename

Specifies the name of the disk pool whose catalog data must be imported into the backup catalog.

--drive/-D drivename

Specifies the name of the tape volume whose data is being imported into the backup catalog. If no drive is specified, any available tape drive may be used for the catalog operation.

Examples

The catalog command creates a catalog import job. When the catalog import job completes, you can use the `catxcr` command to display the transcript associated with this job.

In [Example 2-13](#) (page 2-17), the `lsvol` command lists the volumes in tape drive `vt1`. The `catalog` command then imports and catalogs the volume with the volume ID `VOL000001`. Cataloging this volume will begin from the backup image instance with the first available backup section.

The `catxcr` command displays the transcript of the catalog job with the job ID `admin/20`.

Example 2-13 Cataloging a Volume

```
ob> lsvol --drive vt1
Inventory of library vlib1:
  * in   1:                volume RMAN-DEFAULT-000001, barcode
8ebd80f28e4a1039fd900163e359724, 42134336 kb remaining, content manages reuse
```

```

    in   dte:          volume VOL000001, barcode 3066e1068e4a10395a300163e359724,
41805312 kb remaining, lastse 2
    *: in use list
ob> catalog -V --vid VOL000001 --firstfullimage --priority 100
Info: catalog import request 1 submitted; job id is admin/20.
ob> catxcr admin/20
2013/04/25.02:44:31

-----
2013/04/25.02:44:31
2013/04/25.02:44:31          Transcript for job admin/20 running on brhost1
2013/04/25.02:44:31
Volume label:
    Volume tag:          3066e1068e4a10395a300163e359724
    Volume UUID:         35af92b6-8e4a-1030-b7a1-00163e359724
    Volume ID:           VOL000001
    Volume sequence:     1
    Volume set owner:    root
    Volume set created:  Mon Apr 22 23:47:04 2013

Archive label:
    File number:         1
    File section:       1
    Owner:               root
    Client host:         brhost2
    Backup level:        0
    S/w compression:    no
    Archive created:     Mon Apr 22 23:47:04 2013
    Archive owner:       admin (UUID 2c29a0ce-8e4a-1030-aa47-00163e359724)
    Owner class:         admin (UUID 2c17868c-8e4a-1030-aa47-00163e359724)
    Encryption:         off
    Catalog data:        yes
    Backup image UUID:   35948336-8e4a-1030-b7a1-00163e359724
    Backup instance UUID: 3594834a-8e4a-1030-b7a1-00163e359724
.
.
.
Importing catalog by reading attached data.Reached end of volume set

```

Example 2-14 Cataloging a Disk Pool

This example catalogs the disk pool `dp1`.

```

ob> lsdev --long dp1
dp1:
    Device type:         disk pool
    In service:          yes
    Debug mode:          no
    Capacity:            (not set)
    Consumption:         0
    Free space goal:     (system default)
    Concurrent jobs:     (unlimited)
    Blocking factor:     (default)
    Max blocking factor: (default)
    UUID:                53860d36-2a27-1032-a210-00163e527899
    Attachment 1:
        Host:             brhost3
        Directory:        /net/slc02qdv/scratch/test/osb_ds/temp
ob> catalog --verbose --priority 100 --device dp1
Info: catalog import request 1 submitted; job id is admin/23

```

2.1.8 catds

Purpose

Use the `catds` command to list the contents of a [dataset file](#) created with the `mkds` (page 3-21) command.



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `catds` command.

Syntax

```
catds::=
```

```
catds dataset-file-name...
```

Semantics

dataset-file-name

Specifies the name of a dataset file. Refer to "[dataset-file-name](#) (page 4-7)" for a descriptions of the `dataset-file-name` placeholder.

Example

Example 2-15 Displaying the Contents of a Dataset

This example displays the contents of the dataset file named `basicsummary.ds`, which is a sample dataset file included with Oracle Secure Backup.

```
ob> catds basicsummary.ds
# SAMPLES/basicsummary, pfg, 03/01/02
# review of basic dataset statements

# This dataset ties together all of the features introduced
# this far. It describes the root file systems and a couple of
# specific directories on the /home file system of each host.
# For each directory tree, it excludes any file ending in
# ".a" and ".o".

include dataset admin/default_rules # get domain defaults from
                                     # this file

include host sporky                   # back up these 3 hosts,
include host sparky
include host spunky

include path /                         # saving these file systems and
include path /home/software           # directories on each host
include path /home/doc
```

```
include optional pathlist /pl.qr      # read additional names from
                                      # this pathlist file on each
                                      # named host, if it exists

exclude name *.a                      # but in each tree, don't save
                                      # files ending
exclude name *.o                      # in these suffixes
```

2.1.9 catrpt



See Also:

["Reports Commands \(page 1-19\)"](#) for related commands

Purpose

Use the `catrpt` command to display one or more reports related to media movement. You can use these reports to assist in managing the media life cycle.

In many cases, it is still necessary to rely upon printed reports to manage media as they are moved from one [location](#) to another. The `catrpt` command provides the following report types:

- Pick lists
A list of media that must be moved from its current location to its next location. Useful as a checklist when removing media from a [tape library](#) or standalone [tape drive](#).
- Distribution lists or packing lists
A list of media being moved from its current location to its next location. Useful as a printed list to include with media that are being shipped to another location. Also useful to send to an off-site storage vendor when media are scheduled for return from storage.
- Inventory lists
A list of media and its present location
- Exceptions
A list of media not in the correct location specified by its [rotation policy](#), such as lost volumes, volumes not stored in the correct tape library, and expired volumes still in rotation.

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `catrpt` command.

Syntax 1

Use the following syntax to display [volume](#) pick or distribution reports.

```
catrpt::=
```

```
catrpt --type/-t { pick | distribution } job-id...
```

Semantics 1

--type /-t

Specifies the report type, pick or distribution, to be displayed for the specified jobs.

job-id

The job ID of the media movement or volume duplication job.

Syntax 2

Use the following syntax to display a volume location report.

```
catrpt::=
```

```
catrpt --type/-t location [ --location/-L location_name ] [ --intransit/-I ]
```

Semantics 2

--type/-t location

Specifies the report type to be displayed for the specified location.

--location location_name

Specifies the location for which you want a location report.

--intransit/-I

Specifies that only volumes in transit from one location to another be listed. A volume is considered in transit from the time it is removed from a location as part of a media movement job until it is loaded into its next location and appears in an Oracle Secure Backup inventory of that location.

Syntax 3

Syntax 3

Use the following syntax to display an exception or missing report.

```
catrpt::=
```

```
catrpt --type/-t { exception | missing } [ --location/-L location_name ]
```

Semantics 3

--type/-t

Specifies the report type to be displayed for the specified location.

--location location_name

Specifies the location for which you want an exception or missing report.

Syntax 4

Use the following syntax to display a volume schedule report.

```
catrpt::=
```

```
catrpt  
{ --type/-t schedule } [ --from/-F from_date ] [ --to/-T to_date ]  
[ --location/-L location_name ]
```

Semantics 4

--type /-t schedule

Specifies the report type to be displayed for the specified location.

--from

Specifies the oldest schedule date to be displayed. If no `--to` option is specified, then Oracle Secure Backup displays all schedules from the `--from` date to the present.

--to

Specifies the most recent schedule date to be displayed. If no `--from` date is specified, then Oracle Secure Backup displays all schedules older than the `--to` date.

--location

Specifies the location for which you want a volume schedule report.

Example

Example 2-16 Listing Media Movement Reports

This example uses the `catrpt` command to display a pick list of the media movement job created in [Example 2-44](#) (page 2-78).

```
ob> catrpt --type pick 2
                Oracle Secure Backup Pick List Report
                Location - vlib1
```

Volume ID	Barcode	Move Date	Next Loc
VOL000001	e53b658a2d2710390a700163e527899	2013/11/12	lib1

2.1.10 catxcr

Purpose

Use the `catxcr` command to display one or more job transcripts. Oracle Secure Backup maintains a running transcript for each job. The transcript describes the details of the job's operation. Oracle Secure Backup creates this transcript when dispatching the job for the first time and updates it as the job progresses. When a job requires [operator](#) assistance, Oracle Secure Backup prompts for assistance by using the transcript.



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to list another user's jobs, then you must have the right to [list any job, regardless of its owner](#) (page 8-5). If you are attempting to list your own jobs, then you must have the right to [list any jobs owned by user](#) (page 8-5).

If you are attempting to respond to another user's jobs, then you must have the right to [modify any job, regardless of its owner](#) (page 8-5). If you are attempting to respond

to your own jobs, then you must have the right to [modify any jobs owned by user](#) (page 8-5).

Syntax

catxcr::=

```
catxcr [ --level/-l msglevel ] [ --noinput/-N ] [ --msgno/-m ]
[ --start/-s msgno | --head/-h nlines | --tail/-t nlines ]
[ --follow/-f ] job-id...
```

Semantics

--level /-l *msglevel*

Displays only lines with *msglevel* or higher message levels. You can specify *msglevel* either numerically or by name. The default level is 4 (request), which are the normal messages generated by Oracle Secure Backup. To request and view lower level messages, you must request that they be generated when the job is initiated, by using the `--debug` option of the [catalog](#) (page 2-15) command.

Each message that Oracle Secure Backup writes to a transcript is tagged with a message number and a message level. The message number indicates the position of the message in the transcript.

Note:

The message number may not correspond to the physical line number because a given message can span multiple physical lines.

The message level identifies the content of the message as being in an ordered category in [Table 2-1](#) (page 2-23).

Msg Number	Msg Name	Msg Description
0	debug2	debug (extra output) message
1	debug1	debug message
2	verbose	verbose mode output
3	info	informational message
4	request	message requested by user
5	summary	operational summary message
6	warning	warning message
7	error	error message (operation continues)
8	abort	error message (operational is canceled)
9	fatal	error message (program stops)

--noinput/-N

Suppresses input requests. By default, when a request for input is recognized, `catxcr` pauses and enables you to respond to the prompt. Specifying this option suppresses this action.

--msgno/-m

Prefixes each line with its message number.

--start/-S msgno

Starts displaying at the line whose message number is *msgno*.

--head/-h nlines

Displays the first *nlines* of the transcript. If `--level` is not specified, then `obtool` uses `--level 4` as a default, which means that *nlines* is a count of the default level (or higher). If `--level` is specified, then *nlines* is a count of lines of the specified level or higher.

--tail nlines

Displays the last *nlines* of the transcript. If `--level` is not specified, then `obtool` uses `--level 4` as a default, which means that *nlines* is a count of the default level (or higher). If `--level` is specified, then *nlines* is a count of lines of the specified level or higher.

--follow/-f

Monitors the transcript for growth continually and displays lines as they appear. By default, the `catxcr` command displays the requested number of lines and stops. You can exit from `--follow` mode by pressing Ctrl-C.

job-id

Specifies job identifiers of jobs whose transcripts are to be displayed. If a *job-id* refers to a job that has dependent jobs, then `obtool` displays transcripts of all dependent jobs. When `catxcr` displays multiple transcripts, it prefixes each line with its *job-id*. Run the `lsjob` (page 2-149) command to display job identifiers.

Examples**Example 2-17 Displaying a Job Transcript**

This example displays the transcript for a job whose ID is `sbt/1.1`.

```
ob> catxcr sbt/1.1
2013/03/21.10:19:39

2013/03/21.10:19:39
2013/03/21.10:19:39          Transcript for job sbt/1.1 running on osbsvr1
2013/03/21.10:19:39
Volume label:
  Volume tag:           ADE202
  Volume ID:            RMAN-DEFAULT-000001
  Volume sequence:     1
  Volume set owner:    root
  Volume set created:  Mon Mar 21 10:19:39 2013
  Media family:        RMAN-DEFAULT
  Volume set expires:  never; content manages reuse
```

Example 2-18 Displaying the Transcript for a Hanging Backup

In [Example 2-9](#) (page 2-13), `backup job admin/6` is not proceeding. In this example, running `catxcr` reveals that Oracle Secure Backup cannot find a usable tape for the backup. The most common cause of this problem is lack of eligible tapes in the [tape library](#).

You can respond to this situation by pressing the Enter key to return to the `obtool` prompt or opening an additional window. Use the `borrowdev` (page 2-12) command to gain control of the [tape drive](#). After making a tape available with the `unlabelvol` (page 3-146) or `insertvol` (page 2-105) command, complete the job by running `catxcr` and then `go`.

End of tape has been reached. Please wait while I rewind and unload the tape. The Volume ID of the next tape to be written is VOL000007. The tape has been unloaded.

```
obtar: couldn't perform auto-swap - can't find usable volume in library (OB device mgr)
Enter a command from the following list:
load <n>      .. load the tape from element <n> into the drive
unload <n>    .. unload the tape from the drive into element <n>
help         .. display other commands to modify drive's database
go           .. to use the tape you selected
quit        .. to give up and abort this backup or restore
:
```

Example 2-19 Displaying a Job Continuously

This example continually displays the transcript for job `sbt/1.1`. The example disables input requests and displays all message levels.

```
ob> catxcr --noinput --follow --level 0 sbt/1.1
```

Example 2-20 Displaying Warnings for a Job

This example displays all errors and warnings for jobs `admin/1.1` and `admin/2`.

```
ob> catxcr --level warning admin/1.1 admin/2
```

2.1.11 cd

Purpose

Use the `cd` command to change the directory that you are browsing in the Oracle Secure Backup [catalog](#). Options to the `cd` command affect subsequent [ls](#) (page 2-114) and [restore](#) (page 3-99) commands.

Browsing the catalog is equivalent to browsing the contents of backup images and backup image instances. The `obtool` utility displays the contents of the images in a directory structure much like a live file system. You can only browse directories whose contents have been backed up.



See Also:

"[Browser Commands](#) (page 1-12)" for related commands

Prerequisites

The [rights](#) needed to run the `cd` command depend on the [browse backup catalogs with this access](#) (page 8-3) setting for the [class](#).

Syntax

```
cd::=
```

```
cd [ --host/-h hostname ] [ --viewmode/-v viewmode ]
[ --select/-s data-selector[,data-selector]... ]
[ pathname ]
```

Semantics

--host/-h *hostname*

Defines the name of the host computer assigned with the [mkhost](#) (page 3-26) or [renhost](#) (page 3-87) commands. You must set the host before you can browse its file system in the Oracle Secure Backup catalog. You can also use the [set](#) (page 3-140) `host` command to set the host.

--viewmode/-v *viewmode*

Specifies the mode in which to view directory contents in the Oracle Secure Backup catalog. The `cd` command remains in *viewmode* until you change it to a different setting. Valid values for *viewmode* are as follows:

- `exact` makes visible only those directory entries that match the data selector and are present in the current path.
- `inclusive` makes visible all entries regardless of the current data selector (default).
- `specific` makes visible all entries that match the specified data selector.

--select/-s *data-selector*

Specifies the Oracle Secure Backup catalog data that applies to an operation. Refer to "[data-selector](#) (page 4-6)" for the *data-selector* placeholder.



Note:

The data selector values specified by `cd` do not affect the [lsbu](#) (page 2-122) command, which lists all backups unless a *data-selector* is specified by `lsbu`.

pathname

Specifies the path name to browse in the Oracle Secure Backup catalog.

Example

Example 2-21 Changing Directories

This example sets the host to `brhost2`, changes into the `root` directory of the Oracle Secure Backup catalog, and displays its contents.

```
ob> cd --host brhost2
ob> cd /
ob> ls
/home
```

2.1.12 cdds

Purpose

Use the `cdds` command to change the [dataset directory](#) on the [administrative server](#). This command enables you to move up and down a dataset directory tree.

 **See Also:**

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `cdds` command.

Syntax

```
cdds::=  
cdds [ dataset-dir-name ]
```

Semantics***dataset-dir-name***

Specifies the name of a dataset directory into which you want to change. Refer to "[dataset-dir-name](#) (page 4-7)" for a descriptions of the *dataset-dir-name* placeholder.

Example**Example 2-22 Making a Dataset Directory**

This example lists the contents of the top-level directory, changes into the `mydatasets` subdirectory, and then shows the name of the current directory.

```
ob> lsds  
Top level dataset directory:  
mydatasets/  
ob> cdds /mydatasets  
ob> pwdds  
/mydatasets
```

2.1.13 cdp

Purpose

Use the `cdp` command to set the identity of the current policy or policy class. Policies are represented in a directory structure with a slash (/) as root and the policy classes as subdirectories. You can use `cdp` to navigate this structure and [pwdp](#) (page 3-77) and [lsp](#) (page 2-157) to display policy information.

 **See Also:**

- "[Policy Commands](#) (page 1-18)" for related commands
- [Defaults and Policies](#) (page 7-1) for a complete list of policies and policy classes

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `cdp` command.

Syntax

```
cdp::=
```

```
cdp [ policy-name ]
```

Semantics

policy-name

Specifies the name of a policy or a class of policies. If omitted, then `obtool` sets the current policy to a slash (/).

Example

Example 2-23 Browsing Policy Information

This example uses the [pwdp](#) (page 3-77), [lsp](#) (page 2-157), and `cdp` commands to browse the policies and find the value for the daemon policy `webautostart`.

```
ob> pwdp
/
ob> lsp
daemons          daemon and service control policies
devices          device management policies
index            index catalog generation and management policies
local            Oracle Secure Backup configuration data for the local machine
logs            log and history management policies
media            general media management policies
naming           WINS host name resolution server identification
ndmp            NDMP Data Management Agent (DMA) defaults
operations       policies for backup, restore and related operations
scheduler       Oracle Secure Backup backup scheduler policies
security        security-related policies
testing         controls for Oracle Secure Backup's test and debug tools
ob> cdp daemons
ob> lsp
auditlogins      no [default]
obixdmaxupdaters 2 [default]
obixdrechecklevel structure [default]
obixdupdaternicevalue 0 [default]
webautostart     yes
webpass          (set)
windowscontrolcertificateservice no [default]
ob> cdp webautostart
ob> lsp
webautostart     yes
```

2.1.14 chclass

Purpose

Use the `chclass` command to change the attributes of a user [class](#).

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chclass` command.

See Also:

- ["Class Commands \(page 1-13\)"](#) for related commands
- [Classes and Rights](#) (page 8-1) for a descriptions of the default Oracle Secure Backup classes and [rights](#)

Syntax

`chclass::=`

```
chclass [ --modself/-m { yes | no } ] [ --modconfig/-M { yes | no } ]
[ --backupsself/-k { yes | no } ] [ --backuppriv/-K { yes | no } ]
[ --restself/-r { yes | no } ] [ --restpriv/-R { yes | no } ]
[ --listownjobs/-j { yes | no } ] [ --modownjobs/-J { yes | no } ]
[ --listanyjob/-y { yes | no } ] [ --modanyjob/-Y { yes | no } ]
[ --mailinput/-i { yes | no } ] [ --mailerrors/-e { yes | no } ]
[ --mailrekey/-g { yes | no } ] [ --browse/-b browserights ]
[ --querydevs/-q {yes | no}] [ --managedevs/-d {yes | no} ]
[ --listownbackups/-s {yes | no} ] [ --modownbackups/-S {yes | no} ]
[ --listanybackup/-u {yes | no} ] [ --modanybackup/-U {yes | no} ]
[ --orauser/-o {yes | no} ] [ --orarights/-O oraclerights ]
[ --fsrights/F fsrights ] [ --listconfig/-L {yes | no} ]
[ --modcatalog/-c {yes | no} ]
classname...
```

Semantics

See "[mkclass](#) (page 3-2)" for descriptions of the options.

classname

The name of the class to be modified. Class names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example

Example 2-24 Changing Classes

This example lists every user who can run backups with administrator privileges, grants this privilege to `user`, and then confirms that the grant was successful.

```
ob> lsclass --backuppriv yes
admin
operator
ob> chclass --backuppriv yes user
ob> lsclass --backuppriv yes
admin
operator
user
```

2.1.15 chdev

Purpose

Use the `chdev` command to change the attributes of a configured tape drive, tape library, disk pool, or cloud storage device. Use the [mkdev](#) (page 3-6) command to initially configure a tape device, disk pool, or cloud storage device.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chdev` command.

Usage Notes

While using `chdev` with ACSLS libraries or tape drives contained in an ACSLS library, certain device attributes that affect library operations cannot be modified when `obacslibd` is running. Such attributes can be modified only when `obacslibd` is stopped.



See Also:

More information about attributes that cannot be modified when `obacslibd` is running is available at:

- "[Semantics 4](#) (page 2-34)" for tape drives contained within an ACSLS library
- "[Semantics 5](#) (page 2-34)" for ACSLS tape libraries
- "[Semantics 6](#) (page 2-35)" for ACS cartridge access port (CAP) within an ACSLS library

Syntax 1

Use the following syntax to reconfigure a tape drive.

```
chdev::=
```

```
chdev [ --attach/-a aspec[,aspec]... ]
[ --addattach/-A aspec[,aspec]... ]
[ --rmattach/-R aspec[,aspec]... ]
[ --inservice/-o | --notinservice/-O ] [ --wwn/-W wwn ]
[ --library/-l devicename ] [ --dte/-d dte ]
[ --ejection/-j etype ]
[ --minwritablevolumes/-m n ]
[ --blockingfactor/-f bf ] [ --maxblockingfactor/-F maxbf ]
[ --automount/-m { yes | no } ] [ --erate/-e erate ]
[ --current/-T se-spec ] [ --uselist/-u se-range ]
```

```
[ --usage/-U duration ] [ --positioninterval/-q positioninterval ]
[ --serial/-N serial-number ] [ --model/-L model-name ]
[ --updateserialnumber/-S ]
devicename...
```

Syntax 2

Use the following syntax to reconfigure a tape library.

chdev::=

```
chdev [ --attach/-a aspec[,aspec]... ]
[ --addattach/-A aspec[,aspec]... ]
[ --class/-x vtl ]
[ --rmattach/-R aspec[,aspec]... ]
[ --inservice/-o | --notinservice/-O ][ --wwn/-W wwn ]
[ --autoclean/-C { yes | no } ][ --cleanemptiest/-E { yes | no } ]
[ --cleaninterval/-i { duration | off } ]
[ --barcodereader/-B { yes | no | default } ]
[ --barcodesrequired/-b { yes | no | default } ]
[ --unloadrequired/-Q { yes | no } ]
[ --serial/-N serial-number ] [ --model/-L model-name ]
[ --updateserialnumber/-S ]
[ --ejection/-j etype] [ --minwritablevolumes/-V minvols]
devicename...
```

Semantics 1 and 2

The following options enable you to reconfigure a tape drive or tape library. Refer to "[mkdev](#) (page 3-6)" for descriptions of options not included in this section.

--addattach/-A *aspec*

Adds a device [attachment](#) for a tape drive or tape library. Refer to "[aspec](#) (page 4-1)" for a description of the *aspec* placeholder.

--class/-x vtl

Specifies library class as VTL.

--rmattach/-R *aspec*

Removes a device attachment for a tape drive or tape library. Refer to "[aspec](#) (page 4-1)" for a description of the *aspec* placeholder.

--uselist/-u *se-range*

Specifies a range of [storage elements](#) that the device can use. This option only applies to a tape drive contained in a tape library.

By default, Oracle Secure Backup allows all tapes in a tape library to be accessed by all tape drives in the tape library. For libraries containing multiple tape drives which perform backups concurrently, you might want to partition the use of the tapes. For example, you might want the tapes in half the storage elements to be available to the first tape drive and the second half to be available to the second tape drive. Alternatively, you might want to set up different use lists for different types of backups on a single tape drive.

Changes to the `uselist` value for a tape device are not recognized by jobs that run when you enter the `chdev` command. If a job is stalled for lack of usable volumes, for example, you cannot rescue the job by adding storage elements with a `chdev --uselist` command. The `chdev` operation succeeds, but the job remains stalled. You must cancel and restart the job for the `chdev` changes to take effect.

Refer to "[se-range](#) (page 4-27)" for a description of the *se-range* placeholder.

--usage/-U duration

Specifies the amount of time a tape drive has been used since it was last cleaned. Refer to "duration (page 4-14)" for a description of the *duration* placeholder. The `mkdev` (page 3-6) command enables you to request a cleaning cycle for a specific interval. Specify the `--usage` option on `chdev` to initialize the configured interval to reflect tape drive usage since the last cleaning.

--ejection/-j etype

Specifies the means by which tapes are ejected. Values are `automatic`, `ondemand`, or `manual`.

--minwritablevolumes/-m n

Specifies the threshold for the minimum number of writeable volumes before Oracle Secure Backup initiates early `volume` rotation.

--serial/-N serial-number

Specifies the serial number for the tape device.

If you explicitly enter a serial number with the `mkdev` command, then Oracle Secure Backup stores this serial number in the device object. If you specify the *serial-number* argument as null (`' '`), then Oracle Secure Backup opens the device, reads the serial number from the device, and stores the number in the device object.

If the `checkserialnumbers` policy is enabled, then you must enter a serial number with a `chdev --serial` command whenever tape device hardware is changed, as when a broken tape drive in a tape library is replaced. You must enter the number even if no serial number was entered when the device object was created.

**See Also:**

"[checkserialnumbers](#) (page 7-13)"

--updateserialnumber/-S

Semantically equivalent to `--serial` with a null argument. Oracle Secure Backup opens the tape device, reads the serial number from the device, and stores the serial number in the device object.

devicename

Specifies the name of the tape library or tape drive to be reconfigured. Refer to "[devicename](#) (page 4-12)" for the rules governing tape device names.

Syntax 3

Use the following syntax to reconfigure a disk pool.

```
chdev
[--attach/-a aspec[,aspec]...]
[--addattach/-A aspec[,aspec]...]
[--rmattach/-R aspec[,aspec]...]
[--inservice/-o | --notinservice/-O]
[--capacity/-y size-spec] [--concurrentjobs/-J concjobs]
[--blockingfactor/-f bf] [--maxblockingfactor/-F maxbf]
[--freospacegoal/-G freospacegoal]
[--staging/-h {yes | no}]
[--stagerule/-H stage-rule-name [,stage-rule-name]...]
[--addstagerule stage-rule-name [,stage-rule-name]...]
[--mvstagerule [after-stage-rule-name:]
                {start-stage-rule-name} [-end-stage-rule-name]]
```

```
[--rmstagerule stage-rule-name ,[stage-rule-name]...]
devicename...
```

Semantics 3

Refer to "mkdev (page 3-6)" for descriptions of options that are not included in this section.

--attach/-a *aspec*

Redefines the host and file-system directory that store backup image instances for the disk pool. All previous definitions of the disk pool are discarded. However, the backup image instances stored in the file-system directory are not affected.

--addattach/-A *aspec*

Adds a device attachment for a disk pool.

See "[aspec](#) (page 4-1)" for a description of the *aspec* placeholder.

--rmattach/-R *aspec*

Removes a device attachment for a disk pool. See "[aspec](#) (page 4-1)" for a description of the *aspec* placeholder.

--staging/-h {*yes* | *no*}

Enables or disables staging. (Note that a cloud storage device cannot have staging enabled.)

--addstagerule *stage-rule-name* [,*stage-rule-name*]...

Adds stage rule names to the device stage rule list. Provide the list of names as a comma-delimited sequence. The names are added to the end of the list. You can move the names anywhere in the list by issuing another `chdev` command with the `--mvstagerule` option.

This option cannot be used if the `--stagerule` option or the `--mvstagerule` option is specified.

--mvstagerule [*after-stage-rule-name*][:*start-stage-rule-name*] [*-end-stage-rule-name*]

Moves one or more stage rules in the device stage rule list. If *after-stage-rule-name* followed by a colon character is specified, then a rule, or rules, are moved to after *after-stage-rule-name* in the list of stage rules, otherwise; the rules are moved to the beginning of the list.

The specified rules can be either a single rule on the list, or a range of rules specified by *start-stage-rule-name-end-stage-rule-name*.

This option cannot be used if the `--stagerule` option, the `--addstagerule` option, or the `--rmstagerule` option is specified.

--rmstagerule *stage-rule-name* [,*stage-rule-name*]...

Removes one or more stage rules from the device stage rule list.

This option cannot be used if the `--stagerule` option, the `--addstagerule` option, or the `--mvstagerule` option is specified.

Syntax 4

Use the following syntax for changing the configuration of a tape drive contained within an ACSLS tape library.

```
chdev::=
```

```
chdev [ --attach/-a aspec ] [ --inservice/-o | --notinservice/-0 ]
[ --addattach/-A aspec[,aspec]... ] [ --rmattach/-R aspec[,aspec]... ]
```

```
[ --wwn/-W wwn ] [ --library/-l devicename ]
[ --lsm/s lsm_id ] [ --panel/p panel_id ] [ --drive/r drive_id ]
[ --blockingfactor/-f bf ] [ --maxblockingfactor/-F maxbf ]
[ --erate/-e erate ] [ --positioninterval/-q positioninterval ]
devicename...
```

Semantics 4

Use the following semantics for changing the configuration of a tape drive contained within an ACSLS tape library. See "[Semantics 1 and 2](#) (page 2-31)" for options not identified here.

When `obacslibd` is running, you cannot modify the following attributes of a tape drive that is contained within an ACSLS library:

- `--lsm/s lsm_id`
- `--panel/p panel_id`
- `--drive/r drive_id`

--addattach/-A *aspec*

Adds a device [attachment](#) for tape drives contained in ACSLS libraries. Refer to "[aspec](#) (page 4-1)" for a description of the `aspec` placeholder.

--rmattach/-R

Removes a device attachment for tape drives contained in ACSLS libraries. Refer to "[aspec](#) (page 4-1)" for a description of the `aspec` placeholder.

--lsm/-s *lsm_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the ACS Library Storage Module where this tape drive resides.

--panel-p *panel_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the panel where this tape drive resides.

--drive -r *drive_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the drive where this tape drive resides.

Syntax 5

Use the following syntax to reconfigure an ACSLS tape library.

```
chdev::=
```

```
chdev [ --attach/-a aspec ] [ --inservice/-o | --notinservice/-O ]
[ --userid/-n acs-userid ] [ --acsid/-g acs_id ] [ --port/-P port_num ]
[ --ejection/-j etype ] [ --minwritablevolumes/-V minvols ]
library_devicename...
```

Semantics 5

Use the following syntax for reconfiguring an ACSLS tape library. See "[Semantics 1 and 2](#) (page 2-31)" for options not identified here.

When `obacslibd` is running, you cannot modify the following attributes of an ACSLS tape library:

- `--attach/-a aspec`

- `--userid/-n acs_userid`
- `--acsid/-g acs_id`
- `--port/-P port_num`

--attach/-a *aspec...*

This option specifies the Oracle Secure Backup [media server](#) and ACSLS server for an ACSLS tape library. The format of *aspec* is `mediaservhostname:acslshost`

--userid/-n *acs_userid*

This option specifies the ACSLS access control user name. This value is optional. If it is specified, then all interactions with an ACSLS server are preceded by this access name.

--acsid/-g *acs_id*

This option specifies the ACS ID value for the ACSLS tape library to control.

--port/-P *port_num*

This option specifies the listening port of the ACSLS server software. Typically this value is 0 or not specified. This option must be specified only when your ACSLS server is located behind a [firewall](#).

Syntax 6

Use the following syntax to associate a symbolic name with an ACS cartridge access port (CAP) within an ACSLS tape library.

```
chdev::=
```

```
chdev [ --library/-L devicename ]
[ --lsm/s lsm_id ] [ --capid/-c cap_id ]
capname
```

Semantics 6

Use the following semantics to associate a symbolic name with an ACS cartridge access port (CAP) within an ACSLS tape library.

When `obacslibd` is running, you cannot modify the following attributes of an ACS CAP within an ACSLS tape library:

- `--lsm/s lsm_id`
- `--capid/-c cap_id`

--library/-L *devicename*

This option specifies the name of the tape library in which the CAP resides. If it is omitted, then the library variable is used. If the library variable is not found and one is not specified, then an error message is displayed.

--capid/-c *cap_id*

This option specifies the hardware location of the CAP within the selected tape library.

--lsm /-s *lsm_id*

This option specifies the ACS Library Storage Module of the CAP within the selected tape library.

capname

The name of the Oracle Secure Backup CAP object to be created.

Syntax 7

Use the following syntax to reconfigure a cloud storage device.

chdev::=

```
chdev --type/-t cloudstorage
[--mediaserver media server,media server,...]
[--addmediaserver mediaserver,mediaserver,...]
[--rmmediaserver mediaserver,mediaserver,...]
[--inservice/-o | --notinservice/-O]
[--segmentsize segment-size]
[--capacity/-y size-spec]
[--username cloud-user]
[--querypassphrase]
[--streamspersjob streams-per-job]
[--concurrentjobs concjobs]
[--blockingfactor/-f bf]
[--maxblockingfactor/-F maxbf]
[--freespacegoal/-G freespacegoal]
[--proxy proxy-url]
[--proxyuser proxy-user]
[--queryproxypass]
[--url cloud-url]
[--force]
devicename...
```

Semantics 7

Use the following semantics to reconfigure a cloud storage device.

Refer to "[mkdev](#) (page 3-6)" for descriptions of options that are not included in this section.

--mediaserver mediaserver[,mediaserver]

Name of the attached media server. If multiple media servers are specified, then Oracle Secure Backup verifies that the container is reachable via all specified media servers.

When a media server is specified, all data is sent from the client to the media server. The media server then buffers and uploads the data to the cloud. Running too many jobs on the same media server may affect performance.

The media server must have a cloud wallet. See *Oracle Secure Backup Installation and Configuration Guide* for information about creating a cloud wallet and importing it into media servers.

--addmediaserver mediaserver[,mediaserver]

Adds one or more media servers

--rmmediaserver mediaserver[,mediaserver]

Removes one or more media servers

--inservice/-o | --notinservice/-O

The `inservice` option sets the status of the cloud storage device so that it is logically available to Oracle Secure Backup. The `notinservice` option sets the status of the cloud storage device so that it is not logically available to Oracle Secure Backup.

--capacity/-y size-spec

Specifies the amount of space that the cloud storage device can occupy in the configured cloud account identity domain. The size-spec placeholder specifies the size of the cloud storage device. Enter a numeric value followed by unit. The unit for cloud storage device size can be one of the following: KB, MB, GB, TB, PB or EB. Enter zero to indicate that there is no limit on the size of the cloud storage device. In this case, the size of the cloud storage device is limited only by the quota purchased for the cloud account identity domain or quota set for the corresponding container configured in cloud storage device.

If the size of backup image instances on the cloud storage device exceeds the specified capacity, then Oracle Secure Backup does not schedule any further jobs for this cloud storage device until the space consumption drops below the capacity. If you use the chdev command to change the size of a cloud storage device, then the value you specify cannot be lower than the space currently occupied by the cloud storage device, or the command will fail.

--username cloud user

User name of the cloud account

--container container name

Name of the container in cloud storage. A container is a storage compartment that provides a way to organize the data stored in Oracle Cloud Infrastructure.

--segmentsize segment size

Oracle Secure Backup stores each backup image by splitting it into multiple segments and storing each segment as a single object in a cloud storage container. The segment size defines the size of object.

--streamsperjob num

Oracle Secure Backup can make multiple connections to Oracle Cloud Infrastructure for faster uploads of data. The streamsperjob value defines the number of connections that Oracle Secure Backup can make per job.

--concurrentjobs num

Specifies the maximum number of jobs that can run concurrently for this device. This includes backup, restore, and device management-related jobs. See [concjobs](#) (page 4-5) for more information.

--blockingfactor/-f bf

Specifies a blocking factor. A blocking factor determines how many 512-byte records to include in each block of data written to the device. By default, Oracle Secure Backup writes 64K blocks, which is a blocking factor of 128.

--maxblockingfactor/-F maxbf

Specifies a maximum blocking factor. The maximum blocking factor controls the amount of data that Oracle Secure Backup initially reads from the device whose blocking factor is unknown.

--freespacegoal/-G freespacegoal

Specifies the percentage of cloud storage device capacity that the device manager must maintain by proactively deleting expired backup image instances.

--proxy proxy url

If the connection to Oracle Cloud Infrastructure is through a proxy server, then specify the proxy server URL.

--proxyuser proxy user

The proxy server user name

--proxypass proxy pass

The proxy user password

--url url to cloudThe URL for the Oracle Cloud storage account. It is defined as *identity domain.storage.oraclecloud.com***--identitydomain identify domain name**

The identity domain name that is associated with the user's cloud storage service.

devicename

Name of the cloud storage device being reconfigured

Examples**Example 2-25 Reconfiguring a Tape Drive**This example reconfigures tape drive `tape1` in tape library `lib1`. The `chdev` command specifies the following:

- The tape drive is in service.
- The **error rate** is 16 (the default is 8).
- The **blocking factor** is 256, which means that `obtool` writes blocks of size 128 KB.
- Tapes can be automounted.

Note that the command line has been reformatted to fit on the page.

```
ob> lsdev --long tape1
tape1:
  Device type:          tape
  Model:               [none]
  Serial number:      06667256
  In service:         yes
  Library:            lib1
  DTE:                1
  Automount:          yes
  Error rate:         8
  Position interval:  [undetermined]
  Debug mode:         no
  Blocking factor:    (default)
  Max blocking factor: (default)
  Current tape:       [unknown]
  Use list:           all
  Drive usage:        none
  Cleaning required:  no
  UUID:               15ec3d48-8b97-102d-94d5-080020a0a249
  Attachment 1:
    Host:              brhost3
    Raw device:        /dev/obt0
ob> chdev --type tape --erate 16 --blockingfactor 256
--maxblockingfactor 256 tape1
ob> lsd --long tape1
tape1:
  Device type:          tape
  Model:               [none]
  Serial number:      06667256
```

```

In service:          yes
Library:            lib1
DTE:               1
Automount:         yes
Error rate:        16
Position interval: [undetermined]
Debug mode:        no
Blocking factor:   256
Max blocking factor: 256
Current tape:      [unknown]
Use list:          all
Drive usage:       none
Cleaning required: no
UUID:             15ec3d48-8b97-102d-94d5-080020a0a249
Attachment 1:
  Host:            brhost3
  Raw device:     /dev/obt0

```

Example 2-26 Reconfiguring a Tape Library

This example reconfigures a tape library called `lib1`. The `chdev` command specifies the following:

- The tape library is in service.
- There is no `barcode` reader.
- The interval between automatic cleaning cycles is 30 hours.
- `obttool` should use the fullest cleaning tape for cleaning.

Note that the command line has been reformatted to fit on the page.

```

ob> lsdev --long --nohierarchy lib1
lib1:
  Device type:      library
  Model:           [none]
  Serial number:   [none]
  In service:      yes
  Debug mode:      no
  Barcode reader:  default (hardware-selected)
  Barcodes required: no
  Auto clean:      no
  Clean interval:  (not set)
  Clean using emptiest: no
  UUID:           f088f234-8d46-1027-90e1-000cf1d9be50
Attachment 1:
  Host:            brhost3
  Raw device:     /dev/lib1
ob> chdev --type library --inservice --barcodereader no --barcodesrequired no
--autoclean yes --cleanemptiest no --cleaninterval 30hours lib1
ob> lsdev --long --nohierarchy lib1
lib1:
  Device type:      library
  Model:           [none]
  Serial number:   [none]
  In service:      yes
  Debug mode:      no
  Barcode reader:  no
  Barcodes required: no
  Auto clean:      yes
  Clean interval:  30hours
  Clean using emptiest: yes

```

```

UUID:                f088f234-8d46-1027-90e1-000cf1d9be50
Attachment 1:
  Host:               brhost3
  Raw device:        /dev/lib1

```

Example 2-27 Reconfiguring a Disk Pool

This example reconfigures a disk pool called `dp1` and creates an attachment to the file-system directory `/scratch/osb_test/virtual_devices/dp3` on the host `brhost3`. The capacity of the disk pool is modified to 50GB and the free space goal is 70%.

```

ob> chdev --attach brhost3:/mydirectory/my_tests/virtual_devices/dp3 --capacity 50GB
--freespacegoal 70 dp1
ob> lsdev -l dp1
dp1:
  Device type:        disk pool
  In service:         yes
  Debug mode:         no
  Capacity:           50.0 GB
  Free space goal:    70%
  Concurrent jobs:    (unlimited)
  Blocking factor:    (default)
  Max blocking factor: (default)
  UUID:               7cbb3ef0-8e57-1030-bb79-00163e359724
  Attachment 1:
    Host:              brhost3
    Directory:         /mydirectory/my_tests/virtual_devices/dp3

```

Example 2-28 Reconfiguring a Cloud Storage Device

This example changes the blocking factor, max blocking factor, streams per job, and segment size of a cloud storage device named `myCloud1`.

```

ob> chdev --segmentsize 20MB -f 2048 -F 2048 --streamsperjob 10 myCloud1
ob> lsdev -l myCloud1
jsmithCloud1:
  Device type:        cloud storage
  In service:         yes
  Debug mode:         no
  Capacity:           (not set)
  Consumption:        191.5 MB
  Reclaimable space: 191.5 MB
  Free space goal:    (system default)
  Concurrent jobs:    5
  Blocking factor:    2048
  Max blocking factor: 2048
  UUID:               186b10d8-a3fa-4f35-9171-80c7c4139297
  Attachment 1:
    Host:              MYHOST
  Staging:            no
  URL:                 example.storage.oraclecloud.com
  Username:            jsmith@example.com
  Container:          myCloud1
  Storage class:       object
  Identity domain:     example
  Segment size:        20.0 MB
  Streams per job:     10
  Number of objects:   23
  Bytes used:          191.7 MB
ob>

```

2.1.16 chdup

Purpose

Change the settings of a [volume](#) duplication policy.

See Also:

"[Volume Duplication Commands](#) (page 1-22)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chdup` command.

Syntax

`chdup::=`

```
chdup
[ --comment/-c commentstring ]
[ --inputcomment/-i ]
[ --trigger/-e dupevent:duration ]
[ --restrict/-r restriction[,restriction]... ]
[ --addrrestrict/-R restriction [,restriction]... ]
[ --rmrestrict/-S restriction[,restriction]... ]
[ --migrate/-m { yes | no } ]
[ --rule/-u duplicationrule[,duplicationrule]... ]
[ --addrule/-U duplicationrule[,duplicationrule]... ]
[ --rmrule/-V duplicationrule[,duplicationrule]... ]
[ --chrule/-h duplicationrule[,duplicationrule]... ]
policyname
```

See Also:

- "[dupevent](#) (page 4-12)" for a description of the *dupevent* placeholder
- "[duration](#) (page 4-14)" for a description of the *duration* placeholder
- "[restriction](#) (page 4-25)" for a description of the *restriction* placeholder

Semantics

--comment/-c *commentstring*

A descriptive comment for the volume duplication policy.

--inputcomment/-i

Allows input of an optional comment. After you run `chdup --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--trigger/-e *dupevent:duration*

Specifies when a volume becomes eligible for duplication. The *duration* placeholder specifies how long after *dupevent* the volume becomes eligible for duplication.

--restrict/-r *restriction...*

Replaces any specified backup container restrictions for this duplication policy with the specified restrictions. If you do not specify a restriction, then this volume duplication policy has no restrictions, and can use any available backup container on any [media server](#) at the discretion of the Oracle Secure Backup scheduling system. By default, there are no restrictions defined for a volume duplication policy.

--addrestrict/-R *restriction...*

Adds specified tape device restrictions to the tape device restriction for this duplication policy. Existing restrictions are retained.

--rmrestrict/-S *restriction...*

Removes specified tape device restrictions from the tape device restriction for this duplication policy. If all restrictions are removed, then volume duplication for this policy can be performed using any tape device in the [administrative domain](#).

--migrate/-m

Specifies volume must be migrated. If this option is set to *yes*, then only one duplication rule can be specified for this volume duplication policy.

--rule/-u *duplicationrule*

Specifies the duplication rules for this duplication policy.

--addrule/-U *duplicationrule*

Adds the specified duplication rule to the set of rules for this duplication policy.

--rmrule/-V *duplicationrule*

Removes the specified duplication rule from the set of rules for this duplication policy.

--chrule/-h *duplicationrule*

This option changes the attributes associated with an existing rule in a duplication policy. The *media-family* field of the duplication rule specified in the `--chrule` option is compared against all duplication rules in the specified duplication policy. For any matching rules the *number* field of the existing duplication rule is replaced with the *number* field from the duplication rule specified in the `--chrule` option.

Example**Example 2-29 Modifying a Duplication Policy**

This example changes the *trigger*, *restriction*, and *rule* settings or the duplication policy `voldup1`, created in [Example 3-11](#) (page 3-25).

```
ob> lsdup
voldup1
ob> chdup --trigger lastwrite:forever --rmrestrict @brhost3 --chrule
RMAN-DEFAULT:3 voldup1
ob> lsdup --long voldup1
voldup1:
  Migrate:                no
  Trigger:                lastwrite : forever
  Rule 1:                 RMAN-DEFAULT : 3
  UUID:                   db4bfd64-18af-1031-b040-00163e527899
```

2.1.17 chhost

Purpose

Use the `chhost` command to change the attributes of a configured Oracle Secure Backup host. Use the `mkhost` (page 3-26) command to configure a host for the first time.

The `chhost` command supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

You cannot modify a host created by the `catalog` (page 2-15) command using `chhost`.



See Also:

"[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chhost` command.

Syntax

`chhost::=`

```
chhost
[ --access/-a { ob | ndmp } ]
[ --inservice/-o | --notinservice/-O ]
[ --disablerds/-d { yes | no | systemdefault } ]
[ --encryption/-e { required | allowed } ]
[ --algorithm/-l { AES128 | AES192 | AES256 } ]
[ --keytype/-t { passphrase | transparent } ]
[ --rekeyfrequency/-g duration ]
[ --passphrase/-s string ]
[ --querypassphrase/-Q ]
[ --keystoreputonly/-T ]
[ --tcpbufsize/-c bufsize ]
[ [ --role/-r role[,role]... ] |
  [ --addrole/-R role[,role]... ] |
  [ --rmrole/-E role[,role]... ] ]
[ [ --ip/-i ipname[,ipname]... ] |
  [ --addip/-I ipname[,ipname]... ] |
  [ --rmip/-P ipname[,ipname]... ] ]
[ --ndmpauth/-A authtype ]
[ { --ndmppass/-p ndmp-password } | --queryndmppass/-q | --dfndmppass/-D ]
[ --ndmpport/-n portnumber ] [ --ndmppver/-v protover ]
[ --ndmpuser/-u ndmp-username ] [ --nocomm/-N ]
[ --ndmpbackuptype/-B ndmp-backup-type ]
[ [ --backupev/-w evariable-name=variable-value ]...
  { [ --addbackupev/-W evariable-name=variable-value ]... |
    [ --rmbackupev/-x evariable-name ]... } ]
[ [ --restoreev/-y evariable-name=variable-value ]... |
  { [ --addrestoreev/-Y evariable-name=variable-value ]...
    [ --rmrestoreev/-z evariable-name ]... } ]
```

```
[ --compression/-K {off | low | medium | basic | high | ""} ]  
hostname...
```

Semantics

Refer to "mkhost (page 3-26)" for options not included in this section.

--access/-a

Specifies an access method for the host. Options are:

- `ob`
Use this option if the host has Oracle Secure Backup installed (UNIX, Linux, or Windows computer) and uses the Oracle Secure Backup internal communications protocol to communicate.
- `ndmp`
Use this option if the host, such as a [filer/Network Attached Storage \(NAS\)](#) device, does not have Oracle Secure Backup installed and uses the [Network Data Management Protocol \(NDMP\)](#) to communicate.

--passphrase/-s

Specifies a passphrase used in generation of the encryption key.

The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the [Oracle Secure Backup user](#) be prompted for the password.

--addrole/-R role

Adds a role to a host. Refer to "[role \(page 4-25\)](#)" for a description of the `role` placeholder.

--keystoreputonly/-T

Adds a key to the key store without making it the active key.

--tcpbufsize/-c bufsize

Specifies [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#) buffer size. The default value is `not set`, in which case global policy `operations/tcpbufsize` applies. The maximum TCP/IP buffer size is 4GB, and the minimum TCP/IP buffer size is 1 KB. If Oracle Secure Backup cannot set TCP/IP buffer size as specified, then it returns a warning. This can happen when the operating system kernel limit is smaller than the specified TCP/IP buffer size. Increasing TCP/IP buffer size also increases TCP/IP advertised window. So to tune backup over a wide area network (WAN), this parameter must be set to a value bigger than the bandwidth times round-trip time.

--rmrole/-E role

Removes a role from a host. Refer to "[role \(page 4-25\)](#)" for a description of the `role` placeholder.

--ipl/-i ipname[,ipname]...

Indicates the IP address of the host computer. You can also use host names for IP addresses. In this case, the host name is resolved by the underlying operating system to an IP address.

If you specify `ipname`, then Oracle Secure Backup never uses the user-assigned host name to obtain the host IP address; instead, it considers each specified `ipname` until it finds one that resolves to a working IP address. If you specified a [PNI \(Preferred](#)

[Network Interface](#)) for this host with the `mkpni` (page 3-40) command, then Oracle Secure Backup considers the PNI address first.

 **Note:**

The use of DHCP to assign IP addresses is not supported for hosts that participate in an Oracle Secure Backup administrative domain. You must assign static IP addresses to all hosts. If you cannot use static IP addresses, then ensure that the DHCP server guarantees that a given host is always assigned the same IP address.

If you do not specify `ipname`, then Oracle Secure Backup tries to resolve the specified `hostname` to obtain the IP address.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--addipl-I *ipname*

Adds an IP address to a host computer.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--rmipl-P *ipname*

Removes an IP address from a host computer.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--nocomm/-N

Suppresses communication with the host computer. This option is useful when you have a host that is no longer connected to their network, but you have tape backups of the host that you might want to restore in the future.

 **Note:**

The `nocomm/-N` option is not supported for NDMP hosts.

--addbackupenvl-W *variable-name=variable-value*

Adds the specified NDMP backup environment variables.

--rmbackupenvl-x *variable-name*

Removes the specified NDMP backup environmental variables.

--addrestoreenvl-Y *variable-name=variable-value*

Adds the specified NDMP restore environmental variables.

--rmrestoreenvl-z *variable-name*

Removes the NDMP restore environmental variables.

--disablerds/-d { *yes* | *no* | *systemdefault* }

Specifies whether Reliable Datagram Socket (RDS) over Infiniband is used for data transfer between clients and the media server. The valid values are:

- `yes`
Oracle Secure Backup does not use RDS for over Infiniband for data transfer between the host and media server.
- `no`
Oracle Secure Backup uses RDS over Infiniband for data transfer between the host and media server.
- `systemdefault`
This is the default setting. Oracle Secure Backup uses the setting made at the administrative domain level to decide if RDS must be used for data transfer. You use the operations policy `disablerds` to specify RDS usage at the administrative level. Therefore, if the `disablerds` operations policy is set to `no`, and the value of `--disablerds` for the host is set to `systemdefault`, the host uses RDS for data transfer.

The `--disablerds` setting at the host level overrides the setting that you made at the administrative domain level by using the `disablerds` operations policy. Therefore, if you set the operations policy `disablerds` to `no`, and, for a particular host, you set the `--disablerds` option of the `chhost` command to `yes`, RDS is not used for data transfer host.

`--compression/-K {off | low | medium | basic | high | ""}`

Specifies the compression option to use.

The possible values are as follows:

off

Software compression is not considered for backups in this host regardless of any global policy, if set.

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the `medium` option. It is slower than the `low` and `medium` options, but faster than the `high` option.

high

Compresses data as much as possible, using extensive CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

"" (empty quotation marks)

Resets any previously set value to the default setting of compression not set.

The default value is that no compression option is set.

hostname

Specifies the name of the host computer for which you want to make configuration changes.

Example

Example 2-30 Changing a Host

This example removes the role of `mediaserver` from host `sfserver1`.

```

ob> lshost
brhost2          client                               (via OB)  in service
brhost3          mediaserver,client                       (via OB)  in service
sfserver1        mediaserver,client                       (via OB)  in service
ndmphost1        client                               (via NDMP) in service
osbsvr1          admin,mediaserver,client           (via OB)  in service
ob> chhost --rmrole mediaserver salessvr1
ob> lshost sfserver1
sfserver1        client                               (via OB)  in service

```

2.1.18 chinstance

Purpose

The `chinstance` command changes the characteristics of a backup image instance.

Prerequisites

You must have the [modify any backup, regardless of its owner](#) (page 8-5) or [modify any backups owned by user](#) (page 8-5) class right to use the `chinstance` command.

Usage Notes

You can modify the expiration date and retention period only for backup image instances that are stored on disk pools.

Syntax

```

chinstance::=
chinstance
[--expiresat/-x date-time | --retain/-r duration ]
{ [--uuid/-u backup-instance-uuid]... | backup-instance-name... }

```

Semantics

--expiresat*/*-x date-time

Specifies the modified expiration time for the backup image instance. See "[date-time](#) (page 4-9)" for information about the format used to specify the expiration time.

--retain*/*-r duration

Specifies the modified duration for which this backup image instance must be valid. See "[duration](#) (page 4-14)" for information about the format used to specify the retention period.

***--uuid*/*-u backup-instance-uuid*]... | *backup-instance-name*...**

Specifies the modified UUID or name for the backup image instance.

Examples

This example modifies the backup image instance `brhost2-20130423-110518.1` and sets its expiration time to 2013/12/31.

```
ob> chinstance --expiresat 2013/12/31 brhost2-20130423-110518.1
ob> lsinstance -l brhost2-20130423-110518.1
Instance name:    brhost2-20130423-110518.1
Type:             file system
Client:           brhost2
Backup level:     0
Container:        dpl
Encryption:       off
Created:          2013/04/23.04:22
Expires:          2013/12/31.01:00   Created by job:      admin/13.1
UUID:            bbada6c0-8e70-1030-b10a-00163e359724
```

2.1.19 chkbw

Purpose

Use the `chkbw` command to check for the existence of a [backup window](#). This command determines whether at least one backup window is available during which backups can run.

If any backup windows exist, then the command generates no output. If no backup windows exist, then the command generates the following output:

Note: no backup windows are configured. Scheduled backups will not run.



See Also:

"[Backup Window Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `chkbw` command.

Syntax

```
chkbw::=
```

```
chkbw
```

Example

Example 2-31 Checking for the Existence of Backup Windows

This example checks whether backup windows exist. In this example, no windows are configured.

```
ob> chkbw
```

Note: no backup windows are configured. Scheduled backups will not run.

2.1.20 chkds

Purpose

Use the `chkds` command to check the syntax in a [dataset file](#). The command generates no output when there are no syntax errors; otherwise, it issues an error. Empty files generate a warning.



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to run the `chkds` command.

Syntax

```
chkds::=
```

```
chkds dataset-file-name...
```

Semantics

dataset-file-name

Specifies the name of a dataset file. Refer to "[dataset-file-name](#) (page 4-7)" for a descriptions of the `dataset-file-name` placeholder.

Examples

Example 2-32 Checking a File for Syntax

This example creates a dataset file with bad syntax and then checks it.

```
ob> mkds --nq --input badsyntax.ds
Input the new dataset contents. Terminate with an EOF or a line
containing just a dot (".").
iclude host brhost2
.
Error: the following problems were detected in dataset badsyntax.ds:
  1: iclude host brhost2
Error: "iclude" - unknown keyword
ob> chkds badsyntax.ds
Error: the following problems were detected in dataset badsyntax.ds:
  1: iclude host brhost2
Error: "iclude" - unknown keyword
```

Example 2-33 Checking Files for Syntax

This example creates two dataset files and then checks them.

```
ob> mkds --nq --input empty.ds
Input the new dataset contents. Terminate with an EOF or a line
containing just a dot (".").
```

```
.
ob> mkds --nq --input goodsyntax.ds
Input the new dataset contents.  Terminate with an EOF or a line
containing just a dot (".").
include host brhost2
include path /home
.
ob> chkds empty.ds goodsyntax.ds
Warning: dataset empty.ds is empty
```

2.1.21 chkdw

Purpose

Use the `chkdw` command to check for the existence of at least one duplication window.



See Also:

"[Duplication Window Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chkdw` command.

Syntax

```
chkdw::=
```

```
chkdw
```

2.1.22 chloc

Purpose

Modify a [location](#) object.



See Also:

"[Location Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chloc` command.

Syntax

```
chloc::=
```

```
chloc
```

```
[ --comment/-c commentstring | --inputcomment/-i commentstring ]
```

```
[ --mailto/-m email-target[,email-target] ]  
[ --addmailto/-a email-target[,email-target] ]  
[ --rmailto/-r email-target[,email-target] ]  
[ --customerid/-I idstring ]  
[ --notification/-n ntype ]  
[ --recalltime/-R duration ]  
locationname...
```

Semantics

--comment/-c *commentstring*

Specifies a descriptive comment for the location. You can specify either `--comment` or `--inputcomment`, but not both.

--inputcomment/-i

Allows input of an optional comment. After you run `chloc --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself. You can specify either `--comment` or `--inputcomment`, but not both.

--mailto/-m *email-target[,email-target]*

Specifies one or more e-mail recipients for the location.

--addmailto/-a *email-target[,email-target]*

Specifies one or more e-mail recipients to be added to the location.

--rmailto/-r *email-target[,email-target]*

Specifies one or more e-mail recipients to be removed from the location.

--customerid/-I *idstring*

A customer ID string. Only valid for a [storage location](#).

--notification/-n *ntype*

The `--notification ntype` option enables you to specify a type of electronic notification to be sent to the offsite vault vendor when media are moved from or to a [storage location](#). The `ntype` value is either `none` or `imftp` (Iron Mountain FTP file).

--recalltime/-R *duration*

The `--recalltime` option enables you to specify the time taken to recall a [volume](#) from this storage location to the data center. This setting is disabled for an [active location](#) and is valid only for offsite storage locations. You can use this setting to determine whether to fail a restore request initiated by [Recovery Manager \(RMAN\)](#) that requires use of tape volumes that cannot be supplied within the specified resource wait time period. This parameter can also be used by the volume cloning feature to determine which volume to recall for a restore operation when multiple copies are available at multiple offsite locations.

locationname

The name of the storage location.

Note:

`all` is a reserved word and cannot be used as a location name.

Example

Example 2-34 Modifying a Location Object

This example modifies the `comment`, `addmailto`, and `customerid` settings for the location object `testloc` created in [Example 3-15](#) (page 3-35).

```
ob> lsloc --long testloc
testloc:
  Recalltime:          1 year
  Mail to:             john.doe@oracle.com
  UUID:                3331c846-18c0-1031-b040-00163e527899
ob> chloc --comment "This is a test storage location" --addmailto
jane.doe@example.com --customerid cust1 testloc
ob> lsloc --long testloc
testloc:
  Comment:             This is a test storage location
  Customer ID:         cust1
  Recalltime:          1 year
  Mail to:             john.doe@oracle.com jane.doe@example.com
  UUID:                3331c846-18c0-1031-b040-00163e527899
```

2.1.23 chmf

Purpose

Use the `chmf` command to alter the attributes of a [media family](#). A media family is a named classification of backup volumes.



See Also:

"[Media Family Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chmf` command.

Usage Notes

Attributes in a media family are applied to a [volume](#) in the media family at [volume creation time](#). The media family attributes are part of the volume's attributes. After data is first written to the volume, you cannot change the volume attributes other than by rewriting the volume. If you change the media family attributes, then these changes do not apply to any volumes that have been created in this family.

Oracle Secure Backup includes a default content-managed media family named `RMAN-DEFAULT`. You cannot delete or rename this media family, although you can reset any options except for the following:

- `--writewindow`
- `--retain`
- `--contentmanaged`

For disk pools, the only media family attribute that is applicable is the expiration time.

Syntax

chmf::=

```
chmf [ --writewindow/-w duration ] [ --retain/-r duration ]
[ [ --vidunique/-u ] | [ --vidfile/-F vid-pathname ] |
  [ --viddefault/-d | [ --vidfamily/-f media-family-name ] ]
[ [ --inputcomment/-i ] | [ --comment/-c comment ] ]
[ --contentmanaged/-C ] [ --append/-a ] [ --noappend/-A ]
[ --rotationpolicy/-R policyname ]
[ --duplicationpolicy/-D policyname ]
[ --acsscratchid/-d acsscratch_id ]
media-family-name...
```

Semantics

Refer to "mkmf (page 3-36)" for descriptions of options that are not included in this section.

--inputcomment/-i

Allows input of an optional comment for the media family. After you run `chmf --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--comment/-c *comment*

Specifies information to store with the media family. To include white space in *comment*, surround the text with quotes.

--rotationpolicy/-R

Specifies the [rotation policy](#) for the media family.
To clear the rotation policy, specify an empty string ("") for the policy name.

--duplicationpolicy/-D

Specifies the duplication policy for the media family.
To remove a duplication policy, specify an empty string for the policy name.

--acsscratchid/-d *acsscratch_id*

For ACSLS libraries this option defines the scratch pool ID from which volumes are pulled. For non-ACSLs libraries this option has no effect. When a volume is unlabeled it is placed back into the scratch pool ID that is defined by the media family it belonged to when it was unlabeled.

When a volume is pulled from a scratch pool and initially labeled, it acquires a permanent media family identical to that which is generated when pre-labeling volumes.

media-family-name

Specifies the name of the media family to change.

Example

Example 2-35 Changing Properties of a Media Family

This example creates a time-managed media family called `full_bkup`. The [write window](#) for volumes in the volume is 7 days. Because the [retention period](#) is 28 days, a volume in the media family expires 35 days after Oracle Secure Backup first writes to it. The example then changes the [retention period](#) from 7 days to 10 days.

```

ob> mkmf --vidunique --writewindow 7days --retain 28days full_bkup
ob> lsmf --long full_bkup
full_bkup:
  Write window:          7 days
  Keep volume set:      28 days
  Appendable:           yes
  Volume ID used:       unique to this media family
ob> chmf --writewindow 10days full_bkup
ob> lsmf --long full_bkup
full_bkup:
  Write window:          10 days
  Keep volume set:      28 days
  Appendable:           yes
  Volume ID used:       unique to this media family

```

2.1.24 chpni

Purpose

Use the `chpni` command to modify the configuration of a Preferred Network Interface (PNI) that was set for a host. The **mkpni** (page 3-40) command enables you to configure a PNI for the first time. You can set multiple PNIs for a particular host.

Prerequisites

You must have the modify administrative domain's configuration right to use the `chpni` command.

Usage Notes

When you use the `chpni` command, in addition to the IP address of the host, you must specify one of the following options: `--client/-c`, `--addclient/-a`, or `--rmclient/-r`.

Syntax

`chpni::=`

```

chpni [{--interface/-i ipname
  [--client/-c client-hostname [,client-hostname] ...]
  [--addclient/-a client-hostname [,client-hostname] ...]
  [--rmclient/-r client-hostname [,client-hostname] ...] } ]
{[--network/-n network/prefix [,ipaddr]]...
  [--addnetwork/-N network/prefix, [ipaddr]]...
  [--rmnetwork/-R network/prefix, [ipaddr]]...
  [--useonly/-o ipaddr]
  [--adduseonly/-A ipaddr]
  [--rmuseonly/-O ipaddr]}
hostname

```

Semantics

--interface/-i ipname

Specifies the IP address or the DNS host name that the specified clients must use when communicating with the server specified by *hostname*.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--client/-c *client-hostname* [,*client-hostname*] ...

Specifies one or more clients that should use the *ipname* when communicating with *hostname*. The *hostname* specifies the host name or internet address of the client as seen from the server. The host name must be a host name that you created with the **mkpni** (page 3-40) command.

--addclient/-a *client-hostname* [,*client-hostname*] ...

Adds a client to the list of PNIs configured for the host.

--rmclient/-r *client-hostname* [,*client-hostname*]...

Removes a client from the list of PNIs configured for the host.

--network/-n *network/prefix,ipaddr*

Updates the existing outbound PNI for *hostname* to the one specified by *network/prefix*.

--addnetwork/-N *network/prefix,ipaddr*

Adds the specified network as an outbound PNI for *hostname*. The network is specified using *network/prefix*. *ipaddr* is optional and specifies the address to which the connection must bind.

--rmnetwork/-N *network/prefix,ipaddr*

Removes the specified network and interface as outbound PNI for the host *hostname*.

--useonly/-o *ipaddr*

Updates the existing outbound PNI for *hostname* to the address specified in *ipaddr*.

--adduseonly/-A *ipaddr*

Configures the IP address specified by *ipaddr* as the only interface that must be used for all outbound connections from the host *hostname*.

--rmuseonly/-O *ipaddr*

Removes the specified *ipaddr* as the only interface that must be used for all outbound connections from *hostname*.

hostname

Specifies the name of the host.

Example**Example 2-36 Adding a PNI for a Host**

This example adds a PNI that specifies that the host *brhost3* must use the IP address 192.0.2.1 when communicating with the server *brhost2*. In this example, a PNI already exists for *brhost2*, and that PNI contains an entry for client *brhost1*.

```
ob> chpni --interface 192.0.2.1 --addclient brhost3 brhost2
ob> lspni
brhost2:
  PNI1:
    interface:      192.0.2.1
    clients:        brhost1, brhost3
```

Example 2-37 Adding a PNI for Outbound Connections for a Host

This example adds a PNI that specifies that the IP address 192.168.1.0 must be used for all outbound connections from the host *brhost2*.

```
ob> chpni --network 192.168.1.0/24 brhost2
ob> lspni
brhost2:
  ONI 1:
    network: 192.168.1.0/24
```

2.1.25 chrot

Purpose

Change the settings of a [rotation policy](#).

See Also:

- "[Rotation Policy Commands](#) (page 1-20)" for information on related commands
- "[mkrot](#) (page 3-42)" for more information on *rotationrule*

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chrot` command.

Syntax

`chrot::=`

```
chrot
[ --comment/-c commentstring | --inputcomment/-i commentstring ]
[ --rule/-u rotationrule[, rotationrule...] ]
[ --addrule/-A rotationrule [, rotationrule...] ]
[ --rmrule/-R rotationrule [, rotationrule...] ]
[ --chrule/-h rotationrule [, rotationrule...] ]
[ --position/-p n ]
policyname...
```

Semantics

--comment/-c *commentstring*

Specifies a descriptive comment for the rotation policy. You can specify either `--comment` or `--inputcomment`, but not both.

--inputcomment/-i

Allows input of an optional comment. After you run `chrot --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself. You can specify either `--comment` or `--inputcomment`, but not both.

--rule/-u *rotationrule*

Specifies the replacement rotation rules for this rotation policy.

Specifying `--rule` in a `chrot` command replaces the rotation rule at the specified `--position` with a new rule, which may have a new location. You can only specify one rule when using `--rule` in conjunction with `--position`. If you do not specify `--position`, then all rotation rules defined for this policy are replaced by the specified rules.

--addrule/-A *rotationrule*

Adds the specified rotation rule to the set of rules for this rotation policy.

--rmrule/-R *rotationrule*

Removes the specified *rotationrule* from the set of rules for this rotation policy.

When removing an existing *rotationrule* from a rotation policy with `--rmrule`, only the location is required. If you specify an `event` or `duration` portion of the *rotationrule*, and they do not match those defined for the existing rule for the specified location, then an error message results.

--chrule/-h

This option changes the attributes associated with an existing rule in a rotation policy. The `location` field of the rotation rule specified in the `--chrule` option is compared against all rotation rules in the specified rotation policy. For any matching rules the `event` and `duration` fields of the existing rotation rule are replaced with the `event` and `duration` fields from the rotation rule specified in the `--chrule` option.

--position/-p *n*

the `--position` value indicates the specific point at which a *rotationrule* is to be added to the existing list of location/duration tuples in the rotation policy. Positions are numbered starting from 1. Rotation rule tuples are inserted immediately before the tuple at the position specified by *n*. For example, if *n*=1, then the tuples are inserted before the first tuple in the list. If *n*=2, then the tuples are inserted between the first and second tuples, and so on. If the `--position` parameter is not specified, then location/duration tuples are inserted after the existing list.

policyname

Specifies the name for a rotation policy, which can be 1-31 characters.

Example**Example 2-38 Changing a Rule in a Rotation Policy**

This example uses `--rule` with `--position` to replace rotation rule 2, and then replace it again, leaving rule 1 intact.

```
ob> lsrot --long rp1
rp1:
  Rotation rule 1:      * : firstwrite : 2 seconds
  Rotation rule 2:      vault : arrival : 1 day
  UUID:                 f7d61560-2d53-102c-8bcf-00163e38b3e7
ob> chrot --rule imvault:arrival:1day --position 2 rp1
ob> lsrot --long rp1
rp1:
  Rotation rule 1:      * : firstwrite : 2 seconds
  Rotation rule 2:      imvault : arrival : 1 day
  UUID:                 f7d61560-2d53-102c-8bcf-00163e38b3e7
ob> chrot --rule Media_Recycle_Bin:arrival --position 2 rp1
ob> lsrot --long rp1
rp1:
  Rotation rule 1:      * : firstwrite : 2 seconds
  Rotation rule 2:      Media_Recycle_Bin : arrival : disabled
  UUID:                 f7d61560-2d53-102c-8bcf-00163e38b3e7
```

2.1.26 chsched

Purpose

Use the `chsched` command to change an existing [backup schedule](#), [volume duplication scan](#), [vaulting scan](#), or [stage scan schedule](#).



See Also:

"[Schedule Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chsched` command.

Syntax 1

Use the following syntax to change an existing backup schedule.

`chsched::=`

```
chsched
[ --dataset/-D dataset-name[,dataset-name]... ]
[ --adddataset/-A dataset-name[,dataset-name]... ]
[ --rmdataset/-R dataset-name[,dataset-name]... ]
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ --encryption/-e { yes | no } ]
[ --restrict/-r restriction[,restriction]... ]
[ --addressrestrict/-E restriction[,restriction]... ]
[ --rmrestrict/-T restriction[,restriction]... ]
[ [ --addtrigger/-a ] |
  [ --chtrigger/-h trigger-number[,trigger-number]... ] |
  [ --rmtrigger/-m trigger-number[,trigger-number]... ] ]
[ [ --day/-d day-date ] [ --time/-t time ]
  [ --level/-l backup-level ] [ --family/-f media-family-name ]
  [ --expires/-x duration ] ]...
[ --compression/-K {off | low | medium | basic | high | ""}]
schedulename...
```

Semantics 1

Refer to "[mksched](#) (page 3-44)" for option descriptions not included in this section.

--dataset/-D dataset-name

Specifies the [dataset](#) to include in the [backup job](#).

--adddataset/-A dataset-name

Adds a dataset to the current schedule.

--rmdataset/-R dataset-name

Removes a dataset from the current schedule.

--enabled/-z

Specifies that the backup schedule be enabled. You can use this option to restart a backup schedule that you earlier disabled.

--disabled/-Z

Specifies that the vaulting scan schedule be disabled. You can use this option to suspend a backup schedule without deleting it. This option is useful when you must take a host out of service temporarily.

--encryption/-e

Specifies encryption flags for the backup schedule or job. Valid values are:

- yes

Backups for these scheduled jobs are always encrypted, regardless of settings for the global or host-specific encryption policies.

- no

This is the default.

If both global and host-specific encryption policies are set to `allowed`, then backups created for these jobs are not encrypted.

If either the global encryption policy or the host-specific encryption policy is set to `required`, then that policy overrides this setting and backups are always encrypted. The encryption algorithm and keys are determined by the policies of each `client` host.

--addrrestrict/-E *restriction*

Adds another `tape drive` to be used by the backup. Refer to "`restriction` (page 4-25)" for a description of the `restriction` placeholder.

--rmrestrict/-T *restriction*

Removes a restriction from a schedule. Refer to "`restriction` (page 4-25)" for a description of the `restriction` placeholder.

--addtrigger/-a

Adds a `trigger` to the schedule. A trigger is a user-defined period in time or sets of times that causes a `scheduled backup` to run. You must specify the `--day` option when adding a trigger. If you specify `--day` but do not specify a time, then the time defaults to 00:00.

--chtrigger/-h *trigger-number*

Edits the specified trigger in the schedule. Specify the `--long` option on the `lssched` (page 2-167) command to obtain trigger numbers.

--rmtrigger/-m *trigger-number*

Removes a trigger from the schedule. Specify the `--long` option on the `lssched` (page 2-167) command to obtain trigger numbers.

--compression/-K {off | low | medium | basic | high | "" }

Specifies a compression option for the backup schedule job that overrides any global and client-level compression options already set.

The possible values are as follows:

off

Software compression is not used for the backup regardless of global and client level policy

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the `medium` option. It is slower than the `low` and `medium` options, but faster than the `high` option.

high

Compresses data as much as possible, using extensive CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

"" (empty quotation marks)

Resets any previously set value to the default setting of compression not set.

The default value is that no compression option is set.

If compression is not specified as part of the `mksched` command, then the client host setting for compression is used. If the client host compression setting is not set, then the domain-level policy is used. If the domain-level policy is also not set, then no software compression is performed for this job.

schedulename

Specifies the name of the schedule.

Syntax 2

Use the following syntax to change an existing vaulting scan schedule.

```
chsched::=
```

```
chsched
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ --location/-L locationname[,locationname]... ]
[ --addlocation/-O locationname[,locationname]... ]
[ --rmlocation/-C locationname[,locationname]... ]
[ --restrict/-r vault_restriction[,vault_restriction] ]
[ --addressrestrict/-E vault_restriction[,vault_restriction] ]
[ --rmrestrict/-T vault_restriction[,vault_restriction] ]
[ --select/-S select_criterion[,select_criterion] ]
[ --addselect/-P select_criterion[,select_criterion] ]
[ --rmselect/-U select_criterion[,select_criterion] ]
[ [ --addtrigger/-a ] |
  [ --chtrigger/-h trigger-number[,trigger-number]... ] |
  [ --rmtrigger/-m trigger-number[,trigger-number]... ] ]
[ [ --day/-d day-date ] [ --time/-t time ] [ --expires/-x duration ] ]...
schedulename...
```

Semantics 2

Refer to "[mksched](#) (page 3-44)" for option descriptions not included in this section.

--enabled/-z

Specifies that the vaulting scan schedule be enabled. You can use this option to restart a vaulting scan schedule that you earlier disabled.

--disabled/-Z

Specifies that the vaulting scan schedule be disabled. You can use this option to suspend a vaulting scan schedule without deleting it. This option is useful when you must take a host out of service temporarily.

--location/-L *locationname*[,*locationname*]...

Specifies a replacement [location](#) to be applied to the vaulting scan schedule. This option replaces the entire set of locations currently defined for the schedule.

--addlocation/-O *locationname*[,*locationname*]...

Adds one or more locations to a vaulting scan schedule.

--rmlocation/-C *locationname*[,*locationname*]...

Removes one or more locations from a vaulting scan schedule.

 **Note:**

The `--location`, `--addlocation`, and `--rmlocation` options are deprecated for vaulting scan schedules in this release, but they are supported for backward compatibility. Oracle recommends that you use the `--restrict`, `--addrestrict`, and `--rmrestrict` options to limit vaulting scans to particular locations.

--restrict/-r *vault_restriction*[,*vault_restriction*]...

Restricts a vaulting scan to one or more locations. The locations can be specified in any of the following forms:

- *location_name*@*cap_name*

The *location_name* is the location that is scanned during a scan job for volumes eligible to be moved. The cartridge access port (CAP) name can be specified only if the location is an ACSLS library.

- *location_name*

If *location_name* is an ACSLS library and no CAP name is specified, then Oracle Secure Backup selects the largest available CAP.

- @*cap_name*

If no location name is specified, then the location of the specified CAP is scanned. This form applies only to ACSLS libraries.

If the ejection type for the library is set to automatic or ondemand, then Oracle Secure Backup exports volumes to the specified CAP during a media movement job. This option replaces the entire set of locations currently defined for the schedule.

--addrestrict/-E *vault_restriction*[,*vault_restriction*]...

Adds one or more locations to a vaulting scan schedule. The locations can be specified in any of the forms listed for the `--restrict` option.

--rmrestrict/-T *vault_restriction*[,*vault_restriction*]...

Removes one or more locations from a vaulting scan schedule. The locations can be specified in any of the forms listed for the `--restrict` option.

--select/-S *select_criterion*[,*select_criterion*]...

Restricts a vaulting scan to one or more media families. This option replaces the entire set of media families currently defined for the schedule.

--addselect/-P *select_criterion*[,*select_criterion*]...

Adds one or more media families to the vaulting scan.

--rmselect/-U *select_criterion*[,*select_criterion*]...

Removes one or more media families from the vaulting scan.

--addtrigger/-a

Adds a [trigger](#) to the schedule. A trigger is a user-defined period in time or sets of times that causes a [scheduled backup](#) to run. You must specify the `--day` option when adding a trigger. If you specify `--day` but do not specify a time, then the time defaults to 00:00.

--chtrigger/-h *trigger-number*

Edits the specified trigger in the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

--rmtrigger/-m *trigger-number*

Removes a trigger from the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

schedulename

Specifies the name of the schedule.

Syntax 3

Use the following syntax to change an existing volume duplication scan schedule.

```
chsched::=
```

```
chsched
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ --location/-L locationname[,locationname]... ]
[ --addlocation/-O locationname[,locationname]... ]
[ --rmlocation/-C locationname[,locationname]... ]
[ [ --addtrigger/-a ] |
  [ --chtrigger/-h trigger-number[,trigger-number]... ] |
  [ --rmtrigger/-m trigger-number[,trigger-number]... ] ]
[ [ --day/-d day-date ] [ --time/-t time ] [ --expires/-x duration ] ]...
schedulename...
```

Semantics 3

Refer to "[mksched](#) (page 3-44)" for option descriptions not included in this section.

--enabled/-z

Specifies that the volume duplication scan schedule be enabled. You can use this option to restart a volume duplication scan schedule that you earlier disabled.

--disabled/-Z

Specifies that the volume duplication scan schedule be disabled. You can use this option to suspend a volume duplication scan schedule without deleting it. This option is useful when you must take a host out of service temporarily.

--location/-L *locationname*

Specifies one or more replacement locations to be applied to a volume duplication scan schedule. This option replaces the entire set of locations currently defined for the schedule. Only an [active location](#) can be specified in a duplication scan schedule.

--addlocation/-O *locationname*

Adds one or more locations to a volume duplication scan schedule. Only an active location can be specified in a duplication schedule.

--rmlocation/-C *locationname*

Removes one or more locations from a volume duplication scan schedule.

--addtrigger/-a

Adds a [trigger](#) to the schedule. A trigger is a user-defined period in time or sets of times that causes a [scheduled backup](#) to run. You must specify the `--day` option when adding a trigger. If you specify `--day` but do not specify a time, then the time defaults to 00:00.

--chtrigger/-h *trigger-number*

Edits the specified trigger in the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

--rmtrigger/-m *trigger-number*

Removes a trigger from the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

schedulename

Specifies the name of the schedule.

Syntax 4

Use the following syntax to change an existing stage scan schedule.

If you remove a stage scan schedule that is referenced in a stage rule, than an error is generated and the stage scan schedule is not deleted.

```
chsched::=
```

```
chsched
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ [ --addtrigger/-a ] |
  [ --chtrigger/-h trigger-number[,trigger-number...] ] |
  [ --rmtrigger/-m trigger-number[,trigger-number...] ] ]
[ [ --day/-d day-date ] [ --time/-t time ]
schedulename...
```

Semantics 4

Refer to "[mksched](#) (page 3-44)" for option descriptions not included in this section.

--enabled/-z

Specifies that the volume duplication scan schedule be enabled. You can use this option to restart a volume duplication scan schedule that you earlier disabled.

--disabled/-Z

Specifies that the volume duplication scan schedule be disabled. You can use this option to suspend a volume duplication scan schedule without deleting it. This option is useful when you must take a host out of service temporarily.

--addtrigger/-a

Adds a [trigger](#) to the schedule. A trigger is a user-defined period in time or sets of times that causes a [scheduled backup](#) to run. You must specify the `--day` option when adding a trigger. If you specify `--day` but do not specify a time, then the time defaults to 00:00.

--chtrigger/-h *trigger-number*

Edits the specified trigger in the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

--rmtrigger/-m *trigger-number*

Removes a trigger from the schedule. Specify the `--long` option on the [lssched](#) (page 2-167) command to obtain trigger numbers.

schedulename

Specifies the name of the schedule.

Example**Example 2-39 Changing a Backup Schedule**

[Example 2-39](#) (page 2-64) starts with a [full backup](#) scheduled to run every Sunday at 9:00 P.M. The first `chsched` command adds a weekday trigger at 4:00 A.M., specifies [media family](#) `full`, and sets the backup to expire after 30 days. The second `chsched` command changes the Sunday trigger to run at noon.

```
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:                backup
  Dataset:             OSB-CATALOG-DS
  Priority:            50
  Encryption:         no
  Comment:            catalog backup schedule
full_backup:
  Type:                backup
  Dataset:             datadir.ds
  Priority:            5
  Encryption:         yes
  Trigger 1:
    Day/date:         sundays
    At:               21:00
    Backup level:     full
    Media family:     (null)
ob> chsched --addtrigger --day "mon tue wed thu fri" --family full --expires
30days --time 04:00 full_backup
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:                backup
  Dataset:             OSB-CATALOG-DS
  Priority:            50
  Encryption:         no
  Comment:            catalog backup schedule
full_backup:
  Type:                backup
  Dataset:             datadir.ds
```

```

Priority:          5
Encryption:       yes
Trigger 1:
  Day/date:       sundays
  At:             21:00
  Backup level:   full
  Media family:   (null)
Trigger 2:
  Day/date:       weekdays
  At:             04:00
  Backup level:   full
  Media family:   full
  Expires after:  30 days
ob> chsched --chtrigger 1 --time 12:00 full_backup
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:           backup
  Dataset:        OSB-CATALOG-DS
  Priority:        50
  Encryption:     no
  Comment:        catalog backup schedule
full_backup:
  Type:           backup
  Dataset:        datadir.ds
  Priority:        5
  Encryption:     yes
Trigger 1:
  Day/date:       sundays
  At:             12:00
  Backup level:   full
  Media family:   (null)
Trigger 2:
  Day/date:       weekdays
  At:             04:00
  Backup level:   full
  Media family:   full
  Expires after:  30 days

```

2.1.27 chssel

Purpose

Use the `chssel` command to change a [database backup storage selector](#) that you previously created with the `mkssel` (page 3-54) command.

See Also:

"[Database Backup Storage Selector Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `chssel` command.

Syntax

Syntax

chssel::=

```

chssel
[ --dbname/-d { * | dbname[,dbname]... } ]
[ --adddbname/-D { * | dbname[,dbname]... } ]
[ --rmdbname/-E dbname[,dbname]... ]
[ --dbid/-i { * | dbid[,dbid]... } ]
[ --adddbid/-I { * | dbid[,dbid]... } ]
[ --rmdbid/-J { * | dbid[,dbid]... } ]
[ --host/-h { * | hostname[,hostname]... } ]
[ --addhost/-H { * | hostname[,hostname]... } ]
[ --rmhost/-K { * | hostname[,hostname]... } ]
[ --content/-c { * | content[,content]... } ]
[ --addcontent/-C { * | content[,content]... } ]
[ --rmcontent/-F { * | content[,content]... } ]
[ --restrict/-r restriction[,restriction]... ]
[ --addrestrict/-R restriction[,restriction]... ]
[ --rmrestrict/-S restriction[,restriction]... ]
[ --copynum/-n { * | 1 | 2 | 3 | 4 } ]
[ --family/-f media_family ]
[ --encryption/-e {off|on|forcedoff|swencryption}]
[ --waittime/-w duration ] [--name/-N name-format]
[--priority/-p default | <schedule-priority>] job priority
sselname...

```

Semantics

--dbname/-d *dbname*

Replaces the current database names for the storage selector with the specified *dbname* values.

--adddbname/-D *dbname*

Adds the specified *dbname* values to the databases currently associated with the storage selector.

--rmdbname/-E *dbname*

Removes the specified *dbname* values from the databases currently associated with the storage selector.

--dbid/-i *dbid*

Replaces the current [database ID \(DBID\)](#) for the storage selector with the specified *dbid* value.

--adddbid/-I *dbid*

Adds the specified *dbid* values to the DBIDs currently associated with the storage selector.

--rmdbid/-J *dbid*

Removes the specified DBIDs from the storage selector.

--host/-h *hostname*

Replaces the current hosts for the storage selector with the specified *hostname* values.

--addhost/-H *hostname*

Adds the specified *hostname* values to the hosts currently associated with the storage selector.

--rmhost/-K *hostname*

Removes the specified *hostname* values from the hosts currently associated with the storage selector.

--content/-c *content*

Replaces the current content types for the storage selector with the specified content types. Refer to "[content](#) (page 4-5)" for a description of the *content* placeholder.

--addcontent/-C *content*

Adds the specified content types to the content types currently associated with the storage selector.

--rmcontent/-F *content*

Removes the specified content types from the content types currently associated with the storage selector.

--restrict/-r *restriction*

Replaces the current backup container restrictions in the storage selector with the specified *restriction* values. Refer to "[restriction](#) (page 4-25)" for a description of the *restriction* placeholder.

--addrestrict/-R *restriction*

Adds the specified *restriction* values to the storage selector.

--rmrestrict/-S *restriction*

Removes the specified *restriction* values from the storage selector.

--copynumber/-n * | 1 | 2 | 3 | 4

Specifies the copy number to which this storage selector applies. The copy number must be an integer in the range 1 to 4. An asterisk (*) specifies that the storage selector applies to any copy number.

--family/-f *media-family*

Replaces the current [media family](#) for the storage selector with the specified family. You create media families with the [mkmf](#) (page 3-36) command.

--waittime/-w *duration*

Replaces the current resource availability time for the storage selector with the specified duration. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

--name/-N *name-format*

Specifies the name assigned to the backup image created by this backup job. You can explicitly specify a name, specify one or more name format variables, or use a combination of name format variable and static values that you specify. See "[name-format](#) (page 4-19)" for a description of the *name-format* placeholder.

--encryption/-e {off | on | forcedoff | swencryption}

Specifies whether backups should be encrypted. In all cases, if the data has been encrypted by RMAN, then Oracle Secure Backup performs no further encryption. Set one of the following options for encryption:

- **ON:** Oracle Secure Backup encrypts the backup data unless it has already been encrypted by RMAN.
- **OFF:** Oracle Secure Backup does not encrypt the backup data unless either the host or global policy is set to required. OFF is equivalent to specifying no value for encryption.
- **FORCEDOFF:** Oracle Secure Backup does not encrypt the database backup, overriding any host-specific encryption settings. The FORCEDOFF setting does not affect RMAN, which can still encrypt the backup data.
- **SWENCRYPTION:** Oracle Secure Backup uses software encryption instead of hardware encryption. This option is provided in case you do not want hardware encryption used in some situations.

 **Note:**

The `encryption` option is only available starting with Oracle Secure Backup 10.3.0.2.0.

`--priority/p job priority`

Specifies a positive integer value that sets the priority for an RMAN backup or RMAN restore job. You can set the job priority value between 1 and 2147483647, with 1 being the highest priority. The default schedule-priority value is 100.

 **See Also:**

[About Setting the Job Priority for RMAN Operations](#) (page C-2)

`sselname`

Specifies one or more names of storage selectors to modify.

Example

Example 2-40 Adding Content Types to a Database Backup Storage Selector

[Example 2-40](#) (page 2-68) creates a backup storage selector named `ssel_full` that specifies that the entire database should be backed up. The example then changes the storage selector to include archived redo logs.

```
ob> mkssel --dbid 1557615826 --host brhost2 --content full --family f1 ssel_full
ob> lssel --long
```

```
ssel_full:
  Content:          full
  Databases:       [all]
  Database ID:     1557615826
  Host:            brhost2
  Restrictions:    [none]
  Copy number:     [any]
  Media family:    f1
  Resource wait time: 1 hour
  UUID:            b5774d9e-92d2-1027-bc96-000cf1d9be50
ob> chssel --addcontent archivelog ssel_full
ob> lssel --long
```

```

ssel_full:
  Contents:          archivelog, full
  Databases:        [all]
  Database ID:      1557615826
  Host:             brhost2
  Restrictions:     [none]
  Copy number:      [any]
  Media family:     f1
  Resource wait time: 1 hour
  UUID:            b5774d9e-92d2-1027-bc96-000cf1d9be50

```

2.1.28 chstage

Purpose

Use the `chstage` command to make changes to an existing stage rule.

Prerequisites

- You must have `admin` class rights to change a stage rule.

Syntax

`chstage::=`

```

chstage [--comment/-c comment]
        [--schedule/-T schedulename]
        [--matchfamily/-f { * | media-family-name[,media-family-name]...}]
        [--addmatchfamily/-F {media-family-name[,media-family-name]...}]
        [--rmmatchfamily/-g {media-family-name[,media-family-name]...}]
        [--dbname/-d { * | dbname[,dbname]...}] |
        [--adddbname/-D dbname[,dbname]...]
        [--rmdbname/-E { dbname[,dbname]...}]
        [--dbid/-i { * | dbid[,dbid]...}]
        [--adddbid/-I {dbid[,dbid]...}]
        [--rmdbid/-J {dbid[,dbid]...}]
        [--fshost/-h { * | fshostname [,fshostname]...}]
        [--addfshost/-H {fshostname [,fshostname]...}]
        [--rmfshost/-K {fshostname[,fshostname]...}]
        [--mincopysize/-s size-spec]
        [--mincopyage/-a duration]
        [--targetfamily/-t target-media-family-name]
        [--restrict/-r restriction[,restriction]...]
        [--addrrestrict/-R restriction[,restriction]...]
        [--rmrestrict/-S restriction[,restriction]...]
        [--encryption/-e {yes | no | forcedoff}]
        [--algorithm/-L enc-algorithm]
        [[--priority {schedule-priority | default}]]
        [--migrate/-m {yes | no}]
        stage-rule-name

```

Semantics

Refer to the [mkstage](#) (page 3-57) for option descriptions not included in this section.

--dbname/-d *dbname*

Specifies one or more database names. A backup that has any of the specified database names matches this rule.

--addmatchfamily/-F *media-family-name*

Adds one or more media families.

--rmmatchfamily/-g *media-family-name*

Removes one or more media families.

--adddbname/-D *dbname*

Adds one or more database names.

--rmdbname/-E { *dbname*

Removes one or more database names.

--adddbid/-I *dbid*

Adds one or more database identifiers.

--rmdbid/-J *dbid*

Removes one or more database identifiers.

--addfshost/-H *fshostname*

Adds one or more Oracle Secure Backup client host names that are used to match only backup image instances for file-system backups.

--rmfshost/-K *fshostname*

Removes one or more Oracle Secure Backup client host names that are used to match only backup image instances for file-system backups.

--addrestrict/-R *restriction*

Adds one or more device restrictions.

--rmrestrict/-S *restriction*

Removes one or more device restrictions.

Example

```
chstage --targetfamily mftarget --restrict vt1 OSB-DEFAULT-STAGE-RULE
```

This example adds the media family `mftarget` and the device `vt1` to the Oracle Secure Backup default stage rule.

2.1.29 chsum

Purpose

Use the `chsum` command to change a [job summary schedule](#).

**See Also:**

"[Summary Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `chsum` command.

Syntax

chsum::=

```

chsum [--days/-d produce-days[,produce-days]...]
      [--reporttime/-t time]
      [--mailto/-m email-target[,email-target]...]
      [--addmailto/-a email-target[,email-target]...]
      [--rmmailto/-r email-target[,email-target]...]
      [--host/-h hostname[,hostname]...]
      [--addhost/-H hostname[,hostname]...]
      [--rmhost/-K hostname[,hostname]...]
      [ [--covers/-c duration] |
        [--since/-s "summary-start-day[ ]time" ]
      ]
      [--backup/-B {yes | no}] [--restore/-R {yes | no}]
      [--orabackup/-b {yes | no}] [--orarestore/-e {yes | no}]
      [--scheduleuled/-S {yes | no}] [--user/-U {yes | no}]
      [--subjobs/-J {yes | no}] [--superseded/-D {yes | no}]
      [--duplication/-P {yes | no}] [--mediamovement/-M {yes | no}]
      [--catimport/-I {yes | no}] [--catalog/-C {yes | no}]
      [--copyinstance/-p {yes | no}] [--copyfromstage/-E {yes | no}]
summary-name...

```

Semantics

Refer to "mksum (page 3-61)" for options not included in this section.

--addmailto/-a email-target[,email-target]

Adds additional email addresses to the job summary schedule.

--rmmailto/-r email-target[,email-target]

Removes email addresses from the job summary schedule.

--addhost/-H

Adds a host to the list of hosts to which this [job summary](#) is limited.

--rmhost/-K

Removes a host from the list of hosts to which this job summary is limited.

summary-name

Specifies the name of the job summary schedule.

Example

Example 2-41 Changing a Job Summary Schedule

This example edits the job summary schedule `weekly_report` and adds the email ID `jim@example.com`. It also changes the days of the week on which the job summary is generated to Wednesday and Friday and the time of the report to 12:00.

```

ob> lssum
weekly_report          Wed at 12:00
ob> chsum --addmailto jim@example.com --days Wed,Fri --reporttime 12:00
weekly_report
ob> lssum --long
weekly_report:
  Produce on:          Wed at 12:00
  Mail to:             lance@example.com jim@example.com
  In the report, include:
    Backup jobs:      no

```

```

Restore jobs:          no
Oracle backup jobs:   no
Oracle restore jobs:  no
Duplication jobs:     no
Scheduled jobs:       yes
User jobs:            yes
Subordinate jobs:     yes
Superseded jobs:     no
Catalog backup jobs:  yes
Media movement jobs: no
Catalog import jobs:  no
Copy instance jobs:   yes
Copy from stage jobs: yes

```

ob>

2.1.30 chuser

Purpose

Use the `chuser` command to change the attributes of an [Oracle Secure Backup user](#).



See Also:

"[User Commands](#) (page 1-22)" for related commands

Prerequisites

If you must modify the attributes of any Oracle Secure Backup user, including yourself, then you must have the [modify administrative domain's configuration](#) (page 8-4) right. To modify only your own password and given name, then you must have the right to [modify own name and password](#) (page 8-6).

Syntax

`chuser::=`

```

chuser [ --class/-c userclass ]
[ --password/-p password | --querypassword/-q ]
[ --pwdlifetime ] [ --pwdgracetime ] [ --pwdreusetime ] [ --changepassword ]
[ --unixname/-U unix-user ] [ --unixgroup/-G unix-group ]
[ --adddomain/-d { windows-domain | * },windows-account[,windows-password] ]...
[ --rmdomain/-r { windows-domain | * } ] [ --ndmpuser/-N { yes | no } ]...
[ --email/-e emailaddr ] [ --givenname/-g givenname ]
[ --preauth/-h preauth-spec[,preauth-spec]... ]
[ --addpreauth/-H preauth-spec[,preauth-spec]... ]
[ --rmpreauth/-X preauth-spec[,preauth-spec]... ]
username...

```

Semantics

Refer to "[mkuser](#) (page 3-64)" for descriptions of `chuser` options not included in this section.

--password/-p *password*

Specifies a password for the Oracle Secure Backup user when logging in to an [administrative domain](#). The maximum character length that you can enter is 16 characters. If you do not specify a password, then the password is null. The minimum password length is determined by the `minuserpasswordlen` security policy. Its default value is 8 characters.

 **See Also:**

["minuserpasswordlen \(page 7-44\)"](#)

The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the Oracle Secure Backup user be prompted for the password.

--powlifetime

Specifies the lifetime of a user password, in number of days.

--pwdgracetime

Specifies the grace time of the password during which the user can continue using the current password even after it has expired.

--pwdreusetime

Specifies the time period after which a user password that was previously used can be reused.

--changepassword

Specifies that the user must change the current password during the next Oracle Secure Backup login.

 **Note:**

To modify Oracle Secure Backup users, you must be a member of a class that has this right enabled. See *Oracle Secure Backup Administrator's Guide* for details.

--adddomain/-d {*windows-domain* | *},*windows-account,windows-password*

Adds Windows domain information to the user account. If the domain is different from an existing domain in the user object, then `--adddomain` adds an entry for the additional domain. If the domain name in `--adddomain` is same as an existing domain in the user object, then `--adddomain` replaces the existing information. Refer to the `--domain` option of the [mkuser](#) (page 3-64) command for more information.

[Example 3-34](#) (page 3-68) describes how to create a user for the Windows domain.

--rmdomain/-r {*windows-domain* | *}

Removes a Windows domain.

--preauth/-h preauth-spec

Authorizes the specified Oracle Secure Backup user identity for the specified operating system user on the specified host. Refer to "[preauth-spec](#) (page 4-23)" for a description of the *preauth-spec* placeholder.

Specifying the `--preauth` option replaces any existing [preauthorization](#) data. You can reset the preauthorization for an Oracle Secure Backup user by specifying an empty string, for example, `--preauth ""`.

--addpreauth/-H preauth-spec

Adds preauthorization objects and preauthorizes Oracle Secure Backup access, but does not replace existing preauthorization data. You can add preauthorizations only if you have the `modify administrative domain configuration` right. Typically, only an Oracle Secure Backup user in the `admin` class has this right.

Refer to "[preauth-spec](#) (page 4-23)" for a description of the *preauth-spec* placeholder.

If you specify *os-username* as a Windows account name, then you must state the Windows domain name explicitly either as wild-card or a specific name. Duplicate preauthorizations are not permitted. Preauthorizations are duplicates if they have the same hostname, userid, and domain.

--rmpreauth/-X preauth-spec

Removes preauthorized access to the specified Oracle Secure Backup user from the specified host or operating system user. Preauthorization attributes, if specified, are ignored. Refer to "[preauth-spec](#) (page 4-23)" for a description of the *preauth-spec* placeholder.

You can remove preauthorizations only if you have the `modify administrative domain configuration` right. Typically, only an Oracle Secure Backup user in the `admin` class has this right.

username

Specifies the name of the Oracle Secure Backup user to be modified.

Example**Example 2-42 Changing an Oracle Secure Backup User**

This example creates Oracle Secure Backup user `bkpadmin`, reassigns this user to the `oracle` class, and then displays information about this user.

```
ob> mkuser bkpadmin --class admin --password "x45y" --givenname "lance" --unixname
bkpadmin --unixgroup "dba" --preauth osbsvr1:bkpadmin+rman+cmdline --ndmpuser no
--email bkpadmin@example.com
ob> chuser --class oracle bkpadmin
ob> lsuser --long bkpadmin
bkpadmin:
  Password:                (set)
  User class:              oracle
  Given name:              lance
  UNIX name:               bkpadmin
  UNIX group:              dba
  Windows domain/acct:    [none]
  NDMP server user:       no
  Email address:          bkpadmin@example.com
  UUID:                   5f437cd2-7a49-1027-8e8a-000cf1d9be50
  Preauthorized access:
    Hostname:              osbsvr1
    Username:              bkpadmin
    Windows domain:       [all]
```

```

RMAN enabled:      yes
Cmdline enabled:   yes

```

Example 2-43 Changing Password Settings for an Oracle Secure Backup User

This example modifies the password settings for the administrative Oracle Secure Backup user `dave01`, created in [Example 3-33](#) (page 3-68). The password change required setting for the user is set to `yes` and the password grace time is set to `disabled`. The example also demonstrates the user being prompted to change the current password during the next login.

```

ob> chuser --changepassword yes --pwdgracetime disabled dave01
ob> lsuser --long dave01
dave01:
  Password:                (set)
  Password last changed:   2012/10/30.02:33
  Password change required: yes
  Password lifetime:      80 days
  Password grace time:    disabled
  Password reuse time:    120 days
  User class:             admin
  Given name:             dave
  UNIX name:              [none]
  UNIX group:             [none]
  Windows domain/acct:    [none]
  NDMP server user:       no
  Email address:          [none]
  UUID:                   7395a468-04dd-1030-93a4-00163e527899
  Preauthorized access:
    Hostname:             brhost3
    Username:             rman
    Windows domain:      [all]
    RMAN enabled:        no
    Cmdline enabled:     yes
ob> logout
[johndoe@slc02qdv reliaty]$ obtool
Oracle Secure Backup 12.1.0.1
login: dave01
Password:
The password has expired; it must be changed
New password:
New password (again):

```

2.1.31 chvol

Purpose

Used to change [volume](#) attributes, including the [rotation policy](#) applied to the volume and its current [location](#).

See Also:

["Volume Rotation Commands \(page 1-22\)"](#)

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `chvol` command.

Usage Notes

If you specify a volume ID that matches multiple volumes in the Oracle Secure Backup volumes catalog, or if the specified volume belongs to a volume set, then Oracle Secure Backup asks which volume or volumes you want to modify.

The form of the response from Oracle Secure Backup depends on the kind of ambiguity it finds. Suppose you want to extend the expiration time on volume VOL000001:

```
obtool> chvol --retain forever -v VOL000001
```

Your selection matches the following volumes:

Volume ID	Barcode	Created
1 VOL000001	SF002463	01/11.04:24
2 VOL000001	SF004011	02/05.11:20
3 VOL000001	SF009774	02/23.01:31

Please select the volume(s) that you wish to modify: 1, 2, ..., a(ll), n(one), or q(uit) [a]:

In this first example, Oracle Secure Backup identifies three volumes with a volume ID matching VOL000001 and asks you which volume or volumes you want to modify. The default is all volumes.

To extend the expiration time on a different volume VOL000008:

```
obtool> chvol --retain forever -v VOL000008
```

The volume VOL000008 belongs to a volume set with the following members:

Volume ID	Barcode	Created
VOL000007	SF002463	01/11.04:24
VOL000008	SF004011	01/11.05:32
VOL000009	SF009774	01/11.07:13

Please select the volume(s) that you wish to modify: a(ll), n(one), or q(uit) [q]:

In this second example, Oracle Secure Backup identifies VOL000008 as a member of a volume set and asks you to modify all or none of its volumes. You cannot select individual members of the volume set. The default choice is quit.

Syntax

`chvol::=`

```
chvol
{ [ --rotationpolicy/-R policyname ] |
  [ --relocate/-M [ --nomovement/-n ] |
    [ --force/-f ] --tolocation locationname |
    [ --missing/-g { yes | no } ] |
    [ --notintransit/-O ] }
[ --duplicationpolicy/-D duplication_policy ]
[ --vsopt/-V { ignore | prompt | all } ]
[ --expiresat/-x date-time | --retain/-r duration ]
```

```
[ --status vol-status ]  
vol-spec [vol-spec]...
```

Semantics

--rotationpolicy/-R *policyname*

Changes the rotation policy assigned to the volume to *policyname*.

--relocate/-M --tolocation/-t *locationname*

Relocates the volume to the specified location.

A volume can be moved from one location in a rotation policy to another with this option. The specified location must be part of the currently assigned rotation policy for the volume. Use the `--rotationpolicy` option to assign a rotation policy to a volume. If you specify the same location for multiple volumes currently at the same location, then Oracle Secure Backup creates one media movement job for all of the volumes. Volumes specified in multiple `chvol --relocate` commands, however, are not merged into a single media movement job.

--relocate/-M --nomovement/-J --tolocation/-t *locationname*

Relocates the volume to the specified location without creating a media movement job for the relocation. The specified location must be part of the currently assigned rotation policy for the volume. Use the `--rotationpolicy` option to assign a rotation policy to a volume.

--relocate/-M --force/-f --tolocation/-t *locationname*

Relocates the volume to the specified location without the restriction that the location be part of the currently assigned rotation policy for the volume. If this location does not match the expected location for the volume, then the volume appears on the exception report.

--missing/-g {*yes* | *no*}

Marks the volume as missing (*yes*) so that a media movement job does not attempt to move it, or not missing (*no*).

--notintransit/-O

Marks the volume as having completed its journey from vault to robot. Oracle Secure Backup updates the current location of the volume and resets its *in-transit* flag.

--duplicationpolicy/-R *policyname*

Changes the duplication policy assigned to the volume to *policyname*. This option has no effect on volumes previously processed in a duplication scan. Specifying `--duplicationpolicy ""` sets the duplication policy to null.

--vsopt/-V [*ignore* | *prompt* | *all*]

Specifies the action to take if a specified volume belongs to a volume set.

The `ignore` option forces Oracle Secure Backup to ignore the volume set membership and change just the selected volume. The `prompt` option displays all volumes in the volume set and prompts you to select one or more volumes to change. The `all` option applies the change to all members of the volume set.

The default behavior is to ignore the volume set membership and change just the selected volume.

--expiresat/-x *date-time*

Changes the expiration times of all specified volumes to *date-time*, subject to the constraint that no expiration time may be reset to a time earlier than the current

expiration time. The expiration date must be applied to all volumes within the volume set.

See "[date-time](#) (page 4-9)" for more information on the *date-time* placeholder.

--retain/-r duration

Changes the expiration times of all specified volumes by adding duration to the creation time of each volume, subject to the constraint that no expiration time may be reset to a time earlier than the current expiration time.

See "[duration](#) (page 4-14)" for more information on the *duration* placeholder.

Note:

The expiration times generated by the `--expiresat/-x` and `--retain/-r` options are written to the volumes database. Changing the expiration time of a volume will only affect the expiration times of archives that are written to the tape after the expiration time is changed. If a catalog import is done of the tape, the database entry for the volume will contain the expiration time for the last archive that was successfully cataloged. Because the `chvol` command only allows increasing the expiration time, the expiration time for the volume will always be equal to or greater than the expiration time of the very first archive on the tape.

--status vol-status

Changes the availability status of the volume for Oracle Secure Backup backup and restore operations.

See "[vol-status](#) (page 4-31)" for more information on the status options available for volumes.

vol-spec...

The [volume ID](#) or [barcode](#) value of one or more volumes.

See "[vol-spec](#) (page 4-31)" for more information on the *vol-spec* placeholder.

Example

Example 2-44 Changing Volume Attributes

This example adds the rotation policy `rotpol` to the volume `VOL000001`. The `chvol` command also changes the location of this volume from the library `vlib1` to `lib1`.

```
ob> lsvol --library vlib1
Inventory of library vlib1:
  in   1:                volume RMAN-DEFAULT-000001, barcode
4c0d6eac2d28103b69500163e527899, 151528320 kb remaining, content manages reuse
  in   dte:              volume VOL000001, barcode e53b658a2d2710390a700163e527899,
153256704 kb remaining, lastse 2
```

```
ob> chvol --rotationpolicy rotpol --relocate --tolocation lib1 --vsopt prompt --
volume VOL000001
Your vol-spec, matched the following volume:
```

Volume ID	Barcode	Created
VOL000001	e53b658a2d2710390a700163e527899	11/11.01:52

```
Do you wish to modify this volume (y{es}, n(o), q(uit))? [y]: y
ob>
```

2.1.32 clean

Purpose

Use the `clean` command to clean a [tape drive](#).



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `clean` command.

Syntax

`clean::=`

```
clean [ --drive/-D drivename ] [ --force/-f ] [ --use/-u se-spec ]
```

Semantics

--drive/-D *drivename*

Specifies the name of the tape drive to clean. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--force/-f

Forces Oracle Secure Backup to clean the tape drive. If there is a tape loaded in the tape drive, then this option unloads the tape, loads the cleaning tape, cleans the tape drive, and then reloads the tape that was originally in the tape drive.

--use/-u *se-spec*

Specifies the number of a storage element containing a cleaning tape. If this option is omitted, then Oracle Secure Backup chooses a cleaning tape based on the setting of the `--cleanemptiest` option that you specified on the [mkdev](#) (page 3-6) command. Refer to "[se-spec](#) (page 4-27)" for a description of the `se-spec` placeholder.

Example

Example 2-45 Cleaning a Tape Drive

This example informs Oracle Secure Backup that you are inserting an unused cleaning tape into element 4 of [tape library](#) `lib1`. The example uses the cleaning tape in element 4 to clean tape drive `tape1`.

```
ob> insertvol --library lib1 clean --uses 0 --maxuses 3 4
ob> clean --drive tape1 --force --use 4
```

2.1.33 closedoor

Purpose

Use the `closedoor` command to close the import/export door of a [tape library](#). This command only works for libraries that support it.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `closedoor` command.

Syntax

```
closedoor::=
```

```
closedoor [ --library/-L libraryname ]
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library on which you want to close the door. If you do not specify a tape library name, then the [library](#) (page 5-3) variable must be set.

Example

Example 2-46 Closing a Library Door

This example closes the door of tape library `lib1`.

```
ob> closedoor --library lib1
```

2.1.34 cpinstance

Purpose

The `cpinstance` command creates a copy of a backup image instance from an existing backup image. Oracle Secure Backup creates a copy instance job that is scheduled for subsequent execution. This process is similar to how backup or restore jobs are created and scheduled.

Prerequisites

You must have the [modify any backup, regardless of its owner](#) (page 8-5) or [modify any backups owned by user](#) (page 8-5) class right to use the `cpinstance` command.

Usage Notes

If multiple copies of a backup image instance exist, then Oracle Secure Backup chooses the best one to use in the copy instance operation. Copying of multiple backup images is not supported when the backup image instances are located on different backup containers. All backup image instances must be located on the same disk pool or tape volume.

You can use the `cpinstance` command to create a new tape volume that contains backup image instances originating from several different volumes. This enables you to archive selected backups thereby creating a single volume on a larger-capacity tape media from a volume set consisting of multiple smaller-capacity tapes. This provides a much finer control over the individual backup image instances.

The blocking factor of the source backup image instance is the blocking factor used to write the instance to the destination device.

Copying Backup Image Instances and Backup Encryption

If the source backup image instance is not encrypted, then the backup image instance copy is also not encrypted. However, if the backup image instance is copied to a tape device that supports hardware encryption and you specify that the backup image instance copy must use hardware encryption, then the copy will be hardware encrypted.

If the source backup image instance is software encrypted, then the original encryption properties are used for the backup image instance copy. You cannot use hardware encryption for a source that has been software encrypted.

For tape devices, if the source backup image instance is hardware encrypted, then the copy uses hardware encrypted if it is written to tape devices that support hardware encryption. If the device does not support hardware encryption, then the backup image instance copy is not encrypted. Oracle Secure Backup uses the source encryption key for all backup image instances that are created from that source. This is applicable for both transient and transparent encryption. If the source backup image instance is encrypted with a passphrase (transient encryption), then you must provide the associated passphrase when prompted by the copy instance job.

Copying Backup Image Instances to a Cloud Storage Device

- The source backup image instance must be software encrypted in order to copy it to a cloud storage device.
- A backup image instance located on a cloud container cannot be copied to a disk pool device or tape volume.
- A backup image instance located on a cloud object container can be copied or migrated to a cloud archive container by using the `--cloudcopy` option.
- A backup image instance located on a cloud archive container cannot be copied to a cloud object container.

Syntax

```
cpinstance::=
```

```
cpinstance
[--priority/-p schedule-priority] [--at/-a date-time]
[--family/-f media-family-name] [--quiet/-q]
[--waitfor/-W duration]
```

```
[--restrict/-r restriction[,restriction]...]
[--encryption/-e encryption] [--algorithm/-L enc-algorithm]
[--storekey/-s] [--migrate/-m] [--cloudcopy/-c]
{ [--uuid/-u backup-image-uuid]... | backup-image-name... }
```

Semantics

--priority/-p *schedule-priority*

Specifies the priority to be assigned to the copy instance job.

--at/-a *date-time*

Specifies the time at which the copy instance job must be run. Refer to "[date-time](#) (page 4-9)" for information about the `date-time` placeholder.

--family/-f *media-family-name*

Specifies the name of the media family that must be associated with the new backup image instance.

If the source backup image instance resides on a content-managed tape volume, then the media family specified by the `--family` option must also be content-managed.

--quiet/-q

Specifies that status messages about the copy instance job must not be displayed. No message is displayed when the copy instance job is sent to the scheduler.

--waitfor/-W *duration*

Specifies the amount of time that Oracle Secure Backup waits for the copy instance job to complete. After the specified duration is exceeded, Oracle Secure Backup exits from `obtool`.

See "[duration](#) (page 4-14)" for information about the `duration` placeholder.

--restrict/-r *restriction*

Restricts the copy instance job to the specified tape devices or disk pools. Refer to "[restriction](#) (page 4-25)" for a description of the `restriction` placeholder.

--encryption/-e *encryption*

Specifies whether to use encryption when creating the new backup image instance. Possible values to set are:

- `yes`
Use encryption for this copy instance job. The encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `no`
Do not use encryption for this copy instance job. This is the default. If the global backup policy or client backup policy is set to required, then those policies supersede this value and encryption is used. If encryption is used, then the encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `forcedoff`
Do not use encryption for this backup job, regardless of global or client backup policy

- transient

Encrypt backups created with this copy instance job using a transient passphrase (supplied with the `--passphrase` or `--querypassphrase` options to backup), and the encryption algorithm specified by the global encryption policy setting.

See "[Copying Backup Image Instances and Backup Encryption](#) (page 2-81)".

--algorithm/-L *enc-algorithm*

Specifies the encryption algorithm used to create the new instance. Set one of the following values for the encryption algorithm: AES128, AES192, or AES256.

--migrate/-m

Deletes the source backup image instance associated with the specified backup image after the new backup image instance has been created. If more than one backup image instances exist, the `cpinstance` command fails. This option is not applicable when the source image instance resides on a tape volume.

--cloudcopy/-c

This option is required when you copy or migrate an instance from an Oracle Cloud object storage container to an Oracle Cloud archive storage container.

--storekey/-s

Specifies that the transient passphrase used to encrypt this backup image instance must be added to the appropriate key stores. The default behavior is that transient passphrases are not stored in any key store.

--uuid/-u *backup-image-uuid*]... | *backup-image-name*...

Specifies either the UUID or the name of the backup image that must be copied to a different backup container.

Examples

This example creates a copy instance job that copies the backup image instance associated with the backup image `fs_bk`. The job is scheduled to run at the time specified by the `--at` option and the backup image instance is created on the disk pool `dp1`. The backup image instance copy is encrypted.

```
ob> cpinstance --at 2013/04/24.20:30:00 --restrict dp2 --encryption yes fs_bk
Info: copy instance for fs_bk.1 submitted; job id is admin/17.
```

2.1.35 ctld daemon

Purpose

Use the `ctld daemon` command to control the operation of Oracle Secure Backup daemons.

See Also:

"[Daemon Commands](#) (page 1-13)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `ctldaemon` command.

Syntax 1

Use the following syntax to suspend or resume scheduling.

```
ctldaemon::=
ctldaemon --command/-c { suspend | resume }
```

Syntax 2

Use the following syntax to send a command to one or more daemons.

```
ctldaemon::=
ctldaemon --command/-c { dump | reinitialize | debugon | debugoff }
[ --host/-h hostname[,hostname]... ] [ daemon-id ]...
```

Semantics

--command/-c

Enables you to temporarily suspend and later resume the obscheduled daemon (Syntax 1). You can suspend obscheduled for troubleshooting purposes.

--command/-c

Enables you to send a control command to an Oracle Secure Backup daemon (Syntax 2). [Table 2-2](#) (page 2-84) lists the `--command` values.

Value	Meaning
dump	Directs the daemon to dump internal state information to its log file.
reinitialize	Directs the daemon to reread configuration data.
debugon	Directs the daemon to generate extra debugging information to its log file.
debugoff	Cancels debug mode. This is the default state.

--host/-h *hostname*

Specifies the name of a host on which the daemon is running. If this option is omitted, then the local host is assumed.

daemon-id

Identifies an Oracle Secure Backup daemon, either a process id (PID) or service name. Possible service names are `observed`, `obscheduled`, `obrobotd`, and `obixd`.

Example

Example 2-47 Suspending the obscheduled Daemon

This example determines whether the `obscheduled` daemon is in a normal state and then suspends it.

```
ob> lsdaemon obscheduled
Process Daemon/          Listen
   ID Service          State          port  Qualifier
```

```

9436 obscheduled normal 42130
ob> ctlddaemon --command suspend
ob> lsdaemon obscheduled
Process Daemon/ Listen
   ID Service      State      port Qualifier
9436 obscheduled suspended 42130

```

2.1.36 discoverdev

Purpose

Use the `discoverdev` command to detect and configure tape devices that are attached to media servers in the administrative domain. You can discover and configure all tape devices in the administrative domain or tape devices attached to specific media servers. The media servers can be attached through [Network Data Management Protocol \(NDMP\)](#) or have the Oracle Secure Backup software installed.

This command also updates existing tape device configuration in case a tape device has already been discovered by more than one media server. Based on this information, `discoverdev` automatically updates [tape device](#) configuration for the [administrative domain](#).

See Also:

"[Device Commands](#) (page 1-15)" for related commands

Note:

The `discoverdev` command is not available on the HP-UX platform.

Oracle Secure Backup detects the following kinds of changes during device discovery:

- Tape devices that were not previously configured but have appeared
For each such tape device, Oracle Secure Backup can create a tape device with a temporarily-assigned name and configures a tape device [attachment](#) for it.
- Tape devices that were previously configured for which an attachment has appeared from another media server.
Oracle Secure Backup adds an attachment to each existing tape device configuration.
- Tape devices that were previously configured for which an attachment has disappeared.
Oracle Secure Backup displays information about the device with a missing attachment.

 **Note:**

The `discoverdev` command does not discover and configure ACSLS libraries and devices. You must use the `mkdev` command to configure ACSLS libraries.

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `discoverdev` command.

While working on Linux 64-bit platforms, you must be familiar with the rules of the kernel's device manager in order to configure persistent tape devices that use the SCSI Generic driver.

Usage Notes

You can run the `discoverdev` command from the administrative server or any media server.

The `discoverdev` command creates a device object containing the attachment information for each device that it discovers and configures. The state of the discovered device depends on the value of the [discovereddevicestate](#) (page 7-15) policy. If this policy is set to `in service`, then the created device object is available for use by Oracle Secure Backup after the initial configuration. When the device being configured is a tape drive, `discoverdev` configures the DTE number automatically for this device.

Oracle Secure Backup assigns default names to tape devices that are configured using `discoverdev`. You can rename these devices using the `rmdev` command.

Device Discovery and SCSI Persistent Binding

By default, Oracle Secure Backup discovers and configures tape devices that are located in the `/dev` directory. On Linux 64-bit platforms, if you use persistent binding to set up SCSI tape devices, then the device files may not be available in the default directory. In such cases, use the `OB_DEVICE_SEARCH_PATH` environment variable to specify the location of the persistent devices so that Oracle Secure Backup can discover and configure these devices. This environment variable must be provided in the `/etc/init.d/observed` or `/etc/rc.d/init.d/functions` script with the value of the directory containing tape persistent device links, such as `OB_DEVICE_SEARCH_PATH=/date/tape/by-id`. The `observed` service must be restarted after this variable is set. The `OB_DEVICE_SEARCH_PATH` cannot be used in RMAN commands or in `obtool` commands.

If you are using `<OSB_INSTALL_DIR>/etc/observed` directly at command line, then you must set the `OB_DEVICE_SEARCH_PATH` environment variable in that particular command shell.

Multiple Hosts Connected to the Same Tape Device

Oracle Secure Backup detects multiple hosts connected to the same tape device by comparing the serial numbers reported by the operating system. If a discovered tape device is accessible by its serial number, then Oracle Secure Backup updates the existing tape device with the newly configured attachment from each host.

Media Servers with Existing Tape Device Configurations

If you run the `discoverdev` command with the `--configure` option for a media server that contains configured tape devices, then Oracle Secure Backup does not reconfigure these devices.

Syntax

`discoverdev::=`

```
discoverdev { --host/-h hostname }... | --accesstype/-a {all | ndmp | ob}}  
[ --configure/-c [--interactive/-i]] [--verbose/-v]  
[ --quiet/-q ] [ --missing/-m ]
```

Semantics

--host *hostname*

Identifies the host name on which the discovery is to take place. The host specified must be a media server. Use a comma-delimited list to specify multiple hosts.

--accesstype/-a {all | ndmp | ob}

Specifies the type of hosts for which discovery must be performed. Set one of the following values for `accesstype`:

- **all**: Devices attached to all media servers in the administrative domain are discovered.
- **ndmp**: Only devices attached to media servers that are accessed using NDMP are discovered.
- **ob**: Only devices attached to media servers accessed using Oracle Secure Backup are discovered.

--configure/-c

Lists information about the devices that are attached to the media server and then creates device objects for each device automatically. If you omit this option, Oracle Secure Backup only displays the details about attached tape devices but does not configure them.

You cannot use this option with the `--missing/-m` option.

--interactive/-i

Configures discovered tape devices interactively. After each tape device is discovered, a prompt is displayed asking if you want to create a corresponding device object for this tape device. The tape device is configured only after user confirmation.

--quiet/-q

Suppresses the display of the discovery tape device status.

--missing/-m

Reports tape devices that were previously configured but are no longer found by the `discoverdev` command. If the attachment for a previously configured tape device is missing, Oracle Secure Backup does not remove the tape device configuration.

You cannot use this option with the `--configure/-c` option.

--verbose/-v

Provides verbose output describing the tape devices discovered.

Example

Example 2-48 Discovering Devices Attached to an Oracle Secure Backup Host

This example discovers devices that are attached to the host `storabck18`. It lists information about the devices including the device name, device type, serial number, and attachment.

```
ob> discoverdev -h storabck18 -c -v
2997a776-14c7-1031-a7be-e26800005003:
  Host: storabck18
  Device type: Library
  Model: STK SL150
  Serial number: 464970G+1333SY1401
  Device name: storabck18_lib_1
  Existing device: No
  Attachment new:
    Host: storabck18
    Raw device: /dev/scsi/changer/c2t500104F000D14F89d1
29ba7ec2-14c7-1031-a7be-e26800005003:
  Host: storabck18
  Device type: Tape
  Model: HP Ultrium 5-SCSI
  Serial number: HU1328WGF6
  Device name: storabck18_tape_1
  Existing device: No
  Attachment new:
    Host: storabck18
    Raw device: /dev/scsi/sequential/c2t500104F000D14F89d0
29ba8a34-14c7-1031-a7be-e26800005003:
  Host: storabck18
  Device type: Tape
  Model: HP Ultrium 5-SCSI
  Serial number: HU1327WEYJ
  Device name: storabck18_tape_2
  Existing device: No
  Attachment new:
    Host: storabck18
    Raw device: /dev/scsi/sequential/c2t500104F000D14F8Cd0
```

2.1.37 dumpdev

Purpose

Use the `dumpdev` command to display [tape device](#) errors logged by Oracle Secure Backup.

Error logs reside on the [administrative server](#) in the `admin/log/device` subdirectory path of the [Oracle Secure Backup home](#).



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `dumpdev` command.

Syntax

```
dumpdev::=
```

```
dumpdev [ --since/-s date-time ] [ --clear/-c [ --nq ] [ --nd ] ]  
{ --dumpfile/-f path... | devicename... }
```

Semantics

--since/-s *date-time*

Limits the display to those errors that have occurred since *date-time*. Refer to "[date-time](#) (page 4-9)" for the *date-time* placeholder.

--clear/-c

Deletes the error log after it has been displayed. You are prompted before each log is deleted.

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--nd

Suppresses the display of the error log. This is useful to clear the error log without displaying it.

--dumpfile/-f *path*

Specifies a path name of the file to be dumped. This option is useful if you have saved a tape device error log file to a file that `dumpdev` would not normally find.

devicename

Dumps the error log file associated with *devicename*. Refer to "[devicename](#) (page 4-12)" for the rules governing tape device names.

Example

Example 2-49 Dumping the Error Log for a Tape Drive

This example dumps the error log for a [tape drive](#) named `10h_tapel`.

```
ob> dumpdev 10h_tapel
```

```
Oracle Secure Backup hardware error log for "10h_tapel", version 1  
  EXABYTE EXB-85058SQANXR1, prom/firmware id 07J0, serial number 06667256  
Tue Jan 10, 2013 at 16:52:26.354 (Eastern Daylight Time) devtype: 14  
  obexec: mchamber-pc://./obt0, args to wst__exec: handle=0x0  
  accessed via host mchamber-pc: Windows_NT 5.1  
  op=16 (eod), buf=0x00, count=1 (0x1), parm=0x00  
  cdb: 11 03 00 00 00 00 space, cnt=0 to eod  
  sense data:  
    70 00 03 FF FF FF FF 15 00 00 00 00 14 00 00 00  
    00 00 03 00 00 00 02 56 D8 2A 03 00 00  
    ec=0, sk=media err, asc=14, ascq=0  
    error is: unrecoverable error
```

```

flags: (none)
returned status: code=unrecoverable error,
resid=0 (0x0), checks=0x0 [ ]

```

2.1.38 dupvol

Purpose

Use the `dupvol` command to duplicate a [volume](#) on demand.

The write window for the original volume is closed when it is duplicated. The write window for the newly created duplicate is also closed unless you choose the volume migration option.

If the duplicated volume was itself a duplicate, then the original volume of the on-demand duplicate is set to the original volume of the duplicated volume.

If an on-demand duplication job is canceled, then no further attempts are made to create the duplicate, and the write window for the original volume is reopened.



See Also:

"[Duplication on Demand Commands](#) (page 1-15)" for related commands

Prerequisites

Two tape drives are required to perform duplication. You must have the right to [manage devices and change device state](#) (page 8-5) to use the `dupvol` command. The size of the destination volume used for duplication must be greater than or equal to the size of the source volume.

Usage Notes

If you specify a volume ID that matches multiple volumes in the Oracle Secure Backup volumes catalog, then Oracle Secure Backup asks which volume or volumes you want to duplicate. You can select one or more of the volumes, all of them, or none of them. The default selection is all volumes.



See Also:

"[chvol](#) (page 2-75)" for a pair of examples illustrating volume ID matching

Syntax

`dupvol::=`

```

dupvol
{ --family/-f media-family }
[ --migrate/-m { yes | no } ] [ --priority/-p schedule-priority ]
[ --quiet/-q ] [ --restrict/-r restriction[,restriction]... ]
[--waitfor/-W duration]
{ --volume/-v vid } [ --tag/-t tag[,tag]... ]

```

Semantics

--family/-f *media-family*

Specifies the [media family](#) to be used to create the duplicate volume. Each media family specified must match the retention mode (either time or content managed) of the [original volume](#).

--migrate/-m

Specifies that the volume must be migrated. If this option is set to `yes`, then only one restriction can be specified. The original volume is marked as expired. Only one volume can be created by the process of migration.

--priority/-p *schedule-priority*

Specifies a numeric priority greater than zero assigned by the [Oracle Secure Backup user](#) to a scheduled duplication. The lower this value, the higher Oracle Secure Backup considers the priority.

--quiet/-q

Does not display job ID or status information when a duplication job is dispatched to the [scheduler](#).

--restrict/-r *restriction*

Defines a [tape device](#), host, or tape device/host pair in the [administrative domain](#) that identifies one or more acceptable tape devices for the duplication. Refer to "[restriction](#) (page 4-25)" for a description of the *restriction* placeholder.

In the absence of a tape device restriction, the duplication runs on the first available tape device. You can specify the restriction as a tape device name (as assigned by [mkdev](#) (page 3-6) or [chdev](#) (page 2-30)) or as an [attachment](#) for a tape device.

--waitfor/-W *duration*

Specifies the amount of time that Oracle Secure Backup waits for the volume duplication to complete. After the specified time duration is exceeded, Oracle Secure Backup exits from obtool.

See [duration](#) (page 4-14) for more information on the *duration* placeholder.

--volume/-v *vid*

Specifies the volume to be duplicated.

--tag/-t *tag*

Specifies the volume to be duplicated based on the [volume tag](#) ([barcode](#)).

Example

Example 2-50 Duplicating a Volume

This example displays how VOL000001 is duplicated using the OSB-CATALOG-MF media family. This volume will not be migrated and is restricted to the tape device vt1.

```
ob> dupvol --family OSB-CATALOG-MF --migrate no --priority 100 --restrict vt1 --
volume VOL000001
Info: volume duplication request 1 (volume VOL000001) submitted; job id is admin/4.
```

2.1.39 edds

Purpose

Use the `edds` command to edit an existing [dataset file](#). You can replace the entire contents of a file in one of these ways:

- Using the `--input/-i` option on the command line, which enables you to input the file on the command line.
- Omitting the `--input/-i` option, which opens a default editor window where you can input data and make changes in the editor. You apply the changes when you exit the editor. The default editor is defined by your `EDITOR` environment variable.



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `edds` command.

Syntax

```
edds::=
```

```
edds [ --nq ] [ --nocheck/-C ] [ --input/-i ] dataset-file-name
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--nocheck/-C

Disables syntactic checking of a dataset file for errors.

--input/-i

Enables you to input or replace the entire contents of a dataset file.

dataset-file-name

Specifies the name of a dataset file. Refer to "[dataset-file-name](#) (page 4-7)" for a descriptions of the `dataset-file-name` placeholder.

Example

Example 2-51 Checking a File for Syntax

This example opens a dataset file that contains bad syntax, replaces its contents with different syntax, and then checks its syntax.

```
ob> catds badsyntax.ds
iclude host brhost2
```

```
ob> edds --nq --input badsyntax.ds
Input the replacement dataset contents. Terminate with an EOF or a line
containing just a dot (".").
include host brhost2
include path /home
.
ob> catds badsyntax.ds
include host brhost2
include path /home
ob> chkds badsyntax.ds
```

2.1.40 exit

Purpose

Use the `exit` command to exit `obtool`. This command is functionally identical to the [quit](#) (page 3-79) command.



See Also:

"[Miscellaneous Commands](#) (page 1-18)" for related commands

Syntax

```
quit::=
exit [ --force/-f ]
```

Semantics

--force/-f

Exits `obtool` even if there are pending backup or restore requests. Specifying `--force` means that pending backup and restore requests are lost.

Normally, you cannot exit `obtool` when there are pending requests. You should submit pending requests to the [scheduler](#) by specifying `--go` on the [backup](#) (page 2-4) or [restore](#) (page 3-99) commands.

Example

Example 2-52 Exiting obtool

This command uses the `--force` option to exit `obtool` when a [backup job](#) is pending.

```
ob> backup --dataset fullbackup.ds
ob> exit
Error: one or more backup requests are pending. Use "quit --force" to
quit now, or send the requests to the scheduler with "backup --go".
ob> exit --force
```

2.1.41 exportvol

Purpose

Use the `exportvol` command to move one or more volumes to the import/export mechanism for removal from the [tape library](#). Typically, you export volumes in bulk. This command is supported only for libraries that have import/export slots.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `exportvol` command.

Syntax 1

Use the following syntax to export a [volume](#) from a tape library or standalone [tape drive](#).

```
exportvol::=
```

```
exportvol [ --library/-L libraryname | --drive/-D drivename ]  
{ vol-range | se-range }
```

Semantics 1

Use the following semantics to export a volume from a tape library or standalone tape drive.

--library/-L *libraryname*

Specifies the name of the tape library from which you want to export volumes. If a tape library is specified, then there are no limitations placed on the [storage elements](#) to be exported. If there are an insufficient number of vacant import/export elements to fulfill the request, then `obtool` reports that the command could not be fully processed. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D *drivename*

Specifies the name of a tape drive in the tape library from which you want to export volumes. If a tape drive is specified, then all of the elements must belong to the use list of the tape drive. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

vol-range

Specifies the volumes to be exported. Refer to "[vol-range](#) (page 4-30)" for a description of the `vol-range` placeholder.

se-range

Specifies the storage elements containing the volumes to be exported. Refer to "[se-range](#) (page 4-27)" for a description of the *se-range* placeholder.

Syntax 2

Use the following syntax to export a volume from an ACS tape library.

```
exportvol::=
exportvol { vol-range | se-range } cap_devicename
```

Semantics 2

Use the following semantics to export a volume from an ACS tape library.

Manual [operator](#) intervention is required to remove the volume from the cartridge access port after an export operation is finished. If an amount of time greater than the policy setting `maxacsidlejectwaittime` passes without such manual operator intervention, then the eject operation is canceled although the cartridges are still located in the cartridge access port. If you find that not all volumes are moving to the cartridge access port before this time period expires, then increase `maxacsejectwaittime`.

vol-range

Specifies the volumes to be exported. Refer to "[vol-range](#) (page 4-30)" for a description of the *vol-range* placeholder.

se-range

Specifies the storage elements containing the volumes to be exported. Refer to "[se-range](#) (page 4-27)" for a description of the *se-range* placeholder.

cap_devicename

This option is available only when you are exporting a volume from an ACS tape library. It defines which ACS cartridge access port to export the volume to.

Example**Example 2-53 Exporting a Volume**

This example exports volume `VOL000003`. Note that the sample output has been reformatted to fit on the page.

```
ob> lsvol --drive tape2 --long
Inventory of library lib2:
  in  mte:          vacant
* in  1:            volume VOL000003, barcode DEV423, oid 111, 47711360 kb
                        remaining
* in  2:            vacant
* in  3:            vacant
* in  4:            vacant
  in  iee1:         vacant
  in  iee2:         vacant
  in  iee3:         vacant
  in  dte:          vacant

*: in use list
ob> exportvol --library lib2 --volume VOL000003
ob> lsvol --drive tape2 --long
Inventory of library lib2:
```

```

    in   mte:          vacant
* in   1:             vacant
* in   2:             vacant
* in   3:             vacant
* in   4:             vacant
    in   iee1:        volume VOL000003, barcode DEV423, oid 111, 47711360 kb
                                remaining, last se 1

    in   iee2:        vacant
    in   iee3:        vacant
    in   dte:         vacant

*: in use list

```

2.1.42 extractvol

Purpose

Use the `extractvol` command to notify Oracle Secure Backup that you have manually removed or are removing one or more volumes from a specified [tape library](#). You can specify the source of volumes you are extracting.

Note that you are not required to use the `extractvol` command if you issue the [inventory](#) (page 2-108) command after removing the volumes.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `extractvol` command.

Syntax

```
extractvol::=
```

```
extractvol [ --library/-L libraryname | --drive/-D drivename ]
{ vol-range | se-range }
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library from which you want to extract volumes. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D *drivename*

Specifies the name of a [tape drive](#) in the tape library from which you want to extract volumes. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

vol-range

Specifies the volumes to be extracted. Refer to "[vol-range \(page 4-30\)](#)" for a description of the `vol-range` placeholder. Run the `lsvol` (page 2-182) command to display volume information.

se-range

Specifies a range of [storage elements](#) from which volumes are to be extracted. Refer to "[se-range \(page 4-27\)](#)" for a description of the `se-range` placeholder.

Example**Example 2-54 Extracting a Volume**

This example notifies Oracle Secure Backup that the volume in storage element 1 of tape library lib1 has been manually removed. Note that the sample `lsvol` (page 2-182) output has been reformatted to fit on the page.

```
ob> lsvol --library lib1
Inventory of library lib1:
  in  1:          volume VOL000002, barcode ADE201, 47711424 kb remaining
  in  2:          volume VOL000001, barcode ADE203, 48359360 kb remaining
  in  dte:        volume RMAN-DEFAULT-000002, barcode ADE202, 47773408 kb
                    remaining, content manages reuse, lastse 3

ob> extractvol --library lib1 1
ob> lsvol --library lib1
Inventory of library lib1:
  in  1:          vacant
  in  2:          volume VOL000001, barcode ADE201, 48359360 kb remaining
  in  dte:        volume RMAN-DEFAULT-000002, barcode ADE202, 47773408 kb
                    remaining, content manages reuse, lastse 3
```

2.1.43 find

Purpose

Use the `find` command to search for selected files and directories while browsing the Backup Catalog.

Prerequisites

The [rights](#) needed to run the `find` command depend on the [browse backup catalogs with this access](#) (page 8-3) setting for the [class](#).

Syntax

```
find ::=
find [--long/-l | --count/-n]
[--host/-h hostname [,hostname]...]
[--ignorecase/-i]
[--max/-m max-entries ]
[--select/-s data-selector ]
[--type/-t {file | dir}]
[--container/-c backup-container]
[--ctype/-y {tape | disk} ]
[--path/-p frompath] [--startat/-S]
[--viewmode/-v viewmode]
name-to-search
```

Semantics

--long/-l

Displays additional information, like the volume id, backup id, and file number, for each entry in the output.

--count/-n

Returns a count of the number of files found in the backup catalog given the search criteria.

--host/-h *hostname*

Specifies the host on which the catalog search is performed. Multiple hosts can be specified through a comma-separated list.

--ignorecase/-i

Specifies that the search made on the entire catalog ignores the case, lowercase or uppercase, of the entries. This condition is applied on the `name to be searched` option.

--max/-m *max-entries*

Specifies that entries in the search output are restricted to the maximum entries selected with this option. If the output contains fewer entries than the specified limit, then all entries are displayed. If the output contains more entries than the specified limit, the result is trimmed. By default, the output lists all entries.

--select/-s *data selector*

Specifies the Oracle Secure Backup catalog data that applies to an operation. Refer to "[data-selector](#) (page 4-6)" for the `data-selector` placeholder.

--type/-t {*file* | *dir*}

Displays the type of output specified in this option. Use `file` to list only file entries. Use `dir` to list only directories. By default, both files and directories are listed.

--container/-c *backup-container*

Searches for files contained on the specified container, tape volume or disk pool, with the `container-spec`. `container-spec` is the name of a disk pool or a volume ID. See "[backup-container](#) (page 4-4)" for more information on containers.

--ctype/-y {*tape* | *disk*}

Searches for files that are stored on the specified backup container. Use `tape` to display backup image instances stored on tape devices and `disk` to display backup image instances stored on disk pools. By default, `find` searches for files stored on all backup containers.

--path/-p

Specifies the path from where the search begins. The result displayed is relative to the provided path. [Oracle Secure Backup wildcard pattern matching](#) is not supported while specifying the path.

--viewmode/-v *viewmode*

Specifies the mode in which to view directory contents in the Oracle Secure Backup catalog. The `find` command remains in viewmode until you change it to a different setting.

Valid values for viewmode are as follows:

- `exact` makes visible only those directory entries that match the data selector and are present in the current path.
- `inclusive` makes visible all entries regardless of the current data selector (default).
- `specific` makes visible all entries that match the specified data selector.

name-to-search

Specifies the name of the file or directory to be searched in the catalog. [Oracle Secure Backup wildcard pattern matching](#) is supported.

Examples**Example 2-55 Finding Backup Entries on a Host**

This example uses the `find` command to list entries in the `/scratch` directory on `brhost2`. The path for the backup entries is provided for the specified host. [Oracle Secure Backup wildcard pattern matching](#) is used as the `*` indicates that backup entries within all folders within the `/scratch` directory must be listed. The specified data selector `all` lists all backup entries from the given path.

```
ob> find -h brhost2 -p /scratch * -s all -l
VOL000001,brhost2: /scratch/osb_test/osb_ds
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test/osb_ds
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test/osb_ds/tmp
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test/osb_ds
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test
Host:          brhost2
Name:          /scratch/osb_test/osb_ds
Last Modified: 2012/12/07.01:59
Size:         0
User/Group:   johndoe.dba
Container:    VOL000001
Backup ID:    11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
File No:     12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2
Section No:  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1
```

Example 2-56 Finding a Type of Entry on a Host

This example uses the `find` command to list only directory backup entries on `brhost2`. The example uses Oracle Secure Backup wildcard pattern matching to list all backed up directories under the `/scratch` directory.

```
ob> find -h brhost2 -t dir -p /scratch *
VOL000001,brhost2: /scratch/osb_test
VOL000001,brhost2: /scratch/osb_test/osb_ds
```

Example 2-57 Finding Backups Using the Hostname

This example uses the `find` command to list backups on the host `obsvr1`.

```
ob> find --host obsvr1 backup
new-obsvr1-mf-000001,obsvr1: /usr/local/oracle/backup
```

2.1.44 id

Purpose

Use the `id` command to display the name of the currently logged in [Oracle Secure Backup user](#).



See Also:

"[Miscellaneous Commands](#) (page 1-18)" for related commands

Prerequisites

No [rights](#) are required to run the `id` command.

Syntax

```
id::=
```

```
id [ --long/-l ]
```

Semantics

--long/-l

Displays the Oracle Secure Backup user and its [class](#). By default `id` displays only the class.

Example

Example 2-58 Displaying the Current User

This example displays the current Oracle Secure Backup user, logs out, logs in again as a different Oracle Secure Backup user, and then displays current user information.

```
ob> id --long
user: admin, class: admin
ob> lsuser
admin          admin
sbt            admin
tadmin        admin
ob> logout
% obtool
Oracle Secure Backup 12.2.0.1.0
login: sbt
ob> id
sbt
```

2.1.45 identifyvol

Purpose

Use the `identifyvol` command to load a specified [volume](#) into a [tape drive](#), read its [volume label](#), and return the volume to its original storage element.

This command is useful if an [inventory](#) (page 2-108) command displays an invalid volume state such as `occupied`, or if you have a valid tape but do not know its contents. If a tape is not new or unlabeled, then you can use `identifyvol` to populate the inventory with the volume contents.

 **See Also:**

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `identifyvol` command.

Syntax

`identifyvol::=`

```
identifyvol [ --drive/-D drivename ] [ --import/-i ]  
[ --obtaropt/-o obtar-option ]... [ se-range ]
```

Semantics

--drive/-D *drivename*

Specifies the name of the tape drive to be used for identifying the volumes. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--import/-i

Reads each [backup image label](#) on the specified volumes. By default `identifyvol` only reads the first label on the volume. You can specify this option to update the volumes [catalog](#) in an [administrative domain](#) with information about tapes generated in other domains.

`identifyvol --import` does not catalog the contents of the backup image instances on the volume, but it lists out the backup image instance labels of all the file sections. For quicker importing of volume information and cataloging of backup catalog data, use the [catalog](#) (page 2-15) command.

[Example B-16](#) (page B-13) shows how you can catalog the contents of a backup image instance using [obtar](#).

--obtaropt/-o *obtar-option*

Specifies `obtar` options that are passed to `obtar` when the volumes are read. For example `-J` enables debug mode and provides more details in backup and restore transcripts. See "[obtar Options](#) (page B-14)" for details on `obtar` options.

 **Note:**

`obtool --import` translates internally to `obtar --zz`. Thus, if you specify the `--import` option, then you cannot also use `--obtaropt` to specify options used in the `obtar -c`, `-x`, or `-t` modes.

se-range

Specifies a range of storage elements containing the volumes to be identified. If *se-range* is omitted, then the volume currently loaded in the specified tape drive is identified. Refer to "se-range (page 4-27)" for a description of the *se-range* placeholder.

Example

This example loads the volumes in storage elements 1 and 3 into tape drive `tape1` and identifies them.

Example 2-59 Identifying Volumes

```
ob> lsvol --library lib1
Inventory of library lib1:
  in  1:          occupied
  in  3:          occupied
ob> identifyvol --drive tape1 1,3
```

Example 2-60 Displaying Backup Image Labels

```
ob> identifyvol --drive drv1 1,3
ob>
ob> identifyvol --import --drive drv1 1,3
Seq Volume          Volume Archive   Client   Backup   Archive Create
#  ID              Tag      File Sect Host      Level    Date & Time
1  RMAN-DEFAULT-000001 NNH024  1 1 D    localhost 0        2010/07/28 15:40:17
1  RMAN-DEFAULT-000001 NNH024  2 1 D    localhost 0        2010/07/28 15:51:04
1  RMAN-DEFAULT-000001 NNH024  3 1 D    localhost 0        2010/07/28 15:51:58
1  RMAN-DEFAULT-000001 NNH024  4 1 D    localhost 0        2010/07/28 16:15:42
End of volume set.
Seq Volume          Volume Archive   Client   Backup   Archive Create
#  ID              Tag      File Sect Host      Level    Date & Time
1  my-medfam-000002   000051  1 1      localhost 0        2010/07/28 16:31:31
End of volume set.
```

2.1.46 importvol

Purpose

Use the `importvol` command to move one or more volumes from the import/export mechanism of a [tape library](#) to [storage elements](#). This command is supported only for libraries that have import/export slots.

The `importvol` command differs from the [movevol](#) (page 3-71) command in the following ways:

- The tape library manager determines the destination storage elements to be used.
- Tapes can be identified during the move.
- A single command can move multiple tapes.

**See Also:**

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `importvol` command.

Usage Notes

If the library to which the `importvol` command is directed has an enabled and functioning barcode reader, then Oracle Secure Backup does not allow specification of the `unlabeled` option. Instead, the barcodes on the volumes being imported are read and used to attempt a lookup in the volumes database.

If a matching record is found in the database, then that record is associated with the target storage element. If the barcode is not found in the database, then a scratch record is created and the state of the associated volume is marked `unknown`.

Syntax

`importvol::=`

```
importvol [ --library/-L libraryname | --drive/-D drivename ]
[ --identify/-i | --import/-m | --unlabeled/-u ]
[ clean --uses/-U n --maxuses/-M n ]
[ --obtaropt/-o obtar-option ]...
iee-range
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library into which tapes are to be imported. If a tape library is specified, then all empty storage elements in the tape library are valid destinations. If there are insufficient destinations to fulfill the request, then `obtool` reports that the command could not be fully processed.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D *drivename*

Specifies the name of a tape drive in the tape library into which tapes are to be imported. If a tape drive is specified, then valid destinations are limited to the storage elements in the use list of that tape drive.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--identify/-i

Reads the [volume ID](#) on each [volume](#). This option is equivalent to running the `identifyvol` (page 2-100) command. This option requires specification of a tape drive.

--import/-m

Reads each [backup image label](#) on each volume. You can use this option to import volume information and archive section information from a different [administrative domain](#). This option requires specification of a tape drive.

This option imports information regarding the tape into volumes and archive catalogs for the specified tape drive.

To import volume information more efficiently and to catalog the backup catalog data for the entire domain, use the [catalog](#) (page 2-15) command.
To import backup metadata stored in the tape, you can also use `--obtaropt` with the `-G` option.

--unlabeled/-u

Marks each imported volume as unlabeled. You cannot specify this option with `--identify` or `--import`.

The `unlabeled` option is not allowed if the library to which the `importvol` command is directed has an enabled and functioning barcode reader.



Note:

This option does not actually unlabeled the volumes. It is equivalent to an `insertvol unlabeled` command.

clean

Imports the specified tapes and marks them as cleaning tapes. The `iee` elements specified in `iee-range` are assumed to have cleaning tapes in them. All the cleaning tapes are assigned the same `uses` and `maxuses` values. This option must be used with the `--uses` and `--maxuses` options.

--uses/-U n

See [insertvol](#) (page 2-105).

--maxuses/-M n

See [insertvol](#) (page 2-105).

--obtaropt/-o *obtar-option*

Specifies [obtar](#) options that are passed to `obtar` when the volumes are read. For example `-J` enables debug mode and provides more details in backup and restore transcripts. See "[obtar Options](#) (page B-14)" for details on `obtar` options. This option is effective only for the `--identify` and `--import` options.

iee-range

Specifies a range of import/export elements containing the volumes to be imported. Refer to "[iee-range](#) (page 4-16)" for acceptable values for `iee-range`.

Examples

Example 2-61 Importing Volumes

This example uses the `importvol` command to update the volumes from import elements `iee1`, `iee2`, and `iee3` in the tape library `lib2`. Here, the tape library and import elements belong to the same Oracle Secure Backup domain.

```
ob> lsvol --long --library lib2
Inventory of library lib2:
  in  mte:          vacant
  in  1:            vacant
  in  2:            vacant
  in  3:            vacant
  in  4:            vacant
  in  iee1:         volume VOL000003, barcode DEV423, oid 111, 47711360 kb remaining, content
manages reuse
  in  iee2:         unlabeled, barcode DEV424, oid 114
```

```

in   iee3:          unlabeled, barcode DEV425, oid 115
in   dte:           vacant
ob> importvol --library lib2 iee1-3
ob> lsvol --long --library lib2
Inventory of library lib2:
in   mte:           vacant
in   1:             volume VOL000003, barcode DEV423, oid 111, 47711360 kb remaining
in   2:             unlabeled, barcode DEV424, oid 114
in   3:             unlabeled, barcode DEV425, oid 115
in   4:             vacant
in   iee1:          vacant
in   iee2:          vacant
in   iee3:          vacant
in   dte:           vacant

```

2.1.47 insertvol

Purpose

Use the `insertvol` command to notify Oracle Secure Backup that you have manually inserted a **volume** into the specified destination in the **tape library** and to specify the properties of the inserted volume. Oracle Secure Backup updates the inventory with the supplied information.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `insertvol` command.

Usage Notes

If the library to which the `insertvol` command is directed has an enabled and functioning barcode reader, then Oracle Secure Backup does not allow specification of the `vol-spec` or `unlabeled` options. Instead, the barcodes on the volumes being inserted are read and used to attempt a lookup in the volumes database.

If a matching record is found in the database, then that record is associated with the target storage element. If the barcode is not found in the database, then a scratch record is created and the state of the associated volume is marked `unknown`.

Syntax 1

Use the following syntax to specify that you have inserted unlabeled or unknown volumes or cleaning tapes.

```
insertvol: :=
```

```
insertvol [ --library/-L libraryname | --drive/-D drivename ]
{ unknown | unlabeled | clean --uses/-u n --maxuses/-m n }
se-range
```

Semantics 1

--library/-L *libraryname*

Specifies the name of the tape library in which you want to insert one or more volumes.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor [tape drive](#) setting.

--drive/-D *drivename*

Specifies the name of a tape drive in the tape library in which you want to insert one or more volumes.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

unknown

Indicates the volume being inserted is of unknown format.

unlabeled

Indicates that the volume inserted is known to be unlabeled or a new volume.

The `unlabeled` option is not allowed if the library to which the `insertvol` command is directed has an enabled and functioning barcode reader and the media policy `barcodesrequired` is set to `yes`.

clean

Indicates that the volume being inserted is a cleaning tape. You must specify this option with the `--uses` and `--maxuses` options.

--uses/-u *n*

Specifies the number of times that the cleaning tape has been used.

--maxuses/-m *m*

Specifies the maximum number of times that you can use the cleaning tape. The number of remaining uses for the cleaning tape is the difference between `--maxuses` and `--uses`.

se-range

Specifies a range of [storage elements](#) into which the volumes are to be inserted. The inventoried state of the target storage elements must be empty before running the `insertvol` command. You can verify that the storage elements are empty by running the `lsvol` command.

Refer to "[se-range](#) (page 4-27)" for a description of the `se-range` placeholder.

Syntax 2

Use the following syntax to specify that you have inserted known or labeled volumes.

```
insertvol::=
```

```
insertvol [ --library/-L libraryname | --drive/-D drivename ]  
[ vol-spec ] se-spec
```

Semantics 2

vol-spec

Specifies the [volume ID](#) or barcode of the inserted volume.

This option is not allowed if the library to which the `insertvol` command is directed has an enabled and functioning barcode reader.

See Also:

"[vol-spec](#) (page 4-31)" for a description of the `vol-spec` placeholder

se-spec

Specifies the storage element into which the volume was inserted. The inventoried state of the target storage element must be empty before running the `insertvol` command. You can verify that the storage element is empty by running the `lsvol` command.

See Also:

"[se-spec](#) (page 4-27)" for a description of the `se-spec` placeholder

The following sequence of events is required:

1. If the target storage element is not currently empty, then use `extractvol` or `movevol` to empty it.
2. Ensure that the storage element is recognized as empty by the `lsvol` command. Run the `inventory` command if it is not.

See Also:

- "[lsvol](#) (page 2-182)"
- "[inventory](#) (page 2-108)"

3. Manually insert a volume.

This step is necessary because the `insertvol` command requires the [barcode](#) to be read from the volume being inserted, which in turn requires that the volume be present before the `insertvol` command is run.

4. Immediately run the `insertvol` command.

Example

Example 2-62 Notifying Oracle Secure Backup of a Manually Inserted Volume

This example informs Oracle Secure Backup that a cleaning tape is inserted into storage element 2 of tape library `lib1`. Note that the sample output is reformatted so that it fits on the page.

```

ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            volume VOL000001, barcode ADE201, oid 102, 48359360 kb
                    remaining
  in  2:            vacant
  in  3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112,
                    47773408 kb remaining, content manages reuse
  in  4:            vacant
  in  iee1:         vacant
  in  iee2:         vacant
  in  iee3:         vacant
  in  dte:          vacant
ob> insertvol --library lib1 clean --uses 0 --maxuses 3 2
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            volume VOL000001, barcode ADE201, oid 102, 48359360 kb
                    remaining
  in  2:            barcode ADE203, cleaning tape: 0 uses, 3 remaining
  in  3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112,
                    47773408 kb remaining, content manages reuse
  in  4:            vacant
  in  iee1:         vacant
  in  iee2:         vacant
  in  iee3:         vacant
  in  dte:          vacant

```

2.1.48 inventory

Purpose

Use the `inventory` command to initiate a scan of the contents of a [tape library](#).

Oracle Secure Backup does not automatically detect changes to a tape library that result from manual actions such as opening the tape library door to move or remove a tape. Use the `inventory` command in such circumstances to make the tape library detect the changes.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to run the `inventory` command.

Syntax

```
inventory::=
```

```
inventory [ --library/-L libraryname | --drive/-D drivename ]
[ --force/-f ][ se-range ]
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library for which you want to update the inventory. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D *drivename*

Specifies the name of a [tape drive](#) in the tape library for which you want to update the inventory.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--force/-f

Forces the tape library to perform a physical inventory of the tape library. Instead of reading from its cache, the tape library updates the inventory by physically scanning all tape library elements.

se-range

Limits the inventory update to a range of storage elements. If you do not specify a storage element range, then all storage elements are included in the inventory update.

Note:

If a tape library does not support the Initialize Element Status with Range operation, then Oracle Secure Backup ignores the range option and performs a full Initialization Element Status operation.

Every data-transfer element (DTE) and import-export element (IEE) is included in the inventory update, no matter whether a storage-element range is specified or not.

See Also:

["se-range \(page 4-27\)"](#) for more information on the `se-range` placeholder

Example

Example 2-63 Taking an Inventory of a Tape Library

This example forces the tape library `lib1` to perform an inventory operation. Note that the sample output has been reformatted so that it fits on the page.

```
ob> inventory --library lib1 --force
ob> lsvol --library lib1
Inventory of library lib1:
* in 2:          volume VOL000001, barcode ADE201, 38919872 kb remaining
  in ieel:       volume VOL000002, barcode ADE203, 38273920 kb remaining, lastse 1
  in dte:        volume RMAN-DEFAULT-000002, barcode ADE202, 38328224 kb remaining, content
manages reuse, lastse 3
```

*: in use list

Example 2-64 Taking an Inventory of a Tape Library that Does not Contain a Barcode Reader

This example displays the inventory of a tape library that does not contain a barcode reader.

The library `lib` does not contain a barcode reader. After performing a forced inventory of the library, some volumes have been manually added to the storage elements 1, 2, and 3. When you use the `lsvol` command to display the list of volumes in the library, you obtain the following output.

```
ob> lsvol -L lib
Inventory of library lib:
in 4: occupied
in 8: occupied
in 9: occupied
in 10: occupied
```

When you force the tape library `lib` to perform an inventory operation, the newly added tapes are displayed in the storage elements as shown by the following output.

```
ob> inv --force -L lib
ob> lsvol -L lib
Inventory of library lib:
in 1: occupied
in 2: occupied
in 3: occupied
in 4: occupied
in 8: occupied
in 9: occupied
in 10: occupied
```

2.1.49 labelvol

Purpose

Use the `labelvol` command to load selected volumes and write a [volume label](#) to each [volume](#).

WARNING:

This command erases all existing data on the selected volumes.

In Oracle Secure Backup, a [volume label](#) typically contains a [volume ID](#)—for example, `lev0-0001`—and a [volume tag](#), which is a [barcode](#). These two attributes uniquely identify a tape. Oracle Secure Backup usually creates a volume label when it first writes to a tape. You might want to label a volume manually in the following circumstances:

- The volume has a barcode but resides in a [tape library](#) without a barcode reader. In this case, you must manually inform Oracle Secure Backup of the barcode so that it can properly be written to the volume label.

- You want to reserve the volume for use in a particular [media family](#). In this case, prelabeling the volume restricts its use to the media family.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Usage Notes

You can also use the `labelvol` to create a pool of tapes that belong to a single media family. To do this, you must use the `-obtaropt` option with `-Xfa:<mediafamily>` as shown in [example 2-61](#) (page 2-112) below.

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `labelvol` command.

Syntax

`labelvol::=`

```
labelvol [ --drive/-D drivename ] [ --barcode/-b barcode ]
[ --force/-f ] [ --obtaropt/-o obtar-option ]... [ se-range ]
```

Semantics

--drive/-D *drivename*

Specifies the name of the [tape drive](#) to be used to label the volume. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--barcode/-b *barcode*

Specifies a barcode for the volume.

--force/-f

Forces the labeling of a volume. Running the command with this option overrides any conditions that would otherwise prevent the `labelvol` command from functioning. This option enables you to [overwrite](#) unexpired volumes. Also, you can [overwrite](#) an incorrect manual entry for a barcode without the currently required prior step of running an [unlabelvol](#) (page 3-146) command.

--obtaropt/-o *obtar-option*

Specifies [obtar](#) options. For example `-j` enables debug mode and provides more details in backup and restore transcripts. See "[obtar Options](#) (page B-14)" for details on `obtar` options.

se-range

Specifies a range of [storage elements](#) holding the volumes to be labeled. If this option is omitted, then the volume currently loaded in the specified tape drive is labeled. Refer to "[se-range](#) (page 4-27)" for a description of the `se-range` placeholder.

Example

Example 2-65 Manually Labeling a Volume

This example reserves the tape in storage element 4 in tape library `lib1` for use by media family `mf_incr`.

```
ob> insertvol unlabeled --library lib1 4
ob> labelvol --drive tape1 --obtaropt -Xfam:mf_incr 4
```

2.1.50 loadvol

Purpose

Use the `loadvol` command to move a [volume](#) from the indicated storage element to the selected [tape drive](#).



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `loadvol` command.

Syntax

```
loadvol::=
```

```
loadvol [ --drive/-D drivename ] [ --mount/-m mode ]
[ --force/-f ] [ --req/-r ] { vol-spec | element-spec }
```

Semantics

--drive/-D *drivename*

Specifies the name of the tape drive in which you want to load a volume. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--mount/-m *mode*

Indicates the mode that the system can use for a volume physically loaded into a tape drive. When a tape is mounted in a tape drive, the tape is positioned in the tape drive so that it is in the correct configuration to perform the specified action. Valid values for *mode* are as follows:

- `read`

This mode mounts the volume for reading only.

- `write`

This mode mounts the volume so that it can append any backups to the end of the volume.

- `overwrite`

This mode mounts a volume on the [tape device](#) and positions it at the beginning of the tape so that the existing contents of the volume are overwritten. If you use this option, then you are granting permission to [overwrite](#) an unexpired volume.

--force/-f

Forces the loading of a volume. If another volume is in the tape drive, then the volume is automatically unloaded.

--req/-r

Loads the volume only if it is not loaded in the tape drive.

vol-spec

Specifies the volume to be loaded. You specify a volume by its [volume ID](#) or its type: `unknown`, `unlabeled`, or `clean`. Refer to "[vol-spec](#) (page 4-31)" for a description of the `vol-spec` placeholder.

element-spec

Specifies the number of a storage element to be loaded. Refer to "[element-spec](#) (page 4-14)" for a description of the `se-spec` placeholder.

Example

Example 2-66 Loading a Volume in a Tape Drive

This example takes a volume from storage element 1 in [tape library](#) `lib1` and loads it into [tape drive](#) `tape1`.

```
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in   mte:          vacant
  in   1:            volume VOL000002, barcode ADE201, oid 110, 47670368 kb remaining
  in   2:            volume VOL000001, barcode ADE203, oid 102, 48319392 kb remaining
  in   3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
                    remaining, content manages reuse
  in   4:            vacant
  in   iee1:         barcode ADE204, oid 114, 47725344 kb remaining, lastse 4
  in   iee2:         vacant
  in   iee3:         vacant
  in   dte:          vacant
ob> loadvol --drive tape1 1
ob> lsvol --drive tape1
Inventory of library lib1:
* in   2:            volume VOL000001, barcode ADE203, 48319392 kb remaining
* in   3:            volume RMAN-DEFAULT-000002, barcode ADE202, 47725600 kb remaining, content
                    manages reuse
  in   iee1:         barcode ADE204, 47725344 kb remaining, lastse 4
  in   dte:          volume VOL000002, barcode ADE201, 47670368 kb remaining, lastse 1

*: in use list
```

2.1.51 logout

Purpose

Use the `logout` command to exit `obtool` and destroy the login token. When you restart `obtool`, it prompts you for a username.

**See Also:**

"[Miscellaneous Commands](#) (page 1-18)" for related commands

Syntax

```
logout::=
```

```
logout
```

Example**Example 2-67 Displaying the Current User**

This example logs out, logs in again as user `admin`, and then displays current user information.

```
ob> logout
% obtool
Oracle Secure Backup 12.2.0.1.0
login: admin
ob> id
admin
```

2.1.52 ls

Purpose

Use the `ls` command to list the names and attributes of file-system objects represented in the Oracle Secure Backup [catalog](#).

Listing the contents of the Oracle Secure Backup catalog is equivalent to listing the contents of backup images and backup image instances. The catalog displays the images in a directory structure much like a live file system. You can only list directories whose contents have been backed up.

**See Also:**

"[Browser Commands](#) (page 1-12)" for related commands

Prerequisites

The [rights](#) needed to run the `ls` command depend on the [browse backup catalogs with this access](#) (page 8-3) setting for the [class](#).

Syntax

```
ls::=
```

```
ls [ --long/-l | --short/-s ] [ --label/-L ] [ --oneperline/-1 ]
[ --reverse/-r ] [ --directory/-d ] [ --backup/-b ] [ --position/-p ]
[ --inode/-i ] [ --nobackupid/-I ] [ --noheader/-H ] [ --notype/-T ]
[ --noerrors/-E ] [ --numberformat/-n numberformat ]
```

```
[ --viewmode/-v viewmode ] [ --ctime/-c | --mtime/-t | --utime/-u ]  
[ --nosort/-X ] [ --noescape/-B ] [ --max/-M max-entries ]  
[ --startat/-S starting-entry ] [ --host/-h hostname ]  
[ --select/-s data-selector[,data-selector]... ] [ --recursive/-R ]  
pathname...
```

Semantics

--long/-l

Displays Oracle Secure Backup catalog data in long form.

If a backup error occurred on an entry, then the `--long` display shows the actual error text. If neither the `--long` option nor the `--backup` option is specified, then `E` is appended to the display name.

--short/-s

Displays Oracle Secure Backup catalog data in short form (default).

--label/-L

Labels the items in the Oracle Secure Backup catalog for ease of reading. See [Example 2-68](#) (page 2-116) for an illustration.

--hostname/-h

Displays entries only belonging to the specified host.

--oneperline/-1

Puts each item on a separate line.

--recursive/-R

Displays all entries that are backed up from a particular path. It lists all entries that are a part of a given directory and data selector.

--reverse/-r

Reverses the listing order.

--directory/-d

Displays information on the current directory in the Oracle Secure Backup catalog.

--backup/-b

Displays the backup information.

If a backup error occurred on an entry, then the `--backup` display appends an `E` on the individual archive section line. If neither the `--long` option nor the `--backup` option is specified, then `E` is appended to the display name.

--position/-p

Displays the physical location of data on the tape when used with the `--backup` option.

--inode/-i

Displays inode of contents. Note that this option is only supported for backup image instances generated by a [Network Data Management Protocol \(NDMP\) data service](#).

--nobackupid/-l

Does not display the [backup ID](#).

--noheader/-H

Displays information without header output.

--notype/-T

Does not use "/" to indicate a directory.

--noerrors/-E

Does not display file-system error messages.

--numberformat/-n *numberformat*

Specifies how to display large numbers. Refer to "[numberformat](#) (page 4-21)" for a description of the *numberformat* placeholder.

--viewmode *viewmode*

Specifies the mode in which to view the Oracle Secure Backup catalog directory contents. Valid values for *viewmode* are as follows:

- *exact* displays only those directory entries that match the data selector and are present in the current path.
- *inclusive* displays all entries, regardless of the current data selector (default).
- *specific* displays all entries that match the data selector.

--ctime/-c

Displays inode change time if `--long` also specified.

--mtime/-t

Displays file modified time if `--long` also specified.

--utime/-u

Displays file used time if `--long` also specified.

--nosort/-X

Does not sort names for display.

--noescape/-B

Does not escape non-displayable characters in filenames. Specify `--noescape` if you want file names that include an ampersand character (&) to display normally.

--max/-M *max-entries*

Specifies the maximum number of entries to display.

--startat/-S *starting-entry*

Specifies the number where the display should start, with 1 as the first item in the listing.

--select/-s *data-selector*

Specifies the Oracle Secure Backup catalog data that applies to an operation. Refer to [data-selector](#) (page 4-6) for the data-selector placeholder.

pathname

Specifies the path names in the Oracle Secure Backup catalog.

Example**Example 2-68 Displaying Information About a File**

This example lists backup data on `brhost2` in short form and then in long form.

```
ob> set host brhost2
ob> ls
home/
```

```

ob> cd home
ob> ls
data/
ob> cd data
ob> ls
backup/
ob> cd backup
ob> ls
bin/ c_files/ tree/
ob> cd tree
ob> ls
file1 levla/ levlb/
ob> ls --long file1
-rwx----- bkpadmin.g527      74      2012/03/02.09:51 file1      (4)
ob> ls --long --label --backup --position file1
Name:          file1
Backup ID:     4
Mode & protection: -rwx-----
Last modified: 2012/03/02.09:51:33
Size:         74
Backup ID:     4
Backup date & time: 2012/03/03.12:13:16
Volume ID:     VOL000002
Volume tag:    DEV423
File number:   11
File section:  1
Requested level: 0
Client:        brhost2
Device:        vtl
Program version: 12.1.0.1.0
Volume creation: 2012/03/02.10:02:27
Position:      0000023A0009

```

2.1.53 lsbackup

Purpose

Use the `lsbackup` command to list each [backup request](#) that you created with the [backup](#) (page 2-4) command. These requests are awaiting delivery to the [scheduler](#).

The `lsbackup` command only lists backup requests that have not yet been sent to the scheduler with the `--go` option. For example, if you create a backup request, specify `--go`, and then run `lsbackup`, `obtool` does not display the request.

See Also:

"[Backup Commands](#) (page 1-10)" for related commands

Prerequisites

You must have the [perform file system backups as privileged user](#) (page 8-6) right if you specified the `--privileged` option when you created the backup. Otherwise, you must have the [perform file system backups as self](#) (page 8-6) right.

Syntax

lsbackup::=

```
lsbackup [ --long/-l | --short/-s ] [ --noheader/-H ] [ backup-item ]...
```

Semantics

--long /-l

Displays data in long form, that is, describes all of the attributes for each job and labels them. Refer to [Example 2-69](#) (page 2-118) for the type of data included. By default this command displays a subset of attributes in tabular form.

--short /-s

Displays data in short form, that is, lists job IDs only.

--noheader/-H

Suppresses column headers when listing data.

backup-item

Specifies an identifier assigned by obtool to a backup created with the [backup](#) (page 2-4) command. The identifier is a small integer number.

Output

[Table 2-3](#) (page 2-118) describes the output of the `lsbackup` command.

Table 2-3 Output of the lsbackup command

Label	Indicates
Dataset	User-specified name of the dataset file used in the backup job
Media family	User-specified name of the media family used in the backup job
Backup level	Level of backup to be performed; setting is <code>full</code> , <code>1</code> to <code>10</code> , <code>incremental</code> , or <code>offsite</code>
Priority	Priority level of the backup job; set a number greater than 0; 1 is the highest priority
Privileged op	Setting is <code>yes</code> or <code>no</code>
Eligible to run	Date and time at which the backup job can begin
Job expires	Date and time the backup job request expires
Restriction	Tape devices to which the backup job is restricted
S/w compression	Compression option to be used in the backup job

If a date reported by `lsbackup` is more than six months earlier or more than two months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier or less than two months in the future, then it is reported in a `mm/dd.hh:mm` format.

Example

Example 2-69 Listing a Backup in Long Form

This example displays full details about pending backup jobs. The `1:` at the beginning of the output is the backup item identifier.

```
ob> lsbackup --long
1:

Dataset: brhost2.ds
Media family: (null)
Backup level: full
Priority: 10
Privileged op: yes
Eligible to run: 2017/01/14.21:00:00
Job expires: 2017/01/19.21:00:00
Restriction: any device
Encryption: off
Hardware encryption: if present
Store catalog on tape: yes
S/w compression: high
```

2.1.54 lsbkup

Purpose

Displays information about backup images created by a backup job. After a backup job completes, Oracle Secure Backup creates a backup image and a backup image instance. Backup images store metadata about a backup such as type of backup, creation date and time, job ID, and host on which the backup was created.

Prerequisites

You must have the [list any backup, regardless of its owner](#) (page 8-4) or [list any backups owned by user](#) (page 8-4) class right to use the `lsbkup` command.

Usage Notes

The backup images instances associated with each backup can be displayed by using the `--instances` option of the `lsbkup` command.

Syntax

`lsbkup::=`

```
lsbkup
[--long/-l | --short/-s] [--noheader/-H]
[--type/-Y {database | filesystem}][--ctype/-y {tape | disk | cloudstorage}]
[ {[--from/-f date-time] [--to/-t date-time]} | [--today/-T] ]
[--instances/-i | --contents/-C] [--duplicates/-D]
[--host/-h hostname]...
[ [--barcode/-b tag]... | [--container/-c backup-container]... |
[--uuid/-u backup-image-uuid]... | backup-image-name... ]
```

Semantics

--long/-l

Displays all the attributes related to each backup image, with multiple lines of information for each backup image.

--short/-s

Displays only the names of the backup images.

--noheader/-H

Omits displaying headers in the command output.

--type/-Y {database | filesystem}

Displays backup images of the specified type only. Use `database` to display Oracle Database backups and `filesystem` to display information about file-system backups. By default, backup images associated with both types of backups are displayed.

--ctype/-y {tape | disk | cloudstorage}

Displays backup images that are stored on the specified backup container. Use `tape` to display backup images stored on tape devices and `disk` to display backup images stored on disk pools. Use `cloudstorage` to display backup images stored on cloud storage devices. By default, backup images stored on all backup containers are displayed.

--from/-f *date-time*

Displays backup images created since the specified date or time. See "[date-time](#) (page 4-9)" for information about specifying the date and time.

--to/-t <*date-time*>

Displays backup images created before the specified date or time. See "[date-time](#) (page 4-9)" for information about specifying the date and time.

--today/-T

Displays backup images created today.

--instances/-i

Displays all the backup image instances associated with a backup image.

--contents/-C

Displays the contents of backup images. For file-system backups, Oracle Secure Backup displays the directory path that is backed up. For Oracle Database backups created using RMAN, Oracle Secure Backup displays the name of the database, the backup piece name, and the type of backup.

--duplicates/-D

Displays duplicate volumes for backup image instances stored on tape. Duplicate volume containers are denoted by a "+" in the display. This option is applicable only if the `--instances` option is specified, as containers are associated only with backup image instances.

--host/-h *hostname*

Displays backup images for the specified host.

--barcode/-b *tag*

Displays only backup images contained in the volume that has the specified barcode.

--container/-c *backup-container*

Displays backup images contained in the specified container (tape volume, disk pool or cloud storage device). See "[backup-container](#) (page 4-4)".

 **Note:**

You can use only one of the following options simultaneously in an `lsbkup` command:

- `--barcode`, `--container`, `--uuid`, and `backup-spec`
- `--contents` and `--instances`

--uuid/-u backup-image-uuid

Displays backup images with the specified UUID. Oracle Secure Backup assigns a unique UUID to each backup image.

backup-image-name

Specifies the name of the backup image whose details must be displayed.

Examples**Example 2-70 Specifying Backup Image Instances for a Specified Host**

This example displays backup images for the host `brhost2`. It also displays details about the backup images instances associated with each backup image.

```
ob> lsbkup --host brhost2 --instances
Backup Image Name      Client      Type      Created      Size
brhost2-20110926-115943 brhost2    FS        2011/09/26.04:59 62.4 MB
Seq      Created      Expires      Encryption  Container(s)
1 2011/09/26.04:59 off          VOL00001
brhost2-20110926-120953 brhost2    FS        2011/09/26.05:09 62.4 MB
Seq      Created      Expires      Encryption  Container(s)
1 2011/09/26.05:09 off          VOL00002
1 2011/09/26.06:09 2011/09/26.16:10 off          STK.pool
```

Example 2-71 Displaying Backup Image Details in Long Format

This example displays, in long format, the details about the backup image `brhost2-20110926-123218`. The `Size` shown in this particular example output is the size of the backup after compression.

```
ob> lsbk -l brhost2-20170422-133707
Backup image name:   brhost2-20170422-133707
Type:               file system
Client:             brhost2
Backup level:       0
Size:               26.2 MB
Uncompress size:    62.5 MB
Backup owner:       admin
Owner class:        admin
Backup date and time: 2017/04/22.06:37
Created by job:     admin/1.1
UUID:               631810e4-09c9-1035-a969-00163e43c05f
```

Example 2-72 Displaying the Contents of Backup Images

This example displays the contents of each backup image. For file-system backups, the name of the directory path backed up is displayed. For Oracle Database backups created using RMAN, the name of the database, the backup piece name, and the type of backup is displayed.

```

ob> lsbkup --contents
      Backup Image Name      Client      Type      Created      Size
brhost2-20110926-123218      brhost2      FS      2011/09/26.05:32      62.4 MB
      Container      File Sect      Level
      VOL000001      1      1      0
      /oracle/work/data/backup
brhost1-20110926-123432      brhost1      DB      2011/09/26.05:34      832.0 KB
      Container      File Sect      Database      Content      Piece Name
      RMAN-DEFAULT-000001      1      1      dbu      archivelog      01mng6eq_1_1
brhost1-20110926-123500      brhost1      DB      2011/09/26.05:35      7.8 MB
      Container      File Sect      Database      Content      Piece Name
      RMAN-DEFAULT-000001      2      1      dbu      autobackup      c-20883-20110926-00
brhost1-20110926-123525      brhost1      DB      2011/09/26.05:35      82.5 MB
      Container      File Sect      Database      Content      Piece Name
      RMAN-DEFAULT-000001      3      1      dbu      full      03mng6gn_1_1

```

2.1.55 lsbu

Purpose

Use the `lsbu` command to list cataloged backups. A catalogued backup is a backup that has completed, either successfully or with errors, and that has been logged in the Oracle Secure Backup [catalog](#).

The `lsbu` command lists backup date and time, [volume ID](#), and so forth. The `ls` (page 2-114) command lists the contents of cataloged backups.



See Also:

"[Browser Commands](#) (page 1-12)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsbu` command.

Syntax

`lsbu::=`

```

lsbu [--long/-l | --short/-s] [--noheader/-H] [--reverse/-r]
      [--level/-L backup-level | --maxlevel/-M backup-level]
      [--inclusions/-i [ --dependencies/-d ] ]
      [--host/-h hostname[,hostname]...] [--duplicates/-D]
      [--backup/-b backup-image-name] [--buuid/u backup-image-uuid]
      [--instance/-I backup-instance-name | --iuuid/U backup-instance-uuid]
      [--path/-p pathname] [data-selector]...

```

Semantics

--long/-l

Displays data in long form. The command displays all attributes of the backups and labels them. By default the command displays a subset of attributes in tabular format.

--short/-s

Displays data in short form. The command displays only [backup IDs](#).

--noheader/-H

Does not display headers for columns.

--reverse/-r

Reverses the listing order.

--level/-L *backup-level*

Displays backups based on [backup level](#). Refer to "[backup-level](#) (page 4-4)" for a description of the *backup-level* placeholder.

--maxlevel/-M *backup-level*

Specifies the maximum backup level to display. Refer to "[backup-level](#) (page 4-4)" for a description of the *backup-level* placeholder.

-inclusions/-i

Displays the paths that were backed up for the set host.

**See Also:**

"[set](#) (page 3-140)" to learn how to set or reset the host

--dependencies/-d

For each [incremental backup](#) listed, display the dependencies on predicate backups.

--host/-h *hostname*

Displays backups of [client](#) *hostname*.

--duplicates/-D

While listing backups, show backup available on duplicate volumes as well. If this option is not specified, then the command shows only the [volume](#) at the [active location](#) or nearest [storage location](#).

--backup/-b *backup-image-name*

Displays backups for the specified backup image name.

--buuid/-u *backup-image-uuid*

Displays backups for the specified backup image UUID.

--instance/-I *backup-instance-name*

Displays backups for the specified backup image instance name.

--iuuid/-U *backup-instance-uuid*

Displays backups for the specified backup image instance UUID.

--path/-p *pathname*

Displays backups based on file-system objects.

data-selector

Specifies the Oracle Secure Backup catalog data that applies to an operation.

**See Also:**

"[data-selector](#) (page 4-6)" for more information on the *data-selector* placeholder

Output

[Table 2-4](#) (page 2-124) describes the output for the `lsbu` command.

Table 2-4 Output of the lsbu command

Label	Indicates
Backup ID	Unique identification number for a backup job; assigned by Oracle Secure Backup
Backup date & time	Starting date and time for a backup job; assigned by the scheduler
Volume ID	Unique volume name with a sequentially numbered suffix; assigned by Oracle Secure Backup
Volume tag	Barcode of the volume
Current location	Current location of the volume
File number	The file number the backup job occupies on a tape containing multiple backups
File section	The number of times a tape is changed during a backup job that spans multiple tapes
Requested level	Defaults to 0 if no previous backup job exists for this directory; assigned by the Oracle Secure Backup user when the backup job is scheduled
Client	Name of the backed up client computer
Device	Name of the tape drive to which the backup is made
Program version	Version of Oracle Secure Backup
Encryption	Encryption enabled or disabled
Algorithm	The encryption algorithm used
Volume creation	Date and time at which Oracle Secure Backup wrote backup image file number 1 to a volume.
Archive Creation	The date and time of archive creation
Instance name	The name of the backup instance

If a date reported by `lsbu` is more than six months earlier or more than two months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier or less than two months in the future, then it is reported in a `mm/dd.hh:mm` format.

Examples**Example 2-73 Listing Cataloged Backups**

This example lists all cataloged backups for host `sales-server`.

```
ob> lsbu -l -h sales-server
Backup ID:          0
  Backup date & time: 2013/01/14.11:37:44
  Volume ID:        VOL000001
```

```

Volume tag:          16ab82c4c4b1102a6f5000423a5a98c
Current location:   vlib1
File number:        2
File section:       1
Requested level:    0
Client:             sales-server
Device:             vtl
Program version:    12.1.0.1.0
Encryption:         on
Algorithm:          aes192
Volume creation:    2009/01/14.11:35:15
Backup ID:          1
Backup date & time: 2013/01/14.11:39:09
Volume ID:          VOL000001
Volume tag:          16ab82c4c4b1102a6f5000423a5a98c
Current location:   vlib1
File number:        3
File section:       1
Requested level:    0
Client:             sales-server
Device:             vtl
Program version:    12.1.0.1.0
Encryption:         hardware
Algorithm:          aes256
Volume creation:    2013/01/14.11:35:15
Backup ID:          2
Backup date & time: 2013/01/14.11:39:27
Volume ID:          VOL000001
Volume tag:          16ab82c4c4b1102a6f5000423a5a98c
Current location:   vlib1
File number:        4
File section:       1
Requested level:    0
Client:             sales-server
Device:             vtl
Program version:    12.1.0.1.0
Encryption:         off
Volume creation:    2013/01/14.11:35:15

```

Example 2-74 Listing Cataloged Backups for a Specific Instance

```

ob> lsbu -l 3
Backup ID:          3
Backup date & time: 2017/08/28.09:38:31
File number:        1
File section:       1
Requested level:    0
Client:             brhost2
Device:             tapel
Program version:    12.2.0.1.0
Archive creation:   2017/08/28.09:38:31
Instance name:      brhost2-20170828-163831.3
Encryption:         off

```

2.1.56 lsbw

Purpose

Use the `lsbw` command to list backup windows. If no [backup window](#) exists, then the command displays the following message:

There are no backup windows.

**See Also:**

"[Backup Window Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsbw` command.

Syntax

`lsbw::=`

```
lsbw [ --short/-s ] day-specifier[,day-specifier]....
```

Semantics**--short/-s**

Displays data in short form. The command displays only the days when the backup window is open. By default the command displays days and times.

day-specifier

Specify a time range in terms of days. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example**Example 2-75 Listing Backup Windows**

This example shows the backup windows created in [Example 2-1](#) (page 2-1).

```
ob> lsbw
weekend          08:00-20:00
weekday         00:00-08:00,20:00-24:00
```

2.1.57 lscheckpoint

Purpose

Use the `lscheckpoint` command to list the identity and attributes of current checkpoints.

**See Also:**

"[Checkpoint Commands](#) (page 1-12)" for related commands

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lscheckpoint` command.

Syntax

lscheckpoint::=

```
lscheckpoint [ --short/-s | --long/-l ] [ --host/-h hostname[,hostname...]... ]...  
[ job-id ]...
```

Semantics

--short/-s

Displays only the IDs of jobs that have checkpoints.

--long/-l

Displays multiple lines for each entry, describing all user-visible information for each checkpoint.

--host/-h *hostname*

Constrains the listing to checkpoints for the host specified by *hostname*.

job-id

Specifies the Oracle Secure Backup-assigned job ID whose checkpoint information you want to display. If this option is absent, then `obtool` displays all checkpoints, or all checkpoints for hosts named specified with the `--host/-h` option.

Output

[Table 2-5](#) (page 2-127) describes the output of the `lscheckpoint` command.

Table 2-5 lscheckpoint Output

Label	Indicates
Job ID	Unique identifier of a scheduled backup or restore job; assigned by Oracle Secure Backup
Host	Name of host
Operation	Type of operation being performed
Checkpoint created	Date and time at which the checkpoint was created
Restartable	Ability to restart a backup job; setting is <i>yes</i> or <i>no</i>
Current context ID	Identification of the currently active checkpoint

If a date reported by `lscheckpoint` is more than six months earlier, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier, then it is reported in a `mm/dd.hh:mm` format.

Example

Example 2-76 Listing Checkpoint Information

This example displays the job information for job `admin/8.1` and then displays the checkpoint information for this job.

```
ob> lsjob --long admin/8.1
admin/8.1:
  Type:          backup br_filer
  Level:         full
  Family:        (null)
```

```

Restartable:          yes
Scheduled time:       none
State:                running since 2013/45/18.17:45
Priority:              100
Privileged op:       no
Run on host:          (administrative server)
Attempts:             1
ob> lscheckpoint --long admin/8.1
Job ID:                admin/8.1
Host:                  br_filer
Operation:             backup
Checkpoint created:   04/18.17:48
Restartable:          yes
Current context ID:   18

```

2.1.58 lsclass

Purpose

Use the `lsclass` command to list the names and attributes of a [Oracle Secure Backup user class](#).

See Also:

- ["Class Commands \(page 1-13\)"](#) for related commands
- [Classes and Rights \(page 8-1\)](#) for a descriptions of the default Oracle Secure Backup classes and [rights](#)

Prerequisites

You must have the [display administrative domain's configuration \(page 8-4\)](#) right to use the `lsclass` command.

Syntax

`lsclass::=`

```

lsclass [ { --long/-l [ --abbreviate/-a ] } | --short/-s ]
  [--modself/-m {yes | no}]      [--modconfig/-M {yes | no}]
    [--backupsself/-k {yes | no}]  [--backuppriv/-K {yes | no}]
    [--restself/-r {yes | no}]     [--restpriv/-R {yes | no}]
    [--listownjobs/-j {yes | no}]  [--modownjobs/-J {yes | no}]
    [--listanyjob/-y {yes | no}]   [--modanyjob/-Y {yes | no}]
    [--mailinput/-i {yes | no}]    [--mailerrors/-e {yes | no}]
    [--mailrekey/-g {yes | no}]    [--browse/-b <browserights>]
    [--querydevs/-q {yes | no}]    [--managedevs/-d {yes | no}]
    [--listownbackups/-s {yes | no}] [--modownbackups/-S {yes | no}]
    [--listanybackup/-u {yes | no}] [--modanybackup/-U {yes | no}]
    [--orauser/-o {yes | no}]      [--orarights/-O oraclerights]
    [--fsrights/-F fsrights]      [--listconfig/-L {yes | no}]
    [--modcatalog/-c {yes | no}]
    [classname]...

```

Semantics

Refer to "mkclass (page 3-2)" for details on options not included in this section. For the `lsclass` command, these options select which classes are to be listed based on whether a class has (`yes`) or lacks (`no`) the specified rights.

--long/-l

Displays data in long form. The command displays all classes and privileges.

--abbreviate/-a

Displays a short description when used with the `--long` option.

--short/-s

Displays data in short form (default). The command displays only the class names.

--fsrights/-F *fsrights*

Enables Oracle Secure Backup users with the specified rights to access Oracle file system backups.

Output

Table 2-6 (page 2-129) describes the output of the `lsclass` command.

Table 2-6 Isclass Output

Label	Indicates
browse	browse backup catalogs with this access (page 8-3) right; values are <code>privileged</code> , <code>notdenied</code> , <code>permitted</code> , <code>named</code> , <code>none</code>
oracle	access Oracle database backups (page 8-3) right; values are <code>owner</code> , <code>class</code> , <code>all</code> , or <code>none</code>
file system	access file system backups (page 8-2) right; values are <code>owner</code> , <code>class</code> , <code>all</code> , or <code>none</code>
listconfig	display administrative domain's configuration (page 8-4) right; values are <code>yes</code> or <code>no</code>
modself	modify own name and password (page 8-6) right; values are <code>yes</code> or <code>no</code>
modconfig	modify administrative domain's configuration (page 8-4) right; values are <code>yes</code> or <code>no</code>
backupself	perform file system backups as self (page 8-6) right; values are <code>yes</code> or <code>no</code>
backuppriv	perform file system backups as privileged user (page 8-6) right; values are <code>yes</code> or <code>no</code>
listownjobs	list any jobs owned by user (page 8-5) right; values are <code>yes</code> or <code>no</code>
modownjobs	modify any jobs owned by user (page 8-5) right; values are <code>yes</code> or <code>no</code>
restself	perform file system restores as self (page 8-7) right; values are <code>yes</code> or <code>no</code>
restpriv	perform file system restores as privileged user (page 8-6) right; values are <code>yes</code> or <code>no</code>
mailinput	receive email requesting operator assistance (page 8-7) right; values are <code>yes</code> or <code>no</code>

Table 2-6 (Cont.) lsclass Output

Label	Indicates
mailerrors	receive email describing internal errors (page 8-7) right; values are <code>yes</code> or <code>no</code>
querydevs	query and display information about devices (page 8-7) right; values are <code>yes</code> or <code>no</code>
managedevs	manage devices and change device state (page 8-5) right; values are <code>yes</code> or <code>no</code>
listanyjob	list any job, regardless of its owner (page 8-5) right; values are <code>yes</code> or <code>no</code>
modanyjob	modify any job, regardless of its owner (page 8-5) right; values are <code>yes</code> or <code>no</code>
oracleuser	perform Oracle database backups and restores (page 8-6) right; values are <code>yes</code> or <code>no</code>

Example**Example 2-77 Displaying Information About a Class**

This example lists the attributes of the `reader` class.

```
ob> lsclass --long --abbreviate reader
reader:
reader:
  browse:      named
  oracle:      none
  file system: none
  listconfig:  no
  modself:     yes
  modconfig:  no
  modcatalog:  no
  backupself:  no
  backuppriv:  no
  listownjobs: no
  modownjobs:  no
  restself:    no
  restpriv:    no
  mailinput:   no
  mailerrors:  no
  mailrekey:   no
  querydevs:  no
  managedevs:  no
  listanyjob:  no
  modanyjob:   no
  oracleuser:  no
  listownbackups: no
  modownbackups: no
  listanybackup: no
  modanybackup: no
```

2.1.59 lsdaemon

Purpose

Use the `lsdaemon` command to list Oracle Secure Backup **daemons** running on a host.



See Also:

"[Daemon Commands](#) (page 1-13)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsdaemon` command.

Syntax

`lsdaemon::=`

```
lsdaemon [ --long/-l | --short/-s ] [ --all/-a ] [ --noheader/-H ]  
[ --host/-h hostname[,hostname]... ] [ daemon-id ]...
```

Semantics

--long/-l

Lists data in long form. The command displays the attributes of each daemon and labels them, for example, `Listen port: 43983`. By default `lsdaemon` displays this data in tabular form.

--short/-s

Lists only the names of the daemons.

--all/-a

Lists the same data as `--long` except in a table format, that is, with column headings instead of labels. This option is enabled by default.

--noheader/-H

Lists data in `--all` format but suppresses column names.

--host/-h *hostname*

Lists daemon data based on the specified host in which the daemons run. If this option is omitted, then the local host is assumed.

daemon-id

Identifies an Oracle Secure Backup daemon, either a process id (PID) or service name. Possible service names are `observed`, `obscheduled`, `obrobotd`, and `obixd`. If this option is omitted, all daemons are displayed.

Output

[Table 2-7](#) (page 2-132) shows the output for the `lsdaemon` command.

Table 2-7 lsdaemon Output

Label	Indicates
Process ID	Number identifying the process in which the daemon is running; assigned by the operating system
Daemon/Service	Name of the daemon; assigned by Oracle Secure Backup
State	State of the daemon; setting is <code>debug</code> or <code>normal</code>
Listen port	TCP port on which the daemon or service is listening for connections
Qualifier	Text string that augments the Daemon/Service name

Examples**Example 2-78 Listing Daemons in Short Form**

This example lists the names of all daemons.

```
ob> lsdaemon --short
observiced
obixd
obscheduled
```

Example 2-79 Listing Daemons in Long Form

This example lists the daemons in long form.

```
ob> lsdaemon --long
Process ID:          9418
  Daemon/Service:    observiced
  State:              debug
  Listen port:        400
  Qualifier:          (none)
Process ID:          12652
  Daemon/Service:    obixd
  State:              normal
  Listen port:        43983
  Qualifier:          brhost2
Process ID:          9436
  Daemon/Service:    obscheduled
  State:              normal
  Listen port:        42130
  Qualifier:          (none)
```

Example 2-80 Listing Daemons in Default Form

This example lists daemon information in the default table format.

```
ob> lsdaemon
Process ID  Daemon/Service  State  Listen port  Qualifier
-----
9418  observiced  debug  400
12652  obixd  normal  43983  brhost2
9436  obscheduled  normal  42130
```

2.1.60 lsdev

Purpose

Use the `lsdev` command to list the names and attributes of one or more configured devices.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsdev` command.

Syntax

`lsdev::=`

```
lsdev [ --long/-l | --short/-s ] [ --inservice/-o | --notinservice/-O ]
[ --reservations/-v | --mount/-m | --description/-d | --borrowed/-b ]
[ --nocomm/-N ] [ --reserved/-r [ --me/-e ] ] [ --nohierarchy/-H ]
[ --notype/-T ] [ --geometry/-g ] [ --verbose/-V ] [--consumption/-c]
[ --attach/-a aspec ] [ --type/-t { cloudstorage| tape | library | cap | disk } ]
devicename...
```

Semantics

--long/-l

Displays data in long form. The command displays the attributes of each device and labels them. Refer to [Example 2-81](#) (page 2-137) for sample output. By default the command displays the device name, type, and status.

--short/-s

Displays data in short form. The command prints the name of each device on a separate line.

--inservice/-o

Displays a list of devices that are logically available to Oracle Secure Backup.

--notinservice/-O

Displays a list of devices that are not logically available to Oracle Secure Backup.

--reservations/-v

Display device reservation data, for example, the name of reserving component, and so forth. You can use the [resdev](#) (page 3-96) command to reserve a device and the [unresdev](#) (page 3-150) to unreserve a device.

--mount/-m

Displays a list of devices with their mount status.

--description/-d

Displays a list of devices with detailed descriptions. For any device missing a description, run the `pingdev devicename` command to create one.

--borrowed/-b

Displays a list of devices with their borrowed status.

--nocomm/-N

Suppresses communication with the device.

--reserved/-r

Lists only those devices that are currently reserved.

--me/-e

Displays devices that are reserved for the logged-in [Oracle Secure Backup user](#). Use with the `--reserved` option.

--nohierarchy/-H

For a [tape library](#), suppresses the display of the tape drives contained in the tape library. By default, display of a tape library also displays the contained tape drives.

--notype/-T

Displays a list of devices without specifying the type ([tape drive](#) or [tape library](#)).

--geometry/-g

Displays the geometry and other characteristics of a tape library.

This option causes an Inquiry command to be sent to the tape device. While not a requirement of the SCSI-2 standard, most modern tape drives and libraries support the Unit Serial Number Inquiry Page, by which a device can be programmatically interrogated as to its serial number. In response, the device returns the resulting vendor, product ID, firmware version, and serial number.

--verbose/-V

Produces verbose output (default). For each device `obtool` displays the device type, name, and status.

--attach/-a *aspec*

Displays the device with the specified [attachment](#). Refer to "[aspec \(page 4-1\)](#)" for a description of the `aspec` placeholder.

--consumption/-c

Displays the amount of space currently used by each disk pool. Oracle Secure Backup also displays a percentage value that represents the percentage of disk pool capacity that has been used.

--type/-t *cloudstorage | tape | library | cap | disk*

Displays the specified type of device: `cloudstorage`, `tape`, `library`, `cap` or `disk`. The `cap` value applies only to ACSLS systems. For ACSLS, the long output of `tape` and `cap` show the appropriate `acs`, `lsm`, `panel`, `ID` information, `access mode` and `priority`.

devicename

Specifies the name of the device for which you want to view attribute data. Refer to "[devicename \(page 4-12\)](#)" for the rules governing device names.

Output

[Table 2-8](#) (page 2-135) describes the output for the `lsdev` command.

Table 2-8 lsdev Output

Label	Indicates
Device type	Type of device. Setting is <code>cloudstorage</code> , <code>tape drive</code> , <code>library</code> , or <code>disk</code> . If the device object was created with the <code>mkdev --class vtl</code> option, then the device type listed by <code>lsdev</code> includes <code>(VTL)</code> .
Model	Manufacturer model, if available
Serial number	Manufacturer serial number, if available
In service	Device eligibility for use. Setting is <code>yes</code> or <code>no</code> .
Debug mode	Assists in troubleshooting problems. Setting is <code>yes</code> or <code>no</code> .
Barcode reader	Setting is <code>yes</code> , <code>no</code> , or <code>default</code>
Barcodes required	Setting is <code>yes</code> , <code>no</code> , or <code>default</code> . If it is set to <code>yes</code> , then tapes must be barcoded to run a backup job
Auto clean	Automatically clean the tape drive heads. Setting is <code>yes</code> or <code>no</code> . Configured separately
Clean interval	Amount of time between cleaning
Clean using emptiest	Use cleaning tape with the most remaining cleanings available. Setting is <code>yes</code> or <code>no</code> .
Unload required	Setting is <code>yes</code> or <code>no</code> .
UUID	Universal Unique Identifier (UUID) for the hardware
Attachment #	Starts at 1 and increments for multiple tape drives or libraries
Host	Host name of the media server
Raw device	Device-specific file name: <code>/dev/rbl#</code> for a tape library and <code>/dev/rbt#</code> for a tape drive
Library	User-assigned Oracle Secure Backup name for the tape library
DTE	Number of the tape drive in the tape library
Automount	Automatically mounts the tape device. Setting is <code>yes</code> or <code>no</code> .
Error rate	Maximum number of errors for each tape before backup job fails

Table 2-8 (Cont.) Isdev Output

Label	Indicates
Position interval	<p>During a backup, Oracle Secure Backup periodically samples the position of the tape. Position interval is the distance between samplings of the tape position expressed in 1KB blocks. Possible values include:</p> <ul style="list-style-type: none"> • [undetermined] The device was not asked what the current position interval is, because the <code>--description</code> option was not specified. • [positioning unsupported] The tape drive does not support positioning. • [positioning disabled in operations policy] An Oracle Secure Backup user has disabled position querying in the operations policy. • <i>interval</i> (from index policy) An Oracle Secure Backup user has specified the indicated position interval in the index policy. • <i>interval</i> (from object) The tape drive has a particular position interval specified in the device object. • <i>interval</i> (from driver) The device driver has decided on the indicated position interval.
Blocking factor	The default value is 128. This value should not be changed arbitrarily because, if you choose a value higher than what is supported by the operating system of the server, then Oracle Secure Backup terminates with an error.
Max blocking factor	Set at optimum value by Oracle Secure Backup. Oracle recommends that you not change these values
Current tape	Original storage element of the tape currently in the DTE in addition to other information about the tape
Use list	Tapes residing in storage elements assigned for this tape drive to use
Drive usage	Amount of time since first use or since last cleaning
Cleaning required	Tape drive cleaning is required. Setting is <code>yes</code> or <code>no</code>
Consumption	Amount of space used by the disk pool or cloud storage device. The value in brackets indicates the percentage of disk pool capacity that has been utilized.
Reclaimable space	Amount of space in the disk pool or cloud storage device that can be freed by deleting expired backup image instances.
Capacity	Total capacity of the disk pool or cloud storage device.
Free space	Percentage of disk pool capacity that the disk pool manager must maintain by proactively deleting expired backup image instances.
Concurrent jobs	Maximum number of jobs that can run concurrently for this disk pool or cloud storage device. This includes backup, restore, and copy instance jobs.
Staging	Whether staging is enabled.
Stage rules	A list of stage rules.
User name	Name of the Oracle Cloud user account. This user account belongs to the defined identity domain.
Container	The name of the Oracle Secure Backup Oracle Cloud container

Table 2-8 (Cont.) Isdev Output

Label	Indicates
Storage class	The cloud storage class, either object or archive.
Segment size	The size specified for segments in the container. (Oracle Secure Backup splits each backup image into multiple segments.)
Streamsperjob	The number of threads created for parallel uploads of backup data.
Number of objects	The number of objects in the cloud container. (Oracle Secure Backup stores each segment as a single object in a cloud container.)
Bytes used	The actual number of bytes consumed in the cloud container. This value includes additional metadata, and possibly uncatalogued backup data, not reported by consumption.
Proxy	The proxy server URL, if the connection to Oracle Cloud is through a proxy server.
Proxy user	The proxy server user name.

Examples

Example 2-81 Listing Details for a Library

This example lists detail for a tape library named `filer_ethel_mc3`.

```
ob> lsdev --long filer_ethel_mc3
filer_ethel_mc3:
  Device type:      library
  Model:           ATL
  In service:      yes
  Debug mode:      no
  Barcode reader:  default (hardware-selected)
  Barcodes required: no
  Auto clean:      no
  Clean interval:  (not set)
  Clean using emptiest: no
  Unload required: yes
  UUID:           8249461c-585c-1027-85c6-000103e0a9fc
  Attachment 1:
    Host:          filer_ethel
    Raw device:    mc3
filer_ethel_nrst7a:
  Device type:      tape
  Model:           Quantum
  In service:      yes
  Library:         filer_ethel_mc3
  DTE:            1
  Automount:      yes
  Error rate:      8
  Position interval: [undetermined]
  Debug mode:      no
  Blocking factor: (default)
  Max blocking factor: (default)
  Current tape:    1
  Use list:        all
  Drive usage:     none
  Cleaning required: no
  UUID:           82665aa4-585c-1027-85c6-000103e0a9fc
  Attachment 1:
```

```

        Host:                filer_ethel
        Raw device:          nrst7a
filer_ethel_nrst8a:
  Device type:              tape
  Model:                    Quantum
  In service:                yes
  Library:                  filer_ethel_mc3
  DTE:                      2
  Automount:                yes
  Position interval:        [undetermined]
  Debug mode:                no
  Blocking factor:          (default)
  Max blocking factor:      (default)
  Current tape:             [unknown]
  Use list:                  all
  Drive usage:              [not set]
  Cleaning required:        [unknown]
  UUID:                     82667cdc-585c-1027-85c6-000103e0a9fc
  Attachment 1:
    Host:                    filer_ethel
    Raw device:              nrst8a

```

Example 2-82 Displaying Space Consumption Details for a Disk Pool

This example displays the amount of space occupied by backup image instances in the disk pool `dp1`. Under Consumption, the percentage value in brackets represents the percentage of total space on the disk pool that is used.

```

ob> lsdev -l dp1

dp1:
  Device type:              disk pool
  In service:                no
  Debug mode:                no
  Capacity:                  10.0 MB
  Consumption:               576.0 KB (5%)
  Reclaimable space:        576.0 KB (5%)
  Free space goal:          (system default)
  Concurrent jobs:          1
  Blocking factor:          (default)
  Max blocking factor:      (default)
  UUID:                      f712590d-97b4-4a33-86a5-8c6ba5f25655
  Staging:                   no
  Stage rules:               aaaaa, bbbbb, ccccc, ddddd
  Attachment 1:
    Host:                     MY-LAP
    Directory:                 c:/diskpool2

```

Example 2-83 Listing Details for a Cloud Storage Device

This example lists details for a cloud storage device named `clo`.

```

ob> lsdev -l clo

clo:
  Device type: cloud storage
  In service: yes
  Debug mode: no
  Capacity: 400.0 GB
  Consumption: 55.5 GB (13%)
  Reclaimable space: 62.4 MB (0%)
  Free space goal: (system default)
  Concurrent jobs: 4

```

```
Blocking factor: (default)
Max blocking factor: (default)
UUID: cd83d04e-7977-1035-83a5-fa163e178731
Attachment 1:
  Host: brhost3
Staging: no
URL: example.storage.oraclecloud.com
Username: jsmith@example.com
Container: ndisk
Storage class: object
Identity domain: example
Segment size: (system default)
Streams per job: (system default)
Number of objects: 8478
Bytes used: 55.9 GB
```

2.1.61 lsds

Purpose

Use the `lsds` command to list [dataset file](#) and [dataset directory](#) names.



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsds` command.

Syntax

```
lsds::=
```

```
lsds [ --long/l | --short/-s ] [ --recursive/-r ] [ dataset-dir-name ]
```

Semantics

--long/-l

Displays data in long form, which means that `obtool` labels the top-level directory. Refer to [Example 2-84](#) (page 2-140) for sample output. This option is the default.

--short/-s

Displays data in short form, which means that `obtool` does not label the top-level directory.

--recursive/-r

Recursively displays directories and dataset files under the specified directory.

dataset-dir-name

Specifies the name of a [dataset directory](#) assigned with `mkds` (page 3-21) or `rends` (page 3-85). Refer to "[dataset-dir-name](#) (page 4-7)" for a descriptions of the `dataset-dir-name` placeholder.

Example

Example 2-84 Displaying the Contents of a Dataset Directory

This example changes into the root of the dataset directory tree, displays the path, and then displays the contents of the directory.

```
ob> cdds /
ob> pwdds
/ (top level dataset directory)
ob> lsds
Top level dataset directory:
mydatasets/
tbrset/
admin_domain.ds
basicsummary.ds
```

2.1.62 lsdup

Purpose

Use the `lsdup` command to list information about duplication policies.



See Also:

["Volume Duplication Commands \(page 1-22\)"](#)

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsdup` command.

Syntax

`lsdup` (page 2-140)::=

```
lsdup [ --short/-s | --long/-l ] [ policyname ]...
```

Semantics

--short/-s

Displays duplication policy information in short form.

--long/-l

Displays duplication policy information in long form.

policyname

Specifies the name of a duplication policy.

Example

Example 2-85 Listing Information About Duplication Policies

This example lists the details of the duplication policy `vo1dup1` created in [Example 3-11](#) (page 3-25).

```
ob> lsdup
voldup1
ob> lsdup --long voldup1
voldup1:
  Migrate:                no
  Trigger:                firstwrite : forever
  Restriction 1:         @brhost3
  Rule 1:                 RMAN-DEFAULT : 2
  UUID:                  db4bfd64-18af-1031-b040-00163e527899
```

2.1.63 lsdw

Purpose

Use the `lsdw` command to list duplication windows.



See Also:

"[Duplication Window Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `lsdw` command.

Syntax

`lsdw::=`

```
lsdw [ --short/-s ] day-specifier[,day-specifier]...
```

Semantics

--short/-s

Displays duplication window information in short form.

2.1.64 lsfs

Purpose

Use the `lsfs` command to list file systems on an [Network Attached Storage \(NAS\)](#) device accessed through [Network Data Management Protocol \(NDMP\)](#).

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lsfs` command.

Syntax

`lsfs::=`

```
lsfs [ --short/-s | --long/-l ] [ --noheader/-H ]
[ --host/-h hostname[,hostname]... ]
[ --logical/-L | --physical/-P ] [ filesystem-name ]...
```

Semantics

--short/-s

Displays file-system data in short form.

--long/-l

Displays file-system data in long form.

--noheader/-H

Suppresses the display of headings.

--host/-h *hostname*

Specifies the name of the host on which the file system resides.

--logical/-L

Indicates that *filesystem-name* is a logical [volume](#) name.

--physical/-P

Indicates that *filesystem-name* is a physical volume name.

filesystem-name

Specifies the name of a file system that resides on the host.

Output

[Table 2-9](#) (page 2-142) describes the output format of the `lsfs` command.

Table 2-9 lsfs Output

Column	Indicates
File-system type	File-system type
File-system status	File-system status; setting is <code>online</code> or <code>offline</code>
Logical volume	Operating system-defined disk volume or partition
Total space	Capacity of Logical Volume
Used space	Amount of disk space used
Total inodes	Number of inodes
Used inodes	Number of used inodes

Example

Example 2-86 Listing File Systems on an NDMP Host

[Example 2-86](#) (page 2-142) displays the file system on the NDMP-accessed host named `br_filer`.

```
ob> lshost
br_filer      client                               (via NDMP) in service
brhost2      client                               (via OB)   in service
brhost3      mediaserver,client                   (via OB)   in service
osbsvr1      admin,mediaserver,client             (via OB)   in service
ob> lsfs --host br_filer --long
```

```

/vol/vol0:
  File system type:      WAFL
  File system status:   online
  Total space:          104.5 GB
  Used space:           71.8 GB
  Available space:      32.7 GB
  Total inodes:         11,164,856
  Used inodes:          4,846,130
ob> lsfs --host br_filer --short
/vol/vol0
ob> lsfs --host br_filer
FS Type  FS Status  Logical Volume  Total Size  Used Size  % Full
WAFL     online    /vol/vol0      104.5 GB   71.8 GB   68.7

```

2.1.65 lshost

Purpose

Use the `lshost` command to display the names and attributes of one or more configured hosts.



See Also:

"Host Commands (page 1-16)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lshost` command.

Syntax

`lshost::=`

```

lshost [ --long/-l | --short/-s ] [ --inservice/-o | --notinservice/-O ]
 [ --unauthenticated/-U ] [ --noroles/-R ] [ --roles/-r role[,role]...
 [ {--admin/-A | hostname} ]...

```

Semantics

--long/-l

Displays host data in long form, which means that `obtool` displays all attributes and labels them. By default `obtool` displays a subset of these attributes in tabular form.

--short/-s

Displays host data in short form, which means that `obtool` displays only the host names.

--inservice/-o

Lists hosts that are logically available to Oracle Secure Backup.

--notinservice/-O

Lists hosts that are not logically available to Oracle Secure Backup.

--unauthenticated/-U

Lists hosts that are not authenticated by the administrative host.

Note that you cannot use the `--unauthenticated` parameter in conjunction with the `--inservice` and `--notinservice` parameters.

--noroles/-R

Suppresses the display of role information.

--roles/-r *role*

Lists hosts having the specified `roles`. Refer to "`role` (page 4-25)" for a description of the `role` placeholder.

--admin/-A *hostname*

Specifies the name of the host computer for which to list data.

Output

[Table 2-10](#) (page 2-144) describes the output of the `lshost` command.

Table 2-10 lshost Output

Label	Indicates
Access mode	Setting is <code>OB</code> or <code>NDMP</code> . You can use <code>NDMP</code> as the access mode for Oracle Secure Backup clients and media servers. For the administrative server, you can use only <code>OB</code> as the access mode <code>OB</code> indicates the host has Oracle Secure Backup installed (on UNIX, Linux, or Windows computer) and uses Oracle Secure Backup internal communications protocol to communicate. <code>NDMP</code> indicates the host does not have Oracle Secure Backup installed (for example, a filer/Network Attached Storage (NAS) device) and uses the Network Data Management Protocol (NDMP) to communicate.
IP names	Indicates the IP address of the host computer
Algorithm	Indicates the encryption algorithm used
Encryption policy	Indicates whether encryption is required or allowed. If set to <code>required</code> , then all backups from this host are encrypted. If set to <code>allowed</code> , then encryption is determined by the global encryption policy and backup job-specific encryption settings. Default is <code>required</code> .
Rekey frequency	Indicates how often a key is generated
Key type	Indicates how the encryption keys are generated
In service	Host is eligible for use; setting is <code>yes</code> or <code>no</code>
Roles	Type of role; setting is <code>client</code> , <code>admin</code> , or <code>media server</code>
Trusted host	Specifies whether this is a trusted host or not. See <i>Oracle Secure Backup Installation and Configuration Guide</i> for more information on trusted hosts.
Any network	Specifies whether Oracle Secure Backup daemons listen for and accept connections from any network interface; setting is <code>default</code> , <code>yes</code> or <code>no</code>
Certificate key size	Specifies the size (in bits) of the public key/private key pair used with the identity certificate for this host
UUID	Universal Unique Identifier; assigned by Oracle Secure Backup

Table 2-10 (Cont.) lshost Output

Label	Indicates
NDMP port	Specifies the TCP port number used for NDMP on NDMP servers (see " port (page 7-30)")
NDMP user name	Specifies the name used to authenticate Oracle Secure Backup to an NDMP server (see " username (page 7-31)")
NDMP password	Specifies the password used to authenticate Oracle Secure Backup to an NDMP server (see " password (page 7-29)")
NDMP backup type	Specifies a default backup type for an NDMP server (see " backuptype (page 7-29)")
NDMP protocol version	Specifies an NDMP protocol version for an NDMP server (see " protocolversion (page 7-30)")
NDMP auth type	Specifies the means by which the Oracle Secure Backup NDMP client authenticates itself to an NDMP server (see " authenticationtype (page 7-28)")
S/w compression	Specifies the compression option to be used for all file system backups in this Oracle Secure Backup client, where it is not set at the job level

Example**Example 2-87 Displaying Host Information**

This example displays information in short form about all hosts and then displays information about `brhost2` in long form.

```
ob> lshost
brhost2      client                (via OB)  in service
brhost3      mediaserver,client    (via OB)  in service
br_filerc    client                (via NDMP) in service
osbsvr1      admin,mediaserver,client (via OB)  in service

ob> lsh -l brhost2
brhost2:
  Access mode:          OB
  IP names:             126.1.1.2
  Disable RDS:         not set (system default)
  TCP/IP buffer size:  not set (global policy)
  S/w compression:    (not set)
  Algorithm:           aes192
  Encryption policy:   allowed
  Rekey frequency:    1 month (system default)
  Key type:            transparent
  In service:         yes
  Roles:              client
  Trusted host:       no
  Certificate key size: 3072
  UUID:               c8d15fd2-2ee3-1035-a955-00163e43c05f
```

2.1.66 lsinstance

Purpose

Use the `lsinstance` command to display information about backup image instances.

Prerequisites

You must have the [list any backup, regardless of its owner](#) (page 8-4) or [list any backups owned by user](#) (page 8-4) class right to use the `lsinstance` command.

Syntax

`lsinstance::=`

```
lsinstance
[--long/-l | --short/-s] [--noheader/-H] [--sections/-S]
[--type/-Y {database | filesystem}] [--ctype/-y {tape | disk | cloudstorage}]
[ {[--from/-f date-time] [--to/-t date-time]} | [--today/-T] ]
[--duplicates/-D] [--expired/-e] [--host/-h hostname]...
[ [--barcode/-b tag]... | [--container/-c backup-container]... |
[--uuid/-u backup-instance-uuid]... | backup-instance-name... ]
```

Semantics

Refer to "[cpinstance](#) (page 2-80)" for descriptions of options that are not included in this section.

--long/-l

Specifies that all the attributes pertaining to each backup image instance must be displayed.

--short/-s

Displays only the names of backup image instances.

--noheader/-H

Omits displaying the headers in the command output.

--sections/-S

Displays the backup sections that are used to store the data corresponding to the backup image instance.

--type/-Y {database | filesystem}

Limits the display of backup image instances to the specified type. Use `database` for backup image instances that are created for Oracle Database jobs. Use `filesystem` for backup image instances created for file-system backups.

--ctype/-y {tape | disk | cloudstorage}

Displays backup image instances that are stored on the specified type of backup container. Use `tape` to display backup image instances stored on tape. Use `disk` to display details about backup image instances stored on disk pools. Use `cloudstorage` to display backup image instances stored on cloud storage devices.

--from/-f *date-time*

Displays backup image instances that were created since the specified date or time. Refer to "[date-time](#) (page 4-9)" for a description of the `date-time` placeholder.

--today/-T

Displays backup image instances that were created today.

--duplicates/-D

Displays duplicate volumes for backup image instances that are stored on tape. Duplicate volume containers are denoted by a "+" in the command output.

--expired/-e

Displays all the expired backup image instances.

--host/-h *hostname*

Displays backup image instances for the specified host.

--barcode/-b

Displays only backup image instances stored on a volume that has the specified barcode.

 **Note:**

You can use one of the following options in an `lsinstance` command: `--barcode`, `--container`, `--uuid`, and `instance-spec`.

Examples**Example 2-88 Listing Duplicate Volumes for Backup Image Instances**

This example displays the duplicate volumes for backup image instances. The details for each instance include the creation time and the backup container on which the backup image instance is stored.

```
ob> lsinstance --duplicates
      Instance Name          Created          Container(s)
brhost2-20121116-145737.1    2012/11/16.06:57 VOL000001
brhost2-20121116-145901.1    2012/11/16.06:59 mfl-000001,mfl-dup-000001+,
                                                                    mfl-000002,mfl-dup-000002+,
```

Example 2-89 Displaying Backup Image Instance Details in Long Format

The following example displays the details of the backup image instance `brhost2-20120503-163309.1` using the long format.

```
ob> lsinstance --long brhost2-20120503-163309.1
Instance name:  brhost2-20120503-163309.1
Type:           file system
Client:         brhost2
Backup level:   0
Container:      pool
Encryption:     off
Created:        2012/05/03.09:33
Expires:        2012/05/03.09:34
Created by job: admin/2.1
UUID:          4b194612-77a6-102f-b437-00163e3e5439
```

Example 2-90 Displaying Backup Sections for a Backup Image Instance

The following example displays the backup sections associated with the backup image instance `brhost2-20130329-123910.1`.

```

ob> lsinstance --sections --long brhost2-20130329-123910.1
Instance name:      brhost2-20130329-123910.1
Type:               file system
Client:             brhost2
Backup level:      0
Container:         spantape-2-000001 (3bf4b0347ad6103bcac00163e309d9f)
                   spantape-2-000002 (3c4f18127ad61038ebd00163e309d9f)
                   spantape-2-000003 (3ca975967ad6103ae8b00163e309d9f)

Encryption:       off
Created:           2013/03/29.05:39
Created by job:    admin/9.1
UUID:             4147ca4e-7ad6-1030-b076-00163e309d9f
Backup Section OID: 107
  File:            1
  Section:         1
  Size:            1.1 MB
  UUID:           4147ca62-7ad6-1030-b076-00163e309d9f
Backup Section OID: 108
  File:            1
  Section:         2
  Size:            1.1 MB
  UUID:           476e32aa-7ad6-1030-b076-00163e309d9f
Backup Section OID: 109
  File:            1
  Section:         3
  Size:            6.0 MB
  UUID:           4a728762-7ad6-1030-b076-00163e309d9f

```

Example 2-91 Displaying Staging Information in Long Format

This example shows the `Stage state` and `Stage rule` fields which are displayed if the instance is created by a `copyfromstage` job that copied the instance to another disk pool device that had staging enabled, and that device then used staging again to copy the instance to another device.

```

ob> lsinstance --long
Instance name:      brhost2-20151015-170355.1
Type:               file system
Client:             brhost2
Backup level:      0
Container:         pool1
Encryption:       off
Created:           2015/10/15.10:03
Expires:           2015/10/15.10:03
Stage state:       stage-complete
Stage rule:        mystagingrule
Created by job:    admin/3.1
UUID:             5177a230-55c7-1033-a532-00163e566d4e
ob>

```

The `Stage rule` field displays the name of the stage rule that resulted in the instance being created. This field is displayed only if the instance was created because of a `copyfromstage` job.

The `Stage state` line is displayed for instances in a disk pool device that are either in the state `stage-in-progress`, or `stage-complete`. This line is not shown for instances in the state, `not-staged`.

2.1.67 lsjob

Purpose

Use the `lsjob` command to obtain the status of the following kinds of scheduled jobs:

- Backup
- Restore
- Duplication
- Scan control
- Media movement
- Copy instance

You can select which jobs to display by date, status, and the degree of detail to display. Each job is assigned an identifier consisting of the username of the logged in [Oracle Secure Backup user](#), a slash, and a unique numeric identifier. An example of a job identifier is `admin/15`.

The `lsjob` command shows all active and pending jobs, with one line for each job, as shown below:

```
ob> lsj -A
Job-ID      Sched time  Contents                               State
admin/1     none       dataset tbrset/entire_backup          completed successfully at 2010/08/17.07:57
admin/1.1   none       backup brhost2                       completed successfully at 2010/08/17.07:57
admin/2     none       restore 1 item to brhost2            completed successfully at 2010/08/17.07:58
```



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to list another user's jobs, then you must have the right to [list any job, regardless of its owner](#) (page 8-5). If you are attempting to list your own jobs, then you must have the right to [list any jobs owned by user](#) (page 8-5).

Syntax

`lsjob::=`

```
lsjob
[ --active/-a ][ --complete/-c ][ --pending/-p ]
[ --inputrequest/-i ][ --all/-A ]
[ { [ --from/-f date-time ] [ --to/-t date-time ] } |
  [ --today/-T ] ]
[ --timescheduled/-e ][ --type/-Y job-type[,job-type]... ]...
[ --host/-h hostname ][ --dataset/-D dataset-name ]
[ --piecename/-E piecename[,piecename]... ]
[ --dbname/-d dbname[,dbname]... ][ --dbid/-I dbid[,dbid]... ]
[ --system/-y | { --username/-u username } | --me/-m ]
[ --superseded/-S ] [ --subjobs/-j | --primary/-P ]
```

```
[ { --short/-s [ --oneperline/-1 ] } | --long/-l ]  
[ --noheader/-H ] [ --results/-r ] [ --progress/-o ] [ --requires/-R ]  
[ --times/-C ] [ --log/-L ] [ --catalog/-G ]  
job-id...
```

Semantics

Use these options to select the jobs to be shown. If you specify no state-based options, then `obtool` displays only active and pending jobs. Multiple options are additive.

State-based job options

Use these options to filter jobs by status. Refer to [Example 2-92](#) (page 2-154) for an illustration.

--active/-a

Shows active jobs, that is, jobs that are currently being processed. By default the `lsjob` command displays active and pending jobs.

--complete/-c

Shows jobs that completed either successfully or unsuccessfully.

--pending/-p

Shows pending jobs, that is, jobs that are not running and are scheduled to be processed in the future. By default the `lsjob` command displays active and pending jobs.

--inputrequest/-i

Shows jobs currently requesting input. For example, a job might require input if you try to restore a backup from a multivolume [volume set](#) while using a standalone [tape drive](#) or if a [volume](#) required for a restore operation is not available in a [tape library](#).

--all/-A

Shows jobs in all states.

job-id

Specifies the job ID of the [scheduled backup](#) and restore job whose status you want to obtain.

Time-based job options

Use these options to filter jobs according to when their state was updated or when they were scheduled to run. Refer to [Example 2-93](#) (page 2-154) for an illustration.

--from/-f date-time

Shows only jobs whose state was updated at *date-time* or later. For example, show jobs that went from pending to active in the last day. Refer to "[date-time](#) (page 4-9)" for the *date-time* placeholder.

--to/-t date-time

Shows only jobs whose state was updated at *date-time* or before. For example, show jobs that went from pending to active before yesterday. Refer to "[date-time](#) (page 4-9)" for the *date-time* placeholder.

--today/-T

Shows only jobs whose state was updated today.

--timescheduled/-e

Uses scheduled time as a selection criteria instead of job modification time. Use either `--today` or `--from` to select the *date-time* range. If you specify neither option, then no constraint is applied to the *date-time* range.

Type/hostname/dataset-based job options

Use these options to filter jobs according to job type, host name, or [dataset](#) identifier. Refer to [Example 2-94](#) (page 2-154) for an illustration.

--type/-Y *job-type*[*job-type*]...

Shows only job entries of the specified type. By default `obtool` displays all types. Refer to "[job-type](#) (page 4-17)" for the *job-type* placeholder.

--host/-h *hostname*

Shows only job entries related to the specified host.

--dataset/-D *dataset*

Shows only job entries related to the specified [dataset file](#). Run the `lsds` (page 2-139) command to display dataset file information.

 **Note:**

When the `--dataset` and `--host` options are both specified, the output of the `lsjob` command is null. The reason is that `lsjob` run with only `--dataset` specified shows no host information, while `lsjob` run with only `--host` specified shows no dataset information.

Username-based job options

Use these options to filter jobs according to who initiated them. Refer to [Example 2-95](#) (page 2-154) for an illustration.

--system/-y

Shows jobs scheduled by Oracle Secure Backup.

--username/-u *username*

Shows jobs belonging to *username*. Run the `lsuser` (page 2-180) command to display all Oracle Secure Backup users.

--me/-m

Shows jobs belonging to the currently logged in Oracle Secure Backup user. Run the `id` (page 2-100) command to display the current Oracle Secure Backup user.

Miscellaneous job options

Use these options to filter jobs according to miscellaneous criteria.

--superseded/-S

Shows jobs that were superseded before they were run.

A job is superseded when an identical job was scheduled after the initial job had a chance to run. For example, suppose you schedule an [incremental backup](#) scheduled every night at 9 p.m. On Wednesday morning you discover that the Tuesday night backup did not run because no tapes were available in the tape library. The

incremental backup scheduled for Wednesday supersedes the backup from the previous night.

--subjobs/-j

Shows subordinate jobs if the selected job has them (default). For example, `lsjob --primary` shows `sbt/25.1`, `sbt/25.2`, and `sbt/25.3` rather than just `sbt/25`.

--primary/-P

Shows only each primary job. For example, `lsjob --primary` shows `sbt/25` rather than `sbt/25.1`, `sbt/25.2`, and `sbt/25.3`.

Format control job options

Use these options to control the display of job information. Refer to [Example 2-96](#) (page 2-154) for an illustration.

--short/-s

Shows only job IDs.

--long/-l

Shows job information in labeled rather than column format.

--noheader/-H

Does not display column headers.

--oneperline/-1

Shows one job ID for each line when used with the `--short` option.

Content level job options

Use these options to filter jobs based on how much content to include. Refer to [Example 2-97](#) (page 2-155) for an illustration.

--results/-r

Shows results for completed jobs when used with the `--complete` option. For example, the results might look like the following:

```
saved 3.4 MB to VOL000003 (tag ADE202), file 12
ok: /home
```

--progress/-o

Shows the progress of active jobs when used with the `--active` option. For example, the progress might look like the following:

```
processed 3.1Mb, 42 files
```

No progress information is displayed for completed jobs, because the `--progress` option applies only to active jobs.

--requires/-R

Shows resources required to run each job. For example, jobs that can run on any device display "requires any device."

--times/-C

Shows all relevant times for each job. For example, the job times might look like the following:

introduced 2013/03/21.16:59, earliest exec 03/23.00:00, last update
2013/03/21.16:59, expires never

--log/-L

Shows the log associated with each job. The log shows data such as when the job was created, which host it was dispatched on, when it completed, and so forth.

--catalog/-G

Shows extended information about catalog recovery backups. Oracle Secure Backup also checks for catalog backup failures and generates an e-mail to the administrator if any are found.

Output

Table 2-11 (page 2-153) describes the output of the `lsjob` command.

Table 2-11 lsjob Output

Label	Indicates
Job ID	Unique Oracle Secure Backup identifier assigned to a scheduled backup or restore job
Type	The type of job. See " job-type (page 4-17)" for more information.
Level	Identifies a backup level. The default level is 0. Refer to " backup-level (page 4-4)" for more information.
Family	Identifies the media family to be used for the job.
Encryption	<p>on for backups encrypted by Oracle Secure Backup</p> <p>transient for backups encrypted by Oracle Secure Backup with a user-supplied one-time passphrase</p> <p>forcedoff for an on-demand backup that was not encrypted, overriding the host-required encryption setting</p> <p>off for backups that are not encrypted</p> <p>hardware for backups encrypted by an encryption-capable tape drive</p> <p>transient_hardware for transient backups encrypted by an encryption-capable tape drive</p> <p>RMAN for backups encrypted by Recovery Manager (RMAN)</p> <p>This field displays <code>awaiting job completion</code> for an RMAN backup job that has not completed. Only when the RMAN backup finishes does this field report the encryption state of the backup.</p> <p>See <i>Oracle Secure Backup Administrator's Guide</i> for more information on backup encryption.</p>
Scheduled time	Time job was scheduled to begin
Contents	Dataset that was used or host that was backed up
State	<p>State of the job; setting is <code>processed</code>, <code>pending</code>, <code>completed successfully</code>, <code>failed</code>, or <code>waiting for input since date-timestamp</code>.</p> <p>Note: The <code>waiting for input since date-timestamp</code> state means the job was running but is now blocked waiting for user input that can be supplied using rpyjob (page 3-137).</p>
Priority	Priority level of the job; 1 is the highest priority
Privileged op	Whether job requires administrator privileges
Run on host	Host on which the job runs

Table 2-11 (Cont.) lsjob Output

Label	Indicates
Attempts	Number of times Oracle Secure Backup attempted to run the job
S/w compression Status	Displays the S/w compression option considered for this job based on the compression setting

Examples**Example 2-92 Filtering Jobs by State**

This example shows jobs in completed state.

```
ob> lsjob --complete
Job ID      Sched time  Contents                                     State
-----
admin/1     none       dataset tbrset/entire_backup                completed successfully at 2013/02/13.10:11
admin/1.1   none       backup brhost2                             completed successfully at 2013/02/13.10:11
admin/2     none       restore 1 item to brhost2                  completed successfully at 2013/02/13.10:11
sbt/1       none       database tstvw1 (dbid=1586108579)          completed successfully at 2013/02/13.10:15
sbt/1.1     none       archivelog backup                          completed successfully at 2013/02/13.10:15
sbt/2       none       database tstvw1 (dbid=1586108579)          completed successfully at 2013/02/13.10:16
sbt/2.1     none       controlfile autobackup                     completed successfully at 2013/02/13.10:16
sbt/3       none       database tstvw1 (dbid=1586108579)          completed successfully at 2013/02/13.10:16
sbt/3.1     none       datafile backup                            completed successfully at 2013/02/13.10:16
sbt/4       none       database tstvw1 (dbid=1586108579)          completed successfully at 2013/02/13.10:17
sbt/4.1     none       restore piece '03ik5p7p_1_1'               completed successfully at 2013/02/13.10:17
```

Example 2-93 Filtering Jobs by Time

This example shows jobs that are active and pending today only.

```
ob> lsjob --today
Job ID      Sched time  Contents                                     State
-----
5           06/13.04:00 dataset datadir.ds                          processed; host backup(s) scheduled
```

Example 2-94 Filtering Jobs by Host

This example shows jobs in all states on host brhost2.

```
ob> lsjob --all --short --oneperline --host brhost2
admin/1.1
admin/2
```

Example 2-95 Filtering Jobs by User

This example shows active and pending jobs for Oracle Secure Backup user sbt.

```
ob> lsjob --user sbt
Job ID      Sched time  Contents                                     State
-----
admin/13    06/23.00:00 dataset fullbackup.ds              future work
```

Example 2-96 Displaying Job Data in Long Format

This example shows active and pending jobs in long format. The Created by user property shows "privileged" indicating that this is an on-demand job that included the --user option.

```
ob> lsjob --long
5:
  Type:                datadir.ds
  Level:               full
  Family:              full
  Encryption:          on
  Created by user:     privileged
  Scheduled time:      06/13.04:00
  State:               processed; host backup(s) scheduled
  Priority:             5
  Privileged op:       no
  Run on host:         (administrative server)
  Attempts:            1
```

Example 2-97 Displaying All Time-Related Data

This example shows all time-related data for active and pending jobs.

```
ob> lsjob --times
Job ID      Sched time  Contents                                     State
-----
5           06/13.04:00 dataset datadir.ds                       processed; host backup(s) scheduled
introduced 2013/02/13.13:37, earliest exec 06/13.04:00, last update
2013/02/13.13:37, expires 2013/03/13.04:00
```

Example 2-98 Displaying Subjob Data in Long Format

This example shows all major fields displayed as part of a subjob in long format.

```
ob> lsjob --long admin/4.1
admin/4.1:
  Type:                backup brhost2
  Level:               full
  Backup name format:  (system default)
  Family:              (null)
  Encryption:          off
  Disable h/w encryption: no
  Store catalog on media: yes
  S/w compression:     low
  Scheduled time:      none
  State:               completed successfully at 2017/06/09.00:10
  Priority:             100
  Privileged op:       no
  Run on host:         brhost3
  Attempts:            1
```

2.1.68 lsloc

Purpose

Use the `lsloc` command to display information about every [location](#) in the [administrative domain](#).



See Also:

"[Location Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsmf` command.

Syntax

```
lsloc::=
```

```
lsloc [ --short/-s | --long/-l ] location-name [ location-name ]...
```

Semantics

--short/-s

Displays data in short form. This option displays only location names.

--long/-l

Displays data in long form.

location-name

Specifies the name of the location to list. If you do not specify a *location-name*, then `obtool` displays all locations.

2.1.69 lsmf

Purpose

Use the `lsmf` command to display information about media families.



See Also:

["Media Family Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsmf` command.

Syntax

```
lsmf::=
```

```
lsmf [ --long/-l | --short/-s ] [ media-family-name ]...
```

Semantics

--long/-l

Displays data in long form. This option displays all [media family](#) attributes and labels them. By default the `lsmf` command displays the name and type of each media family.

--short/-s

Displays data in short form. This option displays only media family names.

media-family-name

Specifies the name of the media family to list. If you do not specify a *media-family-name*, then `obtool` displays all media families.

Output

[Table 2-12](#) (page 2-157) shows the output for the `lsmf` command.

Table 2-12 lsmf Output

Label	Indicates
Write window	Indicates the length of time during which writing to a volume set is permitted
Keep volume set	Amount of time (added to the length of time for the Write Window) before Volume Set expires; default equals <i>never</i>
Appendable	Indicates the volume is appendable; setting is <i>yes</i> or <i>no</i>
Volume ID used	Volume identifier; setting is either <i>system default</i> , unique to this media family, same as for media fam < >, or from file < >
Comment	Optional user-supplied description of this media family

Example**Example 2-99** Listing Media Family Information

[Example 2-99](#) (page 2-157) displays media family data in long format.

```
ob> lsmf --long
RMAN-DEFAULT:
  Keep volume set:      content manages reuse
  Appendable:          yes
  Volume ID used:      unique to this media family
  Comment:             Default media family for RMAN backup jobs
content-man-family:
  Write window:        forever
  Keep volume set:     content manages reuse
  Appendable:          yes
  Volume ID used:      unique to this media family
full_bkup:
  Write window:        10 days
  Keep volume set:     28 days
  Appendable:          yes
  Volume ID used:      unique to this media family
time-man-family:
  Write window:        7 days
  Keep volume set:     28 days
  Appendable:          yes
  Volume ID used:      unique to this media family
```

2.1.70 lsp

Purpose

Use the `lsp` command to list [defaults and policies](#).

The policy data is represented as a directory tree with / as the root. You can use [cdp](#) (page 2-27) to navigate the tree and `lsp` and [pwdp](#) (page 3-77) to display data.

See Also:

- ["Policy Commands](#) (page 1-18)" for related commands
- [Defaults and Policies](#) (page 7-1) for a complete list of policies and policy classes

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsp` command.

Syntax

`lsp::=`

```
lsp [ --short/-s | --long/-l ] [ --dir/-d ] [ --fullname/-f ] [ --novalue/-V ]  
[ --nodefault/-D | --defaultvalue/-v ] [ --type/-t ] [ policy-name ]...
```

Semantics

--short/-s

Displays data in short form (default). This option displays the policy name and setting and indicates whether the setting is the default value.

--long/-l

Displays data in long form. This option is identical to `--short` except that the output includes a brief description of each policy.

--dir/-d

Displays the directory of the specified policy.

--fullname/-f

Display the full path names of the selected policies.

--novalue/-V

Suppresses the display of policy values.

--nodefault/-D

Suppresses the display of default values of the selected policies.

--defaultvalue/-v

Displays the default values of the selected policies.

--type/-t

Displays policies by type.

policy-name

Specifies the name of the policy to display.

Examples

Example 2-100 Listing Log Policies

This example displays the full path name of log policies and suppresses the display of the policy defaults.

```

ob> pwdp
/
ob> lsp --nodefault --fullname --long logs
/logs/adminlogevents          (none)
    Names of events that are logged in the administrative server activity log.
/logs/adminlogfile            (none)
    Pathname of the administrative server activity log.
/logs/clientlogevents         (none)
    Names of events that are logged in each client's local log file.
/logs/jobretaintime           30 days
    Duration for which scheduler job database records are retained.
/logs/logretaintime           7 days
    Duration for which Oracle Secure Backup daemon log entries are retained.
/logs/transcriptretaintime     7 days
    Duration for which backup transcripts are retained.
/logs/unixclientlogfile        (none)
    Pathname of the local activity log file for all UNIX clients.
/logs/windowsclientlogfile     (none)
    Pathname of the local activity log file for all Windows clients.

```

Example 2-101 Listing Policies by Type

This example displays the policies in the class daemons.

```

ob> pwd
/
ob> lsp --type daemons
auditlogins                    no                    [default]
    yes-no
obixdmaxupdaters                2                    [default]
    uint min 1
obixdrechecklevel               structure             [default]
    enum none structure content
obixdupdaternicevalue           0                    [default]
    int
webautostart                    yes
    yes-no
webpass                          (set)
    text
windowscontrolcertificateservice no                    [default]
    yes-no

```

Example 2-102 Listing a Security Password Policy

This example sets the global [password reuse time](#) security policy to 180 days and lists the policy information.

```

ob> setp security/passwordreusetime 180days
ob> lsp --nodefault security/passwordreusetime
passwordreusetime              180 days

```

2.1.71 lspiece

Purpose

Use the `lspiece` command to display information about [Recovery Manager \(RMAN\) backup pieces](#). Backup pieces are the physical members of backup sets. One RMAN [backup piece](#) corresponds to one Oracle Secure Backup [backup image](#). Oracle Secure Backup stores and reports Oracle Database metadata about the contents of each backup piece.

Because the backup pieces might be available on different duplicate volumes as well, the `lspiece` command shows which volumes are at the [active location](#) or nearest [storage location](#).



See Also:

"[Backup Piece Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lspiece` command.

Syntax

`lspiece::=`

```
lspiece [ --long/-l | --short/-s ] [ --noheader/-H ] [ --section/-S ]
[ --oid/-o oid-list ]... [ --host/-h hostname[,hostname]... ]
[ --dbname/-d dbname[,dbname]... ]
[ --dbid/-i dbid[,dbid]... ]
[ --content/-c content[,content]... ]
[ { --vid/-v vid-list | --void/-V oid-list } ]
[ piecename ]...
```

Semantics

--long/-l

Displays data in long form.

--short/-s

Displays data in short form.

--noheader/-H

Does not display header row.

--section/-S

Lists the volume ID and backup sections used by the backup pieces. The volume ID is included with the `--long` output when you specify the `--section` option.

--oid/-o *oid-list*

Specifies one or more backup piece object identifiers. Refer to "[oid-list](#) (page 4-22)" for a description of the `oid-list` placeholder.

--host/-h *hostname*

Specifies the name of the host computer to which the listing applies.

--dbname/-d *dbname*

Specifies the names of the databases whose backup pieces you want to list.

--dbid/-i *dbid*

Specifies the DBIDs of the databases whose backup pieces you want to list.

--content/-c *content*

Specifies the types of backup information contained by the backup piece. Refer to "content (page 4-5)" for a description of the *content* placeholder.

--vid/-v *vid_list* | --void/-V *oid_list*

Specifies that only backup pieces contained on the volumes specified in *vid_list* or *oid_list* are displayed, possibly further restricted by other selection criteria options.

piecename

Specifies the names of the backup pieces to which the listing applies.

Output

[Table 2-13](#) (page 2-161) describes the output of the `lspiece` command.

Table 2-13 lspiece Output

Label	Indicates
Backup piece OID	The backup piece object identifier
Database	The name of the database that was backed up
Database ID	The DBID of the database that was backed up
Content	The content of the backup
Copy number	The backup piece copy number
Created	The creation date of the backup piece
Host	The database host
Piece name	The name of the backup piece
Encryption	Encryption enabled or disabled
Algorithm	The encryption algorithm used

If a date reported by `lspiece` is more than six months earlier, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier, then it is reported in a `mm/dd.hh:mm` format.

Example**Example 2-103 Displaying Backup Pieces**

The following example shows the output of an `lspiece --long` command:

```
ob> lspiece -l
Backup piece OID:      104
Database:             bugfix
Database ID:          1586108579
Content:              full
```

```

Copy number:          0
Created:              2009/01/14.16:34
Host:                 sales-server
Piece name:           05k4q4km_1_1
Encryption:           on
Algorithm:             aes128
Backup piece OID:     107
Database:              bugfix
Database ID:           1586108579
Content:               full
Copy number:          0
Created:              2009/01/14.16:48
Host:                 sales-server
Piece name:           08k4q5dj_1_1
Encryption:           RMAN
Backup piece OID:     108
Database:              bugfix
Database ID:           1586108579
Content:               full
Copy number:          0
Created:              2009/01/14.16:52
Host:                 sales-server
Piece name:           09k4q5me_1_1
Encryption:           forcedoff
Backup piece OID:     109
Database:              bugfix
Database ID:           1586108579
Content:               full
Copy number:          0
Created:              2009/01/14.16:55
Host:                 sales-server
Piece name:           0ak4q5rm_1_1
Encryption:           hardware
Algorithm:             aes256

```

Example 2-104 Displaying Volume ID Used by Backup Pieces

The following example lists the volume ID and backup sections used by backup pieces.

```

ob> lspiece -l -S
Backup piece OID:      100
Database:              oracle
Database ID:           1566049437
Content:               full
Copy number:          0
Created:              2009/07/23.15:07
Host:                 sales-server
Piece name:           03kks4m5_1_1
  BSOID:               100
  Volume ID:           RMAN-DEFAULT-000001
  File:                1
  Sect:                1
Encryption:           off

```

2.1.72 lspni

Purpose

Use the `lspni` command to list [PNI \(Preferred Network Interface\)](#) definitions.

 **See Also:**

"[Preferred Network Interface Commands](#) (page 1-19)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lspni` command.

Syntax

`lspni::=`

```
lspni [ server-hostname ]...
```

Semantics

server-hostname

Specifies the name of the server whose network interfaces are to be listed. If you do not specify a host name, then `obtool` displays all hosts that have a PNI created with the [mkpni](#) (page 3-40) command.

Output

[Table 2-14](#) (page 2-163) describes the output for the `lspni` command.

Table 2-14 lspni Output

Column	Indicates
PNI #	Sequential number, starting at 1, identifying the PNI for inbound connections to this host
UNI #	Identifies the only interface used a PNI for outbound connections from this host
ONI #	Sequential number, starting at 1, identifying the PNI for outbound connections from the host
interface	IP address of the interface
useonly	Only interface that must be used for outbound connections

Example

Example 2-105 Listing PNIs

This example displays the PNIs for servers `brhost2` and `brhost3`.

```
ob> lspni
brhost2:
  ONI 1:
    network:                198.51.100.1/8
    interface:              198.51.100.1
brhost3:
  ONI 1:
    network:                198.51.100.33/24
    interface:              198.51.100.33
```

2.1.73 lsrestore

Purpose

Use the `lsrestore` command to list restore requests. These requests are awaiting delivery to the [scheduler](#).



See Also:

"[Restore Commands](#) (page 1-19)" for related commands

Prerequisites

If you specified that the restore run in privileged mode, or if you are restoring files to a host accessed through [Network Data Management Protocol \(NDMP\)](#), then you must have the right to [perform file system restores as privileged user](#) (page 8-6) to use the `restore` command. Otherwise, you must have the right to [perform file system restores as self](#) (page 8-7).

Syntax

`lsrestore::=`

```
lsrestore [ --long/-l | --detail/-d | { --short/-s [ --oneperline/-1 ] } ]  
[ --position/-x ] [ --noheader/-H ] [ --raw/-R ] [ --catalog/-C ]  
[ restore-item ]...
```

Semantics

--long/-l

Displays restore request data in long form.

--detail/-d

Displays detailed data about the backup to be used in the restore.

--short/-s

Displays restore request data in short form. This item is the default.

--oneperline/-1

Shows one item for each line when used with the `--short` option.

--position/-x

Displays the position of the backup on tape when used with the `--detail` option.

--noheader/-H

Displays data without column headings.

--raw/-R

Displays only raw restore requests, that is, restore requests that do not make use of the Oracle Secure Backup [catalog](#). By default `lsrestore` lists all restore requests.

--catalog/-C

Displays only restore requests that use the Oracle Secure Backup catalog. If you specify `--catalog`, then `lsrestore` does not display raw restore requests. By default `lsrestore` lists all restore requests.

restore-item

Specifies the item number of a restore request. You can display the item numbers for restore requests by running `lsrestore` without any options.

Output

[Table 2-15](#) (page 2-165) describes the output for the `lsrestore` command.

Table 2-15 lsrestore Output

Column	Indicates
Item #	Sequential number, starting at 1, assigned to the restore job
Data saved from	Host and path of data that was backed up
Restore data to	Host and path of data to be restored
Host	Name of host the data is originally from or to which the host is restoring
Path	Operating system location of data on the file system
Priority	Priority of restore job
Created	Creation date of volume set
File number	File number of backup to be restored
Device	Name of device to be used for restore operation
Backup ID	Backup ID for backup to be restored
Volume ID	Volume ID for volume to be used in restore operation
Volume tag	Barcode for volume to be used in restore operation
File section	Backup section to be restored
Position	Position of backup data on tape

Example**Example 2-106 Listing Restore Requests**

[Example 2-106](#) (page 2-165) lists all restore requests in long format.

```
ob> lsrestore --long
1:
  Data saved from:
    Host:          brhost2
    Path:          /data/backup
  Restore data to:
    Host:          brhost3
    Path:          /tmp
  Priority:        100
  Created:        2012/12/02.12:37:07
  File number:    1
  Device:         tape1
  Backup ID:      1
  Volume ID:      VOL000003
  Volume tag:     ADE203
```

File section: 1
Position: 000000000009

2.1.74 lsrot

Purpose

Use the `lsrot` command to list information about rotation policies.



See Also:

"[Rotation Policy Commands](#) (page 1-20)"

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsrot` command.

Syntax

`lsrot::=`

```
[ --short/-s | --long/-l ] rotationname [ rotationname... ]
```

Semantics

--short/-s

Displays policy information in short form.

--long/-l

Displays policy information in long form.

rotationname

Specifies the name of a [rotation policy](#), which must be 1-31 characters.

2.1.75 lsrpt

Purpose

Use the `lsrpt` command to list media management reports.



See Also:

"[Reports Commands](#) (page 1-19)"

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsrpt` command.

Syntax

lsrpt::=

```
lsrpt [ --short/-s | --long/-l ] [ --type/-t reporttype [,reporttype...] ]
job-id ...
```

Semantics

--short/-s

Specifies short form listing.

--long/-l

Specifies long form listing.

--type *l-t reporttype*

Specifies one or more types of report to be displayed. Valid types are `distribution` and `pick`.

job-id

Specifies the identifiers of jobs whose reports are to be listed.

Example

Example 2-107 Listing Media Management Reports

This example lists details of the pick report seen in [Example 2-16](#) (page 2-22)

```
ob> lsrpt --long --type pick 2
2-pick.xml:
Volumes moved:
                VOL000001
Job status      :pending enable by operator
```

2.1.76 lssched

Purpose

Use the `lssched` command to display information about backup, vaulting scan, duplication scan, and stage scan schedules.



See Also:

"[Schedule Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lssched` command.

Syntax

lssched::=

```

lssched [ --short/-s | --long/-l ]
[ --calendar/-c year/month
[ --trigger trigger-number[,trigger-number]... ] ]
[ --type/-Y schedule-type[,schedule-type...] ]
[ --user/-u user-name]
[ schedulename ]...

```

Semantics

--short/-s

Displays schedule data in short form.

--long/-l

Displays schedule data in long form.

--calendar/-c year/month

Restricts display to schedule information in the given month and year.

--trigger trigger-number

Displays [backup schedule](#) information by trigger number. A [trigger](#) is a user-defined period in time or sets of times that causes a [scheduled backup](#) to run.

--type/-Y schedule-type

Specifies the type of schedule to be listed. Valid values are `backup`, `duplicationscan`, `vaultingscan`, and `stagescan`. Multiple schedule types can be specified.

--user/-u user-name

Displays schedules that must be run as Oracle Secure Backup user specified by *user-name*.

schedulename

Specifies the name of the schedule to display.

Output

[Table 2-16](#) (page 2-168) describes the output of the `lssched` command.

Table 2-16 Issched Output

Column	Indicates
Schedule name	User-supplied name identifying the schedule
Type	The schedule type: <code>backup</code> , <code>duplicationscan</code> , <code>vaultingscan</code> , or <code>stagescan</code>
Dataset	Dataset files used
Restrict	Device restrictions
Priority	Priority level of the schedule; set a number greater than 0; 1 is the highest priority
Encryption	Identifies encrypted backups. See <i>Oracle Secure Backup Administrator's Guide</i> for more information on backup encryption.
Comment	User-supplied comment
Trigger #	Instance number of this schedule
Day/date	Scheduled date for the job
At	Scheduled time for the job

Table 2-16 (Cont.) Issched Output

Column	Indicates
Backup level	Level of backup to be performed; setting is full, 1 to 10, incremental, or offsite
Media family	Media family to use
Expires after	When this trigger expires
State	Applies to all schedules. It is either the value enabled or disabled. A disabled schedule does not trigger any actions.
UUID	The unique identifier for the schedule.
Device #	A device number is not displayed when Type has a value of stagescan. .
S/w compression	The compression option to be used in the scheduled backup job.

If a date is more than 6 months earlier or more than 2 months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than 6 months earlier or less than 2 months in the future, then it is reported in a `mm/dd.hh:mm` format.

Examples

Example 2-108 Displaying Backup

This example displays detailed information about backup schedules.

```
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:                backup
  State:               enabled
  Dataset:             OSB-CATALOG-DS
  Priority:             50
  Encryption:          no
  S/w compression:    (not set)
  Comment:             OSB catalog backup schedule
  UUID:               9bf80a66-9026-1035-a574-fa163e8d3d94
  Trigger 1:
    Day/date:          (none)
    At:                00:00
    Backup level:      full
    Media family:      OSB-CATALOG-MF
    Backup name:       (system default)
full_backup:
  Type:                backup
  Dataset:             datadir.ds
  Priority:             5
  Encryption:          yes
  S/w compression:    basic
  UUID:               9bf80a29-9053-1044-a574-fa163e8d38454
  Trigger 1:
    Day/date:          thursdays
    At:                21:00
    Backup level:      full
    Media family:      (null)
  Trigger 2:
    Day/date:          weekdays
    At:                04:00
```

```
Backup level:      full
Media family:     full
Expires after:    30 days
```

Example 2-109 Displaying Backup for the Stage Scan Type

This example displays `lssched` command output for a `stagescan` schedule. Both the short and long forms are shown.

```
ob> lssched --type stagescan mystagescansched
mystagescansched  wednesdays
ob>

ob> lssched --type stagescan --long
mystagescansched:
  Type:                stagescan
  State:               enabled
  Priority:             50
  Comment:             daily stagescan schedule
  UUID:                8f6fbe36-af26-1093-a412-00123e56d54e
  Trigger 1:
    Day/date:          wednesdays
    At:                04:00
  Device 1:            diskdev1
    Stage Rules:       srule1, srule2, sruleminimumtime,
                      srule3, srule4
  Device 2:            diskdev1
    Stage Rules:       srule1, srule2, srule5
  Device 3:            diskdev1
    Stage Rules:       srule6, srule7, srule8
ob>
```

2.1.77 lssection

Purpose

Use the `lssection` command to list backup sections matching the criteria specified on the command line. A [backup section](#) is the portion of a [backup image](#) that occupies one physical [volume](#). Oracle Secure Backup obtains backup section data from the backup sections [catalog](#).

Because the backup sections might be available on different duplicate volumes as well, the `lssection` command shows which volumes are at the [active location](#) or nearest [storage location](#).



See Also:

"[Section Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lssection` command.

Syntax

Issection::=

```

Issection
  [ --long/-l | --short/-s ] [ --noheader/-H ]
  [ --incomplete/-i ] [ --oid/-o oid-list ]...
  [ { { --vid/-v vid-list } | { --void/-V oid-list } }
    [ --file/-f filenumber-list ]... ]

```

Semantics

--long/-l

Displays section data in long form.

--short/-s

Displays only the object ID of each backup section record selected.

--noheader/-H

Displays data without column headings.

--incomplete/-i

Displays section information even if the related volume data is missing from the backup sections catalog.

--oid *oid-list*

Selects backup sections with the object identifiers matching those in *oid-list*. Refer to "[oid-list](#) (page 4-22)" for a description of the *oid-list* placeholder.

--vid *vid-list*

Selects backup sections contained on the volumes whose IDs are supplied in *vid-list*. A *vid-list* is one or more *vid* values separated by commas. Refer to "[vid](#) (page 4-30)" for a description of the *vid* placeholder.

--void *void-list*

Selects backup sections contained on the volumes whose volume object identifiers are supplied in the list. The *void-list* placeholder represents an *oid-list* of volume IDs. Refer to "[oid-list](#) (page 4-22)" for a description of the *oid-list* placeholder.

--file/-f *filenumber-list*

Selects only those backup sections having the file numbers specified the list. Refer to "[filenumber-list](#) (page 4-16)" for a description of the *filenumber-list* placeholder.

Output

[Table 2-17](#) (page 2-171) describes the output of the `Issection` command.

Table 2-17 Issection Output

Column	Indicates
Backup section OID #	Catalog identifier for the backup section
Containing volume	Volume identifier of the tape media where the backup section resides
Containing volume OID	Catalog identifier for the volume

Table 2-17 (Cont.) lssection Output

Column	Indicates
File	File number; identifies which numbered backup the section occupies on a tape containing multiple backups
Section	For a backup that spans multiple tapes; identifies which tape this is in the sequence
Backup level	Level of backup to be performed; setting is <code>full</code> , 1 to 10, <code>incremental</code> , or <code>offsite</code>
Client	Name of Oracle Secure Backup client being backed up
Size	Size of the backup section
Created	Date and time the backup section was created
Attributes	Information about the volume expiration
Encryption	<p><code>on</code> for backups encrypted by Oracle Secure Backup</p> <p><code>transient</code> for backups encrypted by Oracle Secure Backup with a user-supplied one-time passphrase</p> <p><code>forcedoff</code> for an on-demand backup that was not encrypted, overriding the host-required encryption setting</p> <p><code>off</code> for backups that are not encrypted</p> <p><code>hardware</code> for backups encrypted by an encryption-capable tape drive</p> <p><code>transient_hardware</code> for transient backups encrypted by an encryption-capable tape drive</p> <p><code>RMAN</code> for backups encrypted by Recovery Manager (RMAN)</p> <p>This field displays <code>awaiting job completion</code> for an RMAN backup job that has not completed. Only when the RMAN backup finishes does this field report the encryption state of the backup.</p> <p>See <i>Oracle Secure Backup Administrator's Guide</i> for more information on backup encryption.</p>

If a date reported by `lssection` is more than six months earlier, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier, then it is reported in a `mm/dd.hh:mm` format.

Example

Example 2-110 Listing Backup Sections

This example displays the object identifiers of all backup sections in the backup sections catalog. The `lssection` command then displays data for section 108 in the default standard format to determine which volume it is on. The command then displays all backup sections on this volume in long format.

```
ob> lssection --short
  BSOID
    100
    105
    106
    107
    108

ob> lssection --oid 108
  BSOID Volume           File Sect Level Client      Created      Attributes
```

```

108 VOL000002          2 1          0 brhost2    04/19.11:52 never expires

ob> lssection --vid VOL000002 --long
Backup section OID:    105
  Containing volume:   VOL000002
  Containing volume OID: 111
  File:                1
  Section:             1
  Backup level:        0
  Client:              brhost2
  Size:                62.4 MB
  Created:             2013/04/19.11:36
  Attributes:          never expires
Backup section OID:    108
  Containing volume:   VOL000002
  Containing volume OID: 111
  File:                2
  Section:             1
  Backup level:        0
  Client:              brhost2
  Size:                65.3 MB
  Created:             2013/04/19.11:52
  Attributes:          never expires

```

2.1.78 lssnap

Purpose

Use the `lssnap` command to list snapshots on [Network Data Management Protocol \(NDMP\)](#) hosts.



See Also:

"[Snapshot Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lssnap` command.

Syntax

`lssnap::=`

```

lssnap [ --short/-s | --long/-l ] [ --noheader/-H ] [ --reserve/-r ]
[ --host/-h hostname[,hostname]... ]
[ --fs/-f filesystem-name[,filesystem-name]... ]
[ --numberformat/-n numberformat ] [ snapshot-name ]...

```

Semantics

--short/-s

Displays [snapshot](#) data in short form. This option is the default.

--long/-l

Displays snapshot data in long form.

--noheader/-H

Suppresses columns headers when listing data.

--reserve/-r

Displays the reserved space.

--host/-h *hostname*

Specifies the NDMP host. If you do not specify a host name, then Oracle Secure Backup uses the value from the `host` (page 5-3) variable.

--fs/-f *filesystem-name*

Specifies the file system of which the snapshot was taken.

--numberformat/-n *numberformat*

Specifies the format in which to display large numbers. Refer to "numberformat (page 4-21)" for a description of the *numberformat* placeholder.

snapshot-name

Specifies the name of the snapshot to list.

Output

Table 2-18 (page 2-174) describes the output of the `lssnap` command.

Table 2-18 lssnap Output

Label	Indicates
File system	File system captured in the snapshot
Max snapshots	Maximum number of snapshots permitted on this volume
Reserved space	Total reserved space for all snapshots
% reserved space	Percentage of reserved space currently used by all snapshots
Snapshot	Name of the snapshot
Of	Name of the file system
Taken at	Date and time of the snapshot
Used %	Space consumed by this snapshot as a percentage of reserved disk space being used on the volume. This value is calculated by: snapshot size x 100% / reserved space.
Total %	Space consumed by this snapshot as a percentage of total disk space on the volume. This value is calculated by: snapshot size x 100% / total disk space in this volume.
Busy	Whether the snapshot is busy; values are <code>yes</code> and <code>no</code>
Dependency	Whether the snapshot has a dependency on another processing entity (such as <code>snapmirror</code>); values are <code>yes</code> and <code>no</code>

If a date reported by `lssnap` is more than six months earlier, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier, then it is reported in a `mm/dd.hh:mm` format.

Example

Example 2-111 Displaying Snapshots

This example displays snapshots on the NDMP-accessed host `br_filer`. In this example, the `lucy.0` snapshot has used 3% of the space allocated to snapshots on `/vol/vol0` (3% of 44.8 GB) and 1% of the total disk space for the volume `/vol/vol0` (1% of 104 GB).

```
ob> lssnap --long --host br_filer
File system /vol/vol0:
  Max snapshots:          255
  Reserved space:         44.8 GB
  % reserved space:      30
  Snapshot:               lucy.0
    Of:                   /vol/vol0
    Taken at:              2013/03/28.20:52
    Used %:                3
    Total %:               1
    Busy:                  no
    Dependency:            no
  Snapshot:               myhost_snap1
    Of:                   /vol/vol0
    Taken at:              2010/08/21.11:30
    Used %:                12
    Total %:               7
    Busy:                  no
    Dependency:            no
```

2.1.79 lsssel

Purpose

Use the `lsssel` command to display a [database backup storage selector](#).

 **See Also:**

"[Database Backup Storage Selector Commands \(page 1-14\)](#)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lsssel` command.

Syntax

`lsssel::=`

```
lsssel [ --long/-l | --short/-s ]
[ --dbname/-d { * | dbname[,dbname]... } ]
[ --dbid/-i { * | dbid[,dbid]... } ]
[ --host/-h { * | hostname[,hostname]... } ]
[ --content/-c { * | content[,content]... } ]
```

```
[ --copynum/-n { 1 | 2 | 3 | 4 } ]
sselname...
```

Semantics

--long/-l

Displays all attributes of all storage selectors.

--short/-s

Displays only the names of the selected storage selectors.

--dbname/-d dbname

Lists storage selectors applicable to the specified database names.

--dbid/-i dbid

Lists storage selectors applicable to the specified [database ID \(DBID\)](#).

--host/-h hostname

Lists storage selectors applicable to the specified host names.

--content/-c content

Lists storage selectors applicable to the specified content types. Refer to "[content](#) (page 4-5)" for a description of the *content* placeholder.

--copynum/-n 1 | 2 | 3 | 4

Lists storage selectors applicable to the specified copy number.

sselname

Specifies the names of one or more storage selectors to display. This list is filtered by the other selection criteria (if any).

Output

[Table 2-19](#) (page 2-176) describes the output of the `lsssel` command.

Table 2-19 lsssel Output

Label	Indicates
Content	The content types of backups to which this storage selector applies (see " content (page 4-5)")
Databases	The names of the databases to which this storage selector applies
Database ID	The DBIDs of the databases to which this storage selector applies
Host	The database hosts to which this storage selector applies
Restrictions	The names of devices to which backups controlled by this storage selector are restricted.
Copy number	The copy number to which this storage selector applies
Media family	The name of the media family to be used for backups under the control of this storage selector object
Resource wait time	How long to wait for the availability of resources required by backups under the control of this storage selector
Priority	The schedule-priority value set for the RMAN backup and restore operations
UUID	The universal identifier of the storage selector

Example

Example 2-112 Displaying a Database Backup Storage Selector

This example creates a storage selector and then displays information about it.

```
ob> mkssel --dbid * --host brhost2 --content full --family f1 --name %R ssel_new
ob> lsssel --long

ssel_new:
  Content:          full
  Databases:       [all]
  Database IDs:    [all]
  Host:            brhost2
  Restrictions:    [none]
  Copy number:     [any]
  Media family:    f1
  Backup name:     %R
  Encryption:      undefined
  Resource wait time: 1 hour
  Priority:        25
  UUID:           a361f6c4-a53c-1030-ba54-00163e527899
```

2.1.80 lsstage

Purpose

Use the `lsstage` command to list one or more stage rules.

Syntax

`lsstage::=`

```
lsstage [--short/-s | --long/-l]
        [stage-rule-name [stage-rule-name]...]
```

Semantics

--short/-s

Displays only the names of the selected stage rules.

--long/-l

Displays all attributes of all stage rules.

stage-rule-name

Specifies the names of one or more stage rules to display.

Examples

Example 2-113 Listing Stage Rules in Short Format

This example shows the output of the short form of the `lsstage` command. It lists the names of stage rules, the target media family, and the associated stagescan schedule name.

```
ob> lsstage
database_rule      targetmf1      sscanmonat4pm
finance_host_rule  targetmf2      (immediate)
hr_host_rule       targetmf3      sscanmonat4pm
```

```

    purchasing_rule    targetmf1    dailysched
ob>

```

Example 2-114 Listing Stage Rules in Long Format

This example shows the output of the long form of the `lsstage` command.

```

ob> lsstage -long companyArule
Name:                hr_host_rule
Comment:             Company A's staging setup
Copy After:          10days
Schedule:            sscanmonat4pm
Match Media Family:  mf1,mf2
Target Media Family: targetmf1
Restrictions:        tdev1,tdev2,tdev3
Encryption:          Yes
Algorithm:           AES256
Database Names:      foodb
Database Ids:        1956
Hosts:               brhost1, brhost2, brhost3
Priority:             50
Migrate:             yes
ob>

```

2.1.81 Issum

Purpose

Use the `lssum` command to display every [job summary schedule](#).



See Also:

"[Summary Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `lssum` command.

Syntax

```
Issum::=
```

```
lssum [ --long/-l | --short/-s ] [ summary-name ]...
```

Semantics

--long/-l

Displays job summary schedule data in long form.

--short/-s

Displays the [job summary](#) name. By default `lssum` displays the summary name and the date and time at which the report should be generated.

summary-name

Specifies the name of the job schedule summary to list.

Output

[Table 2-20](#) (page 2-179) describes the output of the `lssum` command.

Table 2-20 Issum Output

Column	Indicates
Produce on	Date and time to generate the report
Mail to	E-mail address to which to send reports
Limit report to hosts	Hosts to which the job summary is limited
Backup jobs	Inclusion of information about backup jobs; setting is <code>yes</code> or <code>no</code>
Restore jobs	Inclusion of information about restore jobs; setting is <code>yes</code> or <code>no</code>
Oracle backup jobs	Inclusion of information about Recovery Manager (RMAN) backup jobs; setting is <code>yes</code> or <code>no</code>
Oracle restore jobs	Inclusion of information about RMAN restore jobs; setting is <code>yes</code> or <code>no</code>
Duplication jobs	Inclusion of information about duplication jobs; setting is <code>yes</code> or <code>no</code>
Scheduled jobs	Inclusion of information about scheduled jobs; setting is <code>yes</code> or <code>no</code>
User jobs	Inclusion of information about user jobs; setting is <code>yes</code> or <code>no</code>
Subordinate jobs	Inclusion of information about subordinate jobs; setting is <code>yes</code> or <code>no</code>
Superseded jobs	Inclusion of information about superseded jobs; setting is <code>yes</code> or <code>no</code>
Catalog backup jobs	Inclusion of information about catalog backup jobs; setting is <code>yes</code> or <code>no</code>
Media movement jobs	Inclusion of information about media movement jobs; setting is <code>yes</code> or <code>no</code>
Catalog import jobs	Inclusion of information about catalog import jobs; setting is <code>yes</code> or <code>no</code>
Copy instance jobs	Inclusion of information about copy instance jobs; setting is <code>yes</code> or <code>no</code>
Copy from stage jobs	Inclusion of information about copy from stage jobs; setting is <code>yes</code> or <code>no</code>

If a date reported by `lsbackup` is more than two months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than two months in the future, then it is reported in a `mm/dd.hh:mm` format.

Examples**Example 2-115 Displaying Job Summary Schedules**

This example displays information about the job summary schedule named `weekly_report`.

```
ob> lssum --long
OSB-CATALOG-SUM:
  Produce on:          daily at 06:00
  Covers preceding:    24 hours
  In the report, include:
```

```

Backup jobs:          no
Restore jobs:         no
Oracle backup jobs:  no
Oracle restore jobs: no
Duplication jobs:    no
Scheduled jobs:      yes
User jobs:           yes
Subordinate jobs:    yes
Superseded jobs:     no
Catalog backup jobs: yes
Media movement jobs: no
Catalog import jobs: no
Copy instance jobs:  yes
Copy from stage jobs: yes

```

ob>

2.1.82 lsuser

Purpose

Use the `lsuser` command to display the names and attributes of one or more Oracle Secure Backup users.



See Also:

"[User Commands](#) (page 1-22)" for related commands

Prerequisites

If you must list any [Oracle Secure Backup user](#), then you must have the [display administrative domain's configuration](#) (page 8-4) right. If you are only interested in listing yourself, then you must have the right to [modify own name and password](#) (page 8-6).

Syntax

`lsuser::=`

```

lsuser [ --long/-l | --short/-s ] [ --class/-c userclass ]
[ --unixname/-U unix-user ] [ --unixgroup/-G unix-group ]
[ --domain/-d windows-domain ] [ --ndmpuser/-N ]
[ --email/-e emailaddr ] [ --givenname/-g givenname ]
[ username... ]

```

Semantics

--long/-l

Displays data in long form.

--short/-s

Displays data in short form.

--class/-c *userclass*

Displays Oracle Secure Backup users belonging to a specific [class](#).

--unixname/-U *unix-user*

Displays Oracle Secure Backup users and associated classes by UNIX name.

--unixgroup/-G *unix-group*

Displays Oracle Secure Backup users and associated classes by UNIX group.

--domain/-d *windows-domain*

Displays Oracle Secure Backup users and associated classes by the Windows domain name.

--ndmpuser/-N

Displays Oracle Secure Backup users that have access to [Network Data Management Protocol \(NDMP\)](#) servers.

--email/-e *emailaddr*

Displays Oracle Secure Backup users and their associated classes by their email addresses.

--givenname/-g *givenname*

Displays Oracle Secure Backup users with the given name *givenname*.

username

Specifies the name of the Oracle Secure Backup user whose information you want to display.

Output

[Table 2-21](#) (page 2-181) describes the output of the `lsuser` command.

Table 2-21 lsuser Output

Column	Indicates
Password	User password; setting is (set) or (not set)
Password lifetime	Time validity of the user password
Password grace time	Limited time validity of the user password after it expires
Password reuse time	Time validity after which an old user password can be reused
User class	Name of the user class
Given name	Oracle Secure Backup name
UNIX name	<code>/etc/passwd</code> entry for the user
UNIX group	<code>/etc/group</code> entry for the user
Windows domain/acct	Domain or account name, if applicable
NDMP server user	Setting is <code>yes</code> or <code>no</code>
Email address	E-mail address of the user
UUID	Universal Unique Identifier (UUID) for the user
Hostname	Another computer for which the user is preauthorized to access
Username	User name of the user on another computer for which the user is preauthorized to access
Windows domain	Domain information, if applicable, on another computer for which the user is preauthorized to access

Table 2-21 (Cont.) lsuser Output

Column	Indicates
RMAN enabled	Recovery Manager (RMAN) availability on another computer for which the user is preauthorized to access; setting is <code>yes</code> or <code>no</code>
Cmdline enabled	Command line availability on another computer for which the user is preauthorized to access; setting is <code>yes</code> or <code>no</code> (<code>obtool</code>)

Example**Example 2-116 Displaying Oracle Secure Backup User Information**

This example displays information about Oracle Secure Backup user `bkpadmin`.

```
ob> lsuser
admin          bkpadmin
operator       oracle
reader         sbt
tadmin         user
ob> lsuser --long bkpadmin
bkpadmin:
  Password:                (set)
  Password last changed:   2013/05/20.04:50
  Password change required: no
  Password lifetime:       80 days
  Password grace time:     2 days
  Password reuse time:     120 days
  User class:              admin
  Given name:              dave
  UNIX name:               [none]
  UNIX group:              [none]
  Windows domain/acct:     [none]
  NDMP server user:        no
  Email address:           [none]
  UUID:                    1fa3c57e-a3ac-1030-ba54-00163e527899
  Preauthorized access:
    Hostname:              brhost3
    Username:              rman
    Windows domain:       [all]
    RMAN enabled:         no
    Cmdline enabled:      yes
```

2.1.83 lsvol

Purpose

Use the `lsvol` command to list the volumes in a [tape library](#) or the volumes [catalog](#).

Duplicate volumes are grouped with their [original volume](#) by default. The `lsvol` command shows the original volume `oid` for each duplicate [volume](#).

 **See Also:**

"oid (page 4-21)" for a description of the `oid` placeholder

Oracle Secure Backup uses the following [Small Computer System Interface \(SCSI\)](#) terms to describe basic components of libraries:

- A storage element, identified in the `lsvol` output as a number, contains a volume when it is not in use.
- An import-export element, identified in the `lsvol` output with the prefix `iee`, is used to move volumes into and out of the tape library without opening the door (thus requiring a full physical inventory). It is sometimes called a mail slot and is physically present only on certain libraries.
- A medium transport element, identified in the `lsvol` output as `mte`, moves a volume from a storage element to another element, such as a [tape drive](#).
- A [data transfer element \(DTE\)](#), identified in the `lsvol` output as `dte`, is a tape drive.

Each element has a name that you and Oracle Secure Backup use to identify it. For example, the first storage element is usually named `se1` and the first tape drive is `dte1`. You can omit the `se` prefix when referring to [storage elements](#); you can refer to the tape drive in libraries (when libraries contain only one tape drive) as `dte`.

 **See Also:**

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [query and display information about devices](#) (page 8-7) to use the `lsvol` command.

Syntax 1

Use the following syntax to list the volumes (inventory) in a tape library.

```
lsvol [ --library/-L libraryname | --drive/-D drivename ]
[ --long/-l ]
```

Semantics 1**--library/-L libraryname**

Specifies the name of the tape library holding the volumes to be listed.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D drivename

Specifies the name of a tape drive in the tape library holding the volumes to be listed.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--long/-l

Displays volume information in long format. If you specify `lsvol --long` with no other options, then the command displays an inventory of the `dte`, `mte`, and storage elements of the tape library. If you specify `--long` for particular volumes, then the command displays the OID, [volume ID](#), [barcode](#), volume sequence, and so forth.

Syntax 2

Use the following syntax to list the volumes in the volumes catalog.

```
lsvol [ --short/-s | --long/-l ] [ --relation/-r ] [ --members/-m ]
[ --duplicates/-d ] [ --noheader/-H ] [ --contents/-c ]
{ --all/-a |
  { [ --vid/-v vid[,vid]... ] [ --barcode/-b tag[,tag]... ]
    [ --vset/-V vsetid[,vsetid]... ] [ [ --dset/-S dsetid[,dsetid]... ]
      [ --family/-f media-family-name[,media-family-name]... ]
        [ --location/-C location-name[,location-name]... ]
          [ --attribute/-A volume-attr[,volume-attr]... ]
            [ --oid/-o oid[,oid]... ]
          }...
        [ --novid/-n | --nobarcode/-N ]
      }
    }
```

Semantics 2

--short/-s

Displays volume information in short format. The command displays only the volume ID for each volume.

--long/-l

Displays volume information in long format.

--relation/-r

Groups volumes according to the other options specified. For example, if you specify the `--family` option, then `obtool` sorts according to volumes belonging to the specified [media family](#).

--members/-m

Displays all [volume set](#) members for each volume displayed. This option is the default.

--duplicates/-d

List the duplicates for the volume in addition to the volume itself.

--noheader/-H

Displays information without header output.

--contents/-c

Displays information about the contents of each volume.

Specifying this option displays the size of the backup section, as shown in [Example 2-118](#) (page 2-187).

--all/-a

Displays all volumes in the volumes catalog.

--vid/-v *vid*

Displays the volume having the volume ID *vid*. Refer to "vid (page 4-30)" for a description of the *vid* placeholder.

--barcode/-b *tag*

Displays the volume with the barcode *tag*.

--vset/-V *vsetid*

Displays volumes that are members of the volume set *vsetid*. The *vsetid* represents the *vid* of the first volume in the volume set. Refer to "vid (page 4-30)" for a description of the *vid* placeholder.

--dset/-S *dsetid*

List all duplicates in the duplicate set. The duplicate set ID is the original volume *vid*.

--family/-f *media-family-name*

Displays all volumes of the specified media family. The *media-family-name* placeholder represents the name of a media family assigned with the **mkmf** (page 3-36) or **renmf** (page 3-88) command.

--location/-C *location-name*[, *location-name*]...

Limits the display to volumes in one or more specified locations.

--attribute/-A *volume-attr*

Displays all volumes with the attribute *volume-attr*. Valid values for this placeholder are:

- expired
All expired volumes
- unexpired
All unexpired volumes
- open
All volumes open for writing
- closed
All volumes closed for writing
- recyclable
All volumes that can be recycled

--oid/-o *oid*

Displays volumes with the specified *oid*. Refer to "oid (page 4-21)" for a description of the *oid* placeholder.

--novid/-n

Displays volumes with no volume ID.

--nobarcode/-N

Displays volumes with no barcode.

Output

Table 2-22 (page 2-186) describes the output of the `lsvol` command.

Table 2-22 lsvol Output

Column	Indicates
VOID	Oracle Secure Backup catalog identifier for the volume
OID	The Oracle Secure Backup catalog identifier for the original (parent) of a duplicate volume. It is identical to VOID for a volume that is not a duplicate.
Barcode	Barcode label identifier affixed to the tape case
Volume sequence	Number of the tape in the volume set
Media family	Oracle Secure Backup media family name
Current location	The place the tape current resides
Label host	The media server that labeled the tape originally
Size	The size of the backup section
Created	Date the volume was first written to.
Closes	Last time the tape can be written to
Expires	Date the tape expires and can be overwritten or recycled with doing a force unlabel
Space remaining	Storage capacity remaining on tape

If a date reported by `lsvol` is more than six months earlier or more than two months in the future, then it is reported in a `yyyy/mm/dd` format. If a date is less than six months earlier or less than two months in the future, then it is reported in a `mm/dd.hh:mm` format.



Note:

Oracle Secure Backup assigns each **backup ID** without regard to the time order of backups. For example, backup ID 25 can represent a Monday backup whereas backup ID 6 represents a backup on the following day.

Examples

Example 2-117 Displaying the Volumes in a Library

This example displays the volumes in tape library `lib1`. Note that the sample output has been reformatted to fit on the page.

```
ob> lsvol --long --library lib1
Inventory of library lib1:
  in  mte:          vacant
  in  1:            volume VOL000002, barcode ADE201, oid 110, 16962752 kb remaining
  in  2:            volume VOL000001, barcode ADE203, oid 102, 17619328 kb remaining
  in  3:            vacant
  in  4:            vacant
  in  iee1:         vacant
  in  iee2:         vacant
```

```

in   iee3:          vacant
in   dte:          volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 17017984 kb
                    remaining, content manages reuse, lastse 3

```

Example 2-118 Displaying the Contents of a Volume

This example displays the contents of volume `OSB-CATALOG-MF-000325`. Note that the sample output has been reformatted to fit on the page.

```

ob> lsvol --contents --vid OSB-CATALOG-MF-000325
VOID  OOID  Seq  Volume ID          Barcode  Family          Created
231   231    1   OSB-CATALOG-MF-000325  NEDC2491 OSB-CATALOG-MF  10/07.21:03
Attributes  BSOID  File Sect  Level  Host      Size      Created
never closes 532    1    1    0        osbsvr3  62.4 MB   10/07.21:03
Attributes

```

Example 2-119 Displaying the Volumes that Can be Recycled

This example displays the volumes that can be recycled in tape library `vlib1`. In the command output, for the volume with Volume ID `RMAN-DEFAULT-000001`, the Expires field displays "(content deleted)". This indicates that all the backup pieces on this content-managed volume have been deleted.

The output also displays that the status of this volume is `usable`, stating that it can be used for any Oracle Secure Backup operation.

```

ob> lsvol -l --attribute recyclable
Volume OID:          105
Volume ID:           RMAN-DEFAULT-000001
Barcode:             f6e6b776966d103af1900163e527899
Volume sequence:    1
Media family:       RMAN-DEFAULT
Current location:   vlib1
Label host:         brhost1
Created:            2014/03/25.03:08
Closes:             never
Expires:            never; content manages reuse (content deleted)
Space remaining:    140.8 GB
Original OID:       105
Status:             usable

```

3

obtool Commands: managedev to vfylibs

This chapter describes the [obtool](#) commands in alphabetical order. "[obtool Command Categories](#) (page 1-9)" organizes the obtool commands into various categories.

3.1.1 managedev

Purpose

Use the `managedev` command to manage the contents of disk pool and cloud storage devices.

Prerequisites

You must have a disk pool configured in your domain before using this command.



See Also:

Oracle Secure Backup Administrator's Guide, for more information on managing disk pools

Usage Notes

This command reclaims space that is occupied by expired backup image instances in disk pool and cloud storage devices.

Syntax

```
managedev::=  
  
managedev  
--deleteexpired/-d  
[--clearstage/-k {<stage-rule-name>[,<stage-rule-name>]...}]  
[--interactive/-i]  
[--host/-h hostname [,hostname]...]  
devicename...
```

Semantics

--deleteexpired/-d

Deletes expired backup image instances contained in disk pool and cloud storage devices.

[--clearstage/-k {<stage-rule-name>[,<stage-rule-name>]...}]

Changes the state of a backup image instance on the specified stage devices from `stage-in-progress` to `not-staged`.

This option is only needed in the rare case where a `copyfromstage` job failed catastrophically in a way that did not result in instances that were not copied having their stage state set back to `not-staged`. Instances marked `stage-in-progress` are never staged by a later `stagescan` job. The pool manager space reclaimer does not delete such instances after they expire.

Only backup image instances that match the stage rule are modified.

This option should not be used while either a `stagescan` job or a `copyfromstage` job is running.

--interactive/-i

Displays each backup image instance that is eligible for deletion and prompts you to confirm whether the instance can be deleted.

--host/-h *hostname*

Deletes only the expired backup image instances associated with the specified hosts.

devicename

Specifies the name of the device that is being managed.

Examples

Example 3-1 Deleting Expired Backup Image Instances for a Specified Host

This example deletes all expired image instances associated with the host `brhost3` that are stored on the disk pool `dp1`.

```
ob> lsinstance --expired --host brhost2
      Instance Name          Created          Container(s)
brhost2-20130423-110518.1    2013/04/23.04:05  dp2

ob> managedev --deleteexpired --host brhost2 dp2
Info: deleted 1 expired backup image from device dp2, space reclaimed: 128.0 KB
```

3.1.2 mkclass

Purpose

Use the `mkclass` command to define an [Oracle Secure Backup user class](#).

Oracle Secure Backup predefines several classes, which are described in [Classes and Rights](#) (page 8-1).



See Also:

["Class Commands](#) (page 1-13)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkclass` command.

Syntax

```
mkclass::=
```

```

mkclass [ --modself/-m { yes | no } ] [ --modconfig/-M { yes | no } ]
[ --backupself/-k { yes | no } ] [ --backuppriv/-K { yes | no } ]
[ --restself/-r { yes | no } ] [ --restpriv/-R { yes | no } ]
[ --listownjobs/-j { yes | no } ] [ --modownjobs/-J { yes | no } ]
[ --listanyjob/-y { yes | no } ] [ --modanyjob/-Y { yes | no } ]
[ --mailinput/-i { yes | no } ] [ --mailerrors/-e { yes | no } ]
[ --mailrekey/-g {yes | no}] [ --browse/-b browserights]
[ --querydevs/-q {yes | no}] [ --managedevs/-d {yes | no} ]
[ --listownbackups/-s {yes | no}] [ --modownbackups/-S {yes | no} ]
[ --listanybackup/-u {yes | no}] [ --modanybackup/-U {yes | no} ]
[ --orauser/-o {yes | no}] [ --orairights/-O oraclerights ]
[ --fsrights/F fsrights] [ --listconfig/-L {yes | no} ]
[ --modcatalog/-c {yes | no}]
classname...

```

Semantics

The default for all `mkclass` options that require a `yes` or `no` value is `no`.

--mailrekey/-m {yes | no}

Specifies whether e-mails are sent out to the administrative class when a rekey occurs, encounters errors, or has expired keys.

--modself/-m {yes | no}

Enables Oracle Secure Backup users to modify their own password and given name.

--modconfig/-M {yes | no}

Enables Oracle Secure Backup users to modify (create, modify, rename, and remove) all objects in an Oracle Secure Backup [administrative domain](#). These modifiable objects include objects representing classes, users, hosts, devices, defaults, and policies.

--backupself/-k {yes | no}

Enables Oracle Secure Backup users to run backups under their own user identity.

--backuppriv/-K {yes | no}

Enables Oracle Secure Backup users to run backups as the root or privileged user.

--restself/-r {yes | no}

Enables Oracle Secure Backup users to restore the contents of backup image instances under the restrictions of the access rights imposed by the user's UNIX name/group or Windows domain/account.

--restpriv/-R {yes | no}

Enables Oracle Secure Backup users to restore the contents of backup image instances as a privileged user. On Linux and UNIX hosts, a privileged restore operation runs under the `root` operating system identity. For example, Oracle Secure Backup user `joeblogg` runs under operating system account `root`. On Windows systems, the restore operations runs under the same account as the Oracle Secure Backup service on the Windows [client](#).

--listownjobs/-j {yes | no}

Grants Oracle Secure Backup users the right to view the following:

- Status of scheduled, ongoing, and completed jobs that they configured
- Transcripts for jobs that they configured

--modownjobs/-J {yes | no}

Grants Oracle Secure Backup users the right to modify only jobs that they configured.

--listanyjob/-y {yes | no}

Grants Oracle Secure Backup users the right to view the following:

- Status of any scheduled, ongoing, and completed jobs
- Transcripts for any job

--modanyjob/-Y {yes | no}

Grants Oracle Secure Backup users the right to make changes to all jobs.

--mailinput/-i {yes | no}

Enables Oracle Secure Backup users to receive email when Oracle Secure Backup needs manual intervention. Occasionally, during backup and restore operations, manual intervention of an [operator](#) is required. This situation can occur if a required [volume](#) cannot be found or a volume is required to continue a backup. In such cases, Oracle Secure Backup sends e-mail to all Oracle Secure Backup users who belong to classes having this right.

--mailerrors/-e {yes | no}

Enables Oracle Secure Backup users to receive email messages describing errors that occur during Oracle Secure Backup activity.

--listownbackups/-s {yes | no}

Grants Oracle Secure Backup users the right to view information about backup images and backup image instances that they created.

--listanybackup/-u {yes | no}

Grants Oracle Secure Backup users the right to view information about any backup images or backup image instances in the administrative domain.

--modownbackups/-S {yes | no}

Enables Oracle Secure Backup users to modify backup images or backup image instances that they created.

--modanybackup/-U {yes | no}

Enables Oracle Secure Backup users to modify all backup images or backup images instances in the administrative domain.

--modcatalog/-c {yes | no}

Enables Oracle Secure Backup users to modify backup catalog information.

--querydevs/-q {yes | no}

Enables Oracle Secure Backup users to query the state of devices.

--managedevs/-d {yes | no}

Enables Oracle Secure Backup users to control the state of devices with the `obtool` command.

--listconfig/-L {yes | no}

Enables Oracle Secure Backup users to list objects, for example, hosts, devices, and users, in the [administrative domain](#).

--browser/-b browserights

Grants Oracle Secure Backup users browsing `rights`. Specify one of the following `browserights` values, which are listed in order of decreasing privilege:

- `privileged` means that Oracle Secure Backup users can browse all directories and `catalog` entries.
- `notdenied` means that Oracle Secure Backup users can browse any catalog entries for which they are not explicitly denied access. This option differs from `permitted` in that it allows access to directories having no stat record stored in the catalog.
- `permitted` means that Oracle Secure Backup users are bound by normal UNIX permissions checking (default). Specifically, Oracle Secure Backup users can only browse directories if at least one of the following conditions is applicable:
 - The UNIX user defined in the Oracle Secure Backup identity is listed as the owner of the directory, and the owner has read rights.
 - The UNIX group defined in the Oracle Secure Backup identity is listed as the group of the directory, and the group has read rights.
 - Neither of the preceding conditions is met, but the UNIX user defined in the Oracle Secure Backup identity has read rights for the directory.
- `named` means that Oracle Secure Backup users are bound by normal UNIX rights checking, except that others do not have read rights. Specifically, Oracle Secure Backup users can only browse directories if at least one of the following conditions is applicable:
 - The UNIX user defined in the Oracle Secure Backup identity is listed as the owner of the directory, and the owner has read rights.
 - The UNIX group defined in the Oracle Secure Backup identity is listed as the group of the directory, and the group has read rights.
- `none` means that no Oracle Secure Backup user has any rights to browse any directory or catalog.

--orauser/-o {yes | no}

Enables Oracle Secure Backup users to perform Oracle Database backup and restore operations (`yes` or `no`). This right enables Oracle Secure Backup users to perform any SBT operation, regardless of what other rights they have. For example, an Oracle Secure Backup user with this right can perform SBT restore operations even if the `perform restores as self` right is set to `no`.

--orarights/-O oraclerights

Enables Oracle Secure Backup users with the specified rights to access Oracle Database backups. The `oraclerights` placeholders can be any of the following values:

- `class` means that Oracle Secure Backup users can access SBT backups created by any Oracle Secure Backup user in the same class.
- `all` means that Oracle Secure Backup users can access all SBT backups.
- `none` means that no Oracle Secure Backup user has any rights to access SBT backups.
- `owner` means that Oracle Secure Backup users can access only those SBT backups that they themselves have created (default).

classname

Specifies the name of the class to be created. Class names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example**Example 3-2 Making a Class**

This example creates a class called `backup_admin`. The command accepts the default value of `no` for `--listownjobs`, `--modownjobs`, `--listanyjob`, `--modanyjob`, `--managedevs`, `--orauser`, and `--orarights`. Note that because of space constraints the `mkclass` command in the example spans multiple lines.

```
ob> mkclass --listconfig yes --modself yes --modconfig yes --backupself yes
--backuppriv yes --restself yes --restpriv yes --mailinput yes --mailerrors yes
--querydevs yes --browse privileged backup_admin
ob> lsclass --long backup_admin
backup_admin:
  browse backup catalogs with this access:      privileged
  access Oracle database backups:              owner
  access file system backups:                  owner
  display administrative domain's configuration: yes
  modify own name and password:                yes
  modify administrative domain's configuration: yes
  modify catalog:                              no
  perform file system backups as self:         yes
  perform file system backups as privileged user: yes
  list any jobs owned by user:                 no
  modify any jobs owned by user:               no
  perform file system restores as self:        yes
  perform file system restores as privileged user: yes
  receive email requesting operator assistance: yes
  receive email describing internal errors:    yes
  receive email regarding expired passphrase keys: no
  query and display information about devices: yes
  manage devices and change device state:     no
  list any job, regardless of its owner:       no
  modify any job, regardless of its owner:     no
  perform Oracle database backups and restores: no
  list any backups owned by user:              no
  modify any backups owned by user:            no
  list any backup, regardless of its owner:    no
  modify any backup, regardless of its owner:  no
```

3.1.3 mkdev

Purpose

Use the `mkdev` command to configure a device for use with Oracle Secure Backup. This command assigns Oracle Secure Backup names and attributes to the devices in your [administrative domain](#). Devices include tape devices, tape libraries, disk pools, and cloud storage devices.

To be usable by Oracle Secure Backup, each device must have at least one [attachment](#), which describes a data path between a host and the device itself. In the attachment, you identify a host to which the device is connected and a raw device name through which it is accessed.

 **See Also:**

- "Device Commands (page 1-15)" for related commands
- "mkhost (page 3-26)" to learn about configuring an administrative domain

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkdev` command.

You should disable any system software that scans and opens arbitrary [Small Computer System Interface \(SCSI\)](#) targets before configuring an Oracle Secure Backup [tape device](#). If Oracle Secure Backup has to contend with other system software (such as monitoring software) for access to tape libraries and tape drives, then unexpected behavior can result.

Syntax 1

Use the following syntax to configure a [tape drive](#).

`mkdev::=`

```
mkdev --type/-t tape
[ --attach/-a aspec[,aspec]... ]
[ --inservice/-o | --notinservice/-O ] [ --wwn/-W wwn ]
[ --library/-l devicename ] [ --dte/-d dte ]
[ --blockingfactor/-f bf ] [ --maxblockingfactor/-F maxbf ]
[ --automount/-m { yes | no } ] [ --erate/-e erate ]
[ --current/-T se-spec ] [ --uselist/-u se-range ]
[ --usage/-U duration ] [ --positioninterval/-q positioninterval ]
[ --serial/-N serial-number ] [ --model/-L model-name ]
[ --createdevfile/-k]
devicename...
```

Semantics 1

The following options enable you to configure a tape drive.

--type/-t *tape*

Specifies the device as a tape drive.

--attach/-a *aspec*

Configures an attachment, which is the physical or logical connection of a device to a host. An attachment is distinct from a device and describes a data path between a host and the device.

Oracle Secure Backup uses attachments to access a device, so a device must have at least one attachment to be usable by Oracle Secure Backup. A [Fibre Channel](#)-attached tape drive or [tape library](#) often has multiple attachments, one for each host that can directly access it. Refer to "[aspec](#) (page 4-1)" for a description of the *aspec* placeholder.

--inservice/-o

Specifies that the tape drive is logically available to Oracle Secure Backup.

--notinservice/-O

Specifies that the tape drive is not logically available to Oracle Secure Backup.

--wwn/-W *wwn*

Specifies the worldwide name of the device. Refer to "[wwn](#) (page 4-32)" for an explanation of the *wwn* placeholder.

--library/-l *devicename*

Specifies the name of the tape library in which a tape drive resides.

--dte/-d *dte*

Specifies the [data transfer element \(DTE\)](#) number of a tape drive within its containing tape library. DTE is the SCSI-2 name for a tape drive in a tape library. DTEs are numbered 1 through *n* and are used to identify tape drives in a tape library.

You must specify a *dte* number if `--library` is specified. The *dte* option is not available for standalone tape drives.

When you first configure tape libraries that have multiple drives, while assigning DTE numbers to the drives in Oracle Secure Backup, it is important to observe the DTE numbering scheme from the perspective of the physical library. The numbering of the drives is not an arbitrary, sequential value that you can assign. It must correspond to the correct order within the library; else the following error occurs when Oracle Secure Backup attempts to unload a misconfigured drive: Error: can't execute command - source is empty. To determine the DTE numbers within a tape library, on the user interface or the front panel of the library, find the drive serial number for each DTE number and then ensure that you assign the correct DTE number to the corresponding drive in Oracle Secure Backup. After you configure the drives in Oracle Secure Backup, use the following command to verify that your DTE numbers are accurate:

```
ob> vfylibs -v
```

In the output of the `vfylibs` command, for each drive, the serial number and the DTE number must exactly match the independent output from the user interface or front panel of the library.

--blockingfactor/-f *bf*

Specifies a [blocking factor](#). A blocking factor determines how many 512-byte records to include in each block of data written to the tape. By default, Oracle Secure Backup writes 64K blocks to tape, which is a blocking factor of 128.

--maxblockingfactor/-F *maxbf*

Specifies a maximum blocking factor. The maximum blocking factor controls the amount of data that Oracle Secure Backup initially reads from a tape whose blocking factor is unknown.

The largest value permitted for the maximum blocking factor, which is the number of 512-byte records for each physical tape block, is 4096. This value represents a maximum tape block size of 2MB. This maximum is subject to device and operating system limitations that can reduce this maximum block size.

--automount/-m {*yes* | *no*}

Sets the automount mode. The [mount mode](#) indicates the way in which Oracle Secure Backup can use a volume physically loaded into a tape drive (see the description of "[mountdev](#) (page 3-69)").

A value of *yes* (default) instructs Oracle Secure Backup to mount tapes for backup and restore operations without [operator](#) intervention. If this option is set to *no*, then you must manually mount volumes before they are usable.

A setting of `no` can be useful if you dedicate a tape drive to performing on-demand restore operations, but not backups. If `automount` is set to `yes` for this tape drive when a backup is scheduled, and if the tape drive contains an unmounted, eligible tape, then Oracle Secure Backup uses the tape drive for the backup.

--erate/-e erate

Specifies the [error rate](#) percentage. The error rate is the number of recovered errors divided by the total blocks written, multiplied by 100. Oracle Secure Backup issues a warning if the error rate reported by the device exceeds the value you specify. The default is 8.

Oracle Secure Backup issues a warning if it encounters a SCSI error when trying to read or reset the error counters of the tape drive. Some tape drives do not support the SCSI commands necessary to perform these operations. To avoid these warnings, disable error rate checking by specifying `none` for the error rate.

--current/-T se-spec

Specifies the number of a storage element. This option only applies to a tape drive when the following criteria are met:

- The tape drive is in a tape library.
- The tape drive is known to be loaded with a tape.
- The hardware cannot determine from which storage element the tape drive was loaded.

Refer to "[se-spec](#) (page 4-27)" for a description of the `se-spec` placeholder.

--uselist/-u se-range

Specifies a range of [storage elements](#) that the device can use. This option only applies to a tape drive contained in a tape library.

By default, Oracle Secure Backup allows all tapes in a tape library to be accessed by all tape drives in the tape library. For libraries containing multiple tape drives which perform backups concurrently, you might want to partition the use of the tapes.

For example, you might want the tapes in half the storage elements to be available to the first tape drive and those in the second half to be available to the second tape drive. Alternatively, you might want to set up different use lists for different types of backups on a single tape drive.

Refer to "[se-range](#) (page 4-27)" for a description of the `se-range` placeholder.

--usage/-U duration

Specifies the interval for a cleaning cycle. For example, `--usage 1month` requests a cleaning cycle every month. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder.

You can specify the `--usage` option on the [chdev](#) (page 2-30) command to initialize the configured interval to reflect the amount of time that the tape drive has been used since the last cleaning. For example, specify `--usage 1week` on the `chdev` command to indicate that the most recent cleaning was a week ago.

--positioninterval/-q kb

Specifies the position interval in terms of `kb`, which is the "distance" between samplings of the tape position expressed in 1KB blocks. The maximum allowed position interval is 1048576 (1MB), which is a query interval of 1GB. A position interval of 0 disables position sampling.

During a backup, Oracle Secure Backup periodically samples the position of the tape. [obtar](#) saves this position information in the Oracle Secure Backup [catalog](#) to speed up restore operations. For some devices, however, this sampling can degrade backup

performance. While Oracle Secure Backup has attempted to determine optimal position intervals for all supported tape drive types, you might find that you must adjust the position interval.

The position interval set at the device level overrides the global position interval settings.

--serial/-N *serial-number*

Specifies the serial number for the tape device.

If a serial number is entered, then Oracle Secure Backup stores that serial number in the device object. If no serial number is entered, then the serial number is read and stored in the device object the first time Oracle Secure Backup opens the tape device.



See Also:

"[checkserialnumbers](#) (page 7-13)"

--modell/-L *model-name*

Specifies the model name for the tape device. The model number is usually discovered during device configuration.

--createdevfile/-k

Creates a device file on the media server by using the SCSI information provided in the `--attach` argument. Oracle Secure Backup also creates a device object using this device file.

On Linux and Solaris media servers, the operating system provides the device files and you can use these device files to configure the device. Therefore, you can specify the device file by using the `--attach` argument and the `--createdevfile` argument is not required.

For HP-UX and Windows media servers, if you provide the device file as part of the `--attach` argument, this device file is used for the configuration. If the `--attach` argument provides SCSI information such as target, bus, and LUN information, Oracle Secure Backup uses this information to create a device file on the media server.

For devices attached to AIX media servers, the `--createdevfile` argument creates a text file containing the SCSI bus, target, and LUN information or bus, wwn, and LUN information on the media server. If you provide the name of this text file using the `--attach` argument, Oracle Secure Backup uses this file for the device configuration. If the `--attach` argument provides only the SCSI information and not the text file name, then Oracle Secure Backup uses this information to create a device file on the media server.

devicename

Specifies the name of the tape drive to be configured. If an attachment is specified, then only one *devicename* is allowed. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Syntax 2

Use the following syntax to configure a tape library.

mkdev::=

```
mkdev --type/-t library [ --class/-x vtl ] [ --attach/-a aspec[,aspec]... ]
[ --inservice/-o | --notinservice/-O ] [ --wwn/-W wwn ]
[ --autoclean/-C { yes | no } ] [ --cleanemptiest/-E { yes | no } ]
[ --cleaninterval/-i { duration | off } ]
```

```
[ --barcodereader/-B { yes | no | default } ]
[ --barcodesrequired/-b { yes | no | default} ]
[ --unloadrequired/-Q { yes | no } ]
[ --serial/-N serial-number ] [ --model/-L model-name ]
[ --ejection/-j etype ] [ --minwritablevolumes/-V n ]
[ --createdevfile/-k]
devicename...
```

Semantics 2

The following options enable you to configure a tape library. See "[Semantics 1](#) (page 3-7)" for identical options not listed here.

--type/-t library

Specifies the device as a tape library.

--class/-x vtl

Specifies a virtual tape library.

--autoclean/-C {yes | no}

Specifies whether automatic tape cleaning should be enabled. A cleaning cycle is initiated either when a tape drive reports that it needs cleaning or when a specified usage time has elapsed.

Oracle Secure Backup checks for cleaning requirements when a cartridge is either loaded into or unloaded from a tape drive. If at that time a cleaning is required, then Oracle Secure Backup performs the following steps:

1. Loads a cleaning cartridge
2. Waits for the cleaning cycle to complete
3. Replaces the cleaning cartridge in its original storage element
4. Continues with the requested load or unload

Note that you can run the [clean](#) (page 2-79) command to clean a tape drive manually.

--cleanemptiest/-E {yes | no}

Specifies which cleaning tape to use. This option is useful when a tape library contains multiple cleaning tapes.

The default value of *yes* specifies the emptiest cleaning tape, which causes cleaning tapes to round robin as cleanings are required.

The *no* value specifies that obtool should use the least used cleaning tape, which uses each cleaning tape until it is exhausted, then uses the next cleaning tape until it is exhausted, and so forth.

--cleaninterval/-i {duration | off}

Specifies whether there should be a cleaning interval, and if so, the *duration* of the interval. The default is *off*. The duration is the interval of time a tape drive is used before a cleaning cycle begins. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

If automatic tape drive cleaning is enabled, then *duration* indicates the interval between cleaning cycles. For tape drives that do not report cleaning requirements, you can specify a cleaning interval, for example, *30days*.

--barcodereader/-B {yes | no | default}

Specifies whether a [barcode](#) reader is present. Many devices report whether they have a barcode reader. For these devices you can specify *default*. For devices that do not report this information, specify *yes* or *no*.

--barcodesrequired/-b {yes | no | default}

Specifies whether Oracle Secure Backup requires tapes in the tape library to have readable barcodes.

The default is `no`. If you specify `yes`, and if a tape in the tape library does not have a readable barcode, then Oracle Secure Backup refuses to use the tape. Use `default` or `dft` to use the barcode value specified in the device policy settings.

Typically, Oracle Secure Backup does not discriminate between tapes with readable barcodes and those without. This policy ensures that Oracle Secure Backup can always solicit a tape needed for restore by using both the barcode and the [volume ID](#).

--unloadrequired/-Q {yes | no}

Specifies whether an unload operation is required before moving a tape from a tape drive to a storage element. Typically, you should leave this option set to default of `yes`, which means the value comes from the external device table `ob_drives`. If you encounter difficulties, however, particularly timeouts waiting for offline while unloading a tape drive, then set the value to `no`.

--serial/-N *serial-number*

Specifies the serial number for the tape device.

If a serial number is entered, then Oracle Secure Backup stores that serial number in the device object. If no serial number is entered, then the serial number is read and stored in the device object the first time Oracle Secure Backup opens the tape device.

--modell/-L *model-name*

Specifies the model name for the tape device. The model number is usually discovered during device configuration.

--ejection/-j *etype*

Specifies the means by which tapes are ejected. Values are `automatic`, `ondemand`, or `manual`.

--minwritablevolumes/-V *n*

Specifies the threshold for the minimum number of writeable volumes before Oracle Secure Backup initiates early [volume](#) rotation.

devicename

Specifies the name of the tape library to be configured. If an attachment is specified, then only one *devicename* is allowed. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Syntax 3

Use the following syntax to create and configure a disk pool.

```
mkdev::=
```

```
mkdev --type/-t disk
[--attach/-a <aspec>[,<aspec>]...] [--force/-Y]
[--inservice/-o | --notinservice/-O] [--initialize/-z]
[--capacity/-y size-spec] [--concurrentjobs/-J concjobs]
[--blockingfactor/-f bf] [--maxblockingfactor/-F maxbf]
[--freespacegoal/-G freespacegoal]
[--staging/-h {yes | no}]
[--stagerule/-H [<stage-rule-name>] [,<stage-rule-name>]...]
devicename...
```

Semantics 3

--type/-t *disk*

Specifies that the device is a disk pool.

--attach/-a *aspec*

Configures an attachment, which is the physical or logical connection of a storage device to a host. For a disk pool, the attachment specifies the host name and the file-system directory that stores the backups. The host must be an Oracle Secure Backup host with media server role and must support the NDMP file service extension.

Every disk pool must have at least one attachment to be usable by Oracle Secure Backup. If the directory specified is currently configured as a disk pool in another administrative domain, you cannot configure this disk pool in your domain until you remove it from the previous domain. If the directory specified was previously configured as a disk pool and still contains backup image instances, Oracle Secure Backup displays a message indicating that you can recatalog the contents of the file-system directory so that the existing backups can be used as restore sources. If multiple hosts can access the file-system directory that serves as the repository for a disk pool, then you can identify each host by using separate `--attach` options in the `mkdev` command.

If multiple attach points are specified and the directory specification differs among them, Oracle Secure Backup verifies that each attach point resolves to the same file-system directory. If this verification fails, the disk pool creation is terminated.

Refer to "[aspec \(page 4-1\)](#)" for a description of the *aspec* placeholder.

--force/-Y

Forces the configuration of the disk pool by overriding the domain membership checks that determine if the disk pool being configured is part of another Oracle Secure Backup administrative domain.

--inservice/-o

Sets the status of the disk pool so that it is logically available to Oracle Secure Backup.

--notinservice/-O

Sets the status of the disk pool so that it is not logically available to Oracle Secure Backup.

--initialize/-z

Creates the file-system directory specified in *pathname*, if it does not exist. If this option is not specified, the directory specified must exist on the host. The directory can either be empty or have been configured previously as a disk pool.

--capacity/-y *size-spec*

Specifies the amount of space that the disk pool can occupy on the file-system directory. The [size-spec \(page 4-28\)](#) placeholder specifies the size of the disk pool. Enter a numeric value followed by unit. The unit for disk pool size can be one of the following: KB, MB, GB, TB, PB or EB. Enter zero to indicate that there is no limit on the size of the disk pool. In this case, the size of the disk pool is limited only by the capacity of the underlying file-system that hosts the disk pool.

If the size of backup image instances on the disk pool exceeds the specified capacity, then Oracle Secure Backup does not schedule any further jobs for this disk pool until the space consumption drops below the capacity.

When you use the **chdev (page 2-30)** command to modify the consumption capacity of disk pools, if the value specified by **size-spec (page 4-28)** is lower than the space currently occupied by the disk pool, then the command fails.

-concurrentjobs/-J *concjobs*

Specifies the maximum number of jobs that can run concurrently for this disk pool. This includes backup, restore, and pool management-related jobs. See "**concjobs (page 4-5)**" for more information.

--blockingfactor/-f *bf*

Specifies a blocking factor.

A blocking factor determines how many 512-byte records to include in each block of data written to the disk pool. By default, Oracle Secure Backup writes 64K blocks, which is a blocking factor of 128.

When you copy a backup image instance from a disk pool device to a tape device, the blocking factor used to create the backup image instance on the disk pool device will be the blocking factor used to write the instance to the tape device. It is a best practice to set the blocking factor of the disk pool device to be the same as the blocking factor of the tape device.

**See Also:**

[cpinstance](#) (page 2-80)

--maxblockingfactor/-F *maxbf*

Specifies a maximum blocking factor. The maximum blocking factor controls the amount of data that Oracle Secure Backup initially reads from the disk pool whose blocking factor is unknown.

--freospacegoal/-G *freospacegoal*

Specifies the percentage of disk pool capacity that the disk pool manager must maintain by proactively deleting expired backup image instances.

--staging/-h

Controls whether staging is enabled for the disk pool device. The default value is `no`. If staging is disabled on a disk pool device, then backup images written to the stage disk pool are not be marked for staging. Use the `stagescan` command to mark all backup image instances to be staged.

When this option is used, the `--type/-t disk` option must also be specified on the command.

--stagerule/-H

Sets the device stage rule list. If staging is enabled, then any backup image instance contained in the disk pool device that matches a rule is staged. The rules are tested for a match in the order that they appear in the list. If any rule matches a backup image instance, then all subsequent rules in the list are ignored.

The same stage rule may be used in more than one disk pool.

There should always be at least one scheduled stage rule in the list of rules to ensure that the instances that do not match any rule are automatically staged by the default stage rule. See *Oracle Secure Backup Administrator's Guide* for a description of the default stage rule.

If a stage device is listed in the restriction list for a stage rule, then that rule cannot be added to that stage device. The operation fails and an error message is returned.

When this option is used, the `--type/-t disk` option must also be specified on the command.

devicename

Specifies the name of the disk pool.

Syntax 4

Use the following syntax for configuring a tape drive in an ACSLS tape library:

mkdev::=

```
mkdev --type/-t tape [ --attach/-a aspec[,aspec]... ]
[ --inservice/-o | --notinservice/-O ] [ --wwn/-W wwn ]
[ --library/-l devicename --lsm/s lsm_id --panel/p panel_id
--drive/r drive_id] [ --blockingfactor/-f bf ]
[ --maxblockingfactor/-F maxbf ] [ --erate/-e erate ]
[ --positioninterval/-q <positioninterval>]
devicename...
```

Semantics 4

Use the following semantics for configuring a tape drive in an ACSLS tape library. See "[Semantics 1](#) (page 3-7)" for identical options not listed here.

You can use `mkdev` for an ACSLS tape drive only when `obacslibd` is stopped.

--lsm/-s *lsm_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the ACS Library Storage Module where this tape drive resides.

--panel-p *panel_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the panel where this tape drive resides.

--drive -r *drive_id*

This option is used only for tape drives contained in ACSLS libraries. It defines the ID of the drive where this tape drive resides.

Syntax 5

Use the following syntax is for configuring an ACSLS tape library.

mkdev::=

```
mkdev --type/-t library --class/-x acsls --acsid/-g acs_id
[ --attach/-a aspec... ]
[ --inservice/-o | --notinservice/-O ]
[ --userid/-n acs_userid ] [ --port/-P port_num ]
[ --ejection/-j etype ] [ --minwritablevolumes/-V minvols ]
library_devicename...
```

Semantics 5

Use the following semantics is for configuring an ACSLS tape library. See "[Semantics 1](#) (page 3-7)" for identical options not listed here.

--class/-x *acsls*

This option specifies that this tape library is an ACS tape library.

--attach/-a *aspec...*

This option specifies the Oracle Secure Backup [media server](#) and ACSLS server for an ACSLS tape library. The format of the *aspec* is `mediaservhostname:acslshost`

--acsid/-g *acs_id*

This option specifies the ACS ID value for the ACSLS tape library to control.

--userid/-n *acs_userid*

This option specifies the ACSLS access control user name. This value is optional. If it is specified, then all interactions with an ACSLS server are preceded by this access name.

--port/-P *port_num*

This option specifies the listening port of the ACSLS server software. Typically this value is 0 or not specified. This option must be specified only when your ACSLS server is located behind a [firewall](#).

Syntax 6

Use the following syntax to associate a symbolic name with an ACS cartridge access port (CAP) within an ACSLS tape library. This command does not create or modify the CAP, which is a physical item on the ACS.

mkdev::=

```
mkdev --type/-t cap [ --library/-l devicename ] [ --capid/-c cap_id ]
[ --lsm/-s lsm_id ] capname
```

Semantics 6

Use the following semantics to associate a symbolic name with an ACS cartridge access port (CAP) within an ACSLS tape library.

--library/-L *devicename*

This option specifies the name of the tape library in which the CAP resides. If it is omitted, then the library variable is used. If the library variable is not found and one is not specified, then an error message is displayed.

--capid/-c *cap_id*

This option specifies the hardware location of the CAP within the selected tape library.

--lsm /-s *lsm_id*

This option specifies the ACS Library Storage Module of the CAP within the selected tape library.

capname

The name of the Oracle Secure Backup CAP object to be created.

Syntax 7

Use the following syntax to configure a cloud storage device.

mkdev::=

```
mkdev --type/-t cloudstorage
{--mediasserver media server, media server,...}
[--storageclass cloud-storage-class]
[--inservice/-o | --notinservice/-O]
[--capacity/-y size-spec]
```

```

{--username cloud-user}
{--querypassphrase}
{--container container-name}
[--segmentsize segment-size]
[--streamspersjob streams-per-job]
[--concurrentjobs concjobs]
[--blockingfactor/-f bf]
[--maxblockingfactor/-F maxbf]
[--freespacegoal/-G freespacegoal]
[--proxy proxy-url]
[--proxyuser proxy-user]
[--queryproxypass]
{--url cloud-url}
{--identitydomain identity-domain}
[--force]
devicename...

```

Semantics 7

Use the following semantics to configure a cloud storage device.

See Also:

- [Oracle Cloud Documentation](#) for further information about cloud-related concepts in the following semantics.

--type/-t *cloudstorage*

Specifies that the device is a cloud storage device.

--mediasserver *media server*

Name of the attached media server. If multiple media servers are specified, then Oracle Secure Backup verifies that the container is reachable via all specified media servers.

When a media server is specified, all data is sent from the client to the media server. The media server then buffers and uploads the data to Oracle Cloud. Running too many jobs on the same media server may affect performance.

The media server must have a cloud wallet. See *Oracle Secure Backup Installation and Configuration Guide* for information about creating a cloud wallet and importing it into media servers.

--storageclass *cloud-storage-class*

Oracle Cloud storage class, either of the following:

- *object* — specifies Oracle Cloud Infrastructure Object Storage Classic which provides object storage for files and unstructured data.
- *archive* — specifies Oracle Cloud Infrastructure Archive Storage Classic which provides storage for applications and workloads that require long-term retention.

Restoring data from Object Storage Classic is faster than restoring data from Archive Storage Classic because in Object Storage Classic, the data is available immediately. Whereas, data in Archive Storage Classic is made available in 3-5 hours. The Oracle Secure Backup restore job is in a running state until the data is made available.

See [About Oracle Cloud Infrastructure Object Storage Classic](#)

--inservice/-o | --notinservice/-O

`--inservice` sets the status of the cloud storage device so that it is logically available to Oracle Secure Backup.

`--notinservice` sets the status of the cloud storage device so that it is not logically available to Oracle Secure Backup.

--capacity/-y *size-spec*

Specifies the amount of space that the cloud storage device can occupy in the configured Oracle Cloud account identity domain. The *size-spec* placeholder specifies the size of the cloud storage device. Enter a numeric value followed by unit. The unit for cloud storage device size can be one of the following: KB, MB, GB, TB, PB or EB. Enter zero to indicate that there is no limit on the size of the cloud storage device other than the limit set by the quota purchased for the Oracle Cloud account identity domain.

If the size of backup image instances on the cloud storage device exceeds the specified capacity, then Oracle Secure Backup does not schedule any further jobs for this cloud storage device until the space consumption drops below the capacity.

If you use the `chdev` command to change the size of a cloud storage device, then the value you specify cannot be lower than the space currently occupied by the cloud storage device, or the command will fail.

--username *cloud-user*

Name of the Oracle Cloud user account. This user account belongs to the defined identity domain. The user account must have the `Storage_Administrator` and `Storage_ReadWriteGroup` roles.

--querypassphrase

When the user's pass phrase changes on Oracle Cloud, the `querypassphrase` is used to update the user's pass phrase in the cloud storage device.

--container *container-name*

A container is a storage compartment that provides a way to organize the data stored in Oracle Storage Infrastructure. With this option, Oracle Secure Backup creates a new container with the specified name. If a container of that name already exists, then you must also specify the `--force` option. Oracle Secure Backup never uses an existing container that was not created by Oracle Secure Backup.

--segmentsize *segment-size*

Oracle Secure Backup stores each backup image by splitting it into multiple segments and storing each segment as a single object in the container. The segment size defines the size of object. This option allows you to specify a suitable segment size. The segment size is important because it defines the amount of data that is buffered on the media server. If the segment size is too large, then the `ndmp` process consumes too much memory on the media server and it may affect backup performance or cause other job failures.

--streamspersjob *streams-per-job*

Oracle Secure Backup can make multiple connections to Oracle Storage Infrastructure for faster uploads of data. This option lets you specify a value that defines the number of threads created for parallel uploads of backup data. It also defines the number of buffers allocated for buffering the backup data. If this value is too large, then the `ndmp` process may use a great amount of memory and CPU on the media server, which may affect performance and lead to job failure.

--concurrentjobs *concjobs*

Specifies the maximum number of jobs that can run concurrently for this device. This includes backup, restore, and cloud storage device management-related jobs. If too many concurrent jobs are run on the same media, performance may be affected. Try to evenly distribute the backup job on different media servers.

See "[concjobs](#) (page 4-5)" for more information.

--blockingfactor/-f *bf*

Specifies a blocking factor.

A blocking factor determines how many 512-byte records to include in each block of data written to the device. By default, Oracle Secure Backup writes 64K blocks, which is a blocking factor of 128. Increasing this value may provide an increase in performance.

--maxblockingfactor/-F *maxbf*

Specifies a maximum blocking factor. The maximum blocking factor controls the amount of data that Oracle Secure Backup initially reads from the device whose blocking factor is unknown.

--freespacegoal/-G *freespacegoal*

Specifies the percentage of device capacity that the device manager must maintain by proactively deleting expired backup image instances.

--proxy *proxy-url*

If the connection to Oracle Storage Infrastructure is through a proxy server, then specify the proxy server URL.

--proxyuser *proxy-user*

The proxy server user name

--queryproxypass

The password for the proxy user.

--url *cloud-url*

The endpoint URL provided by Oracle Cloud, which must include your identity domain name. The endpoint URL is usually the following, where `example` is the name of the identity domain: `example.storage.oraclecloud.com`.

--identitydomain *identity-domain*

The identity domain is a construct for managing certain features of Oracle Storage Infrastructure. Many features of Oracle Cloud are managed within and between domains.

--force

Forces association of the device with an existing Oracle Secure Backup created container.

devicename

Specifies the name of the cloud storage device

Examples**Example 3-3 Configuring a Tape Drive**

This example configures a tape drive.

```
ob> lsdev
library      lib1          in service
```

```

drive 1  tape1          in service
library  lib2          in service
drive 1  tape2          in service

```

```

ob> mkdev --type tape --inservice --library lib1 --erate 8 --dte 2
--blockingfactor 128 --uselist 1 --usage 4minute --automount yes hptape

```

```

ob> lsdev
library  lib1          in service
drive 1  tape1          in service
drive 2  hptape        in service
library  lib2          in service
drive 1  tape2          in service

```

Example 3-4 Configuring a Tape Library

This example configures a tape library.

```

ob> mkdev --type library --inservice --barcodereader yes --barcodesrequired yes
--autoclean no --cleanemptiest no hplib1

```

Example 3-5 Configuring a Disk Pool

This example configures a disk pool `dp1` with a capacity of 80GB. The file-system directory that stores backups associated with this disk pool is `/scratch/osb_test/virtual_devices/dp1` on the host `brhost3`. The number of concurrent jobs that can run on this disk pool is 15. When the space utilized exceeds 90 percent of the disk pool capacity, no new backup or restore jobs are scheduled for this disk pool.

```

ob> mkdev --type disk --inservice --attach brhost3:/scratch/osb_test/virtual_devices/
dp1 --capacity 80GB --freespacegoal 90 --concurrentjobs 15 dp1

```

Example 3-6 Configuring a Tape Library with Device File on Linux

This example specifies a device file while configuring the tape library `lib1` on Linux.

```

ob> mkdev -t library -a -J s06:/dev/obl3+stcontroller=1+sttarget=0+stlun=1 lib1
ob> lsdev lib1
lib1:
Device type:      library
Model:           [none]
Serial number:    [none]
In service:      yes
Debug mode:      no
Barcode reader:   default (hardware-selected)
Barcodes required: no
Auto clean:      no
Clean interval:   (not set)
UUID:            7fef35b4-18b1-102d-8c5b-00096b1b77b0
Attachment 1:
Host:            s08
Raw device:      /dev/obl3

```

Example 3-7 Configuring a Cloud Storage Device

This example configures a cloud storage device.

```

mkdev -t cloudstorage --identitydomain testacc --streamsperjob 8 --segmentsize 20mb
--url testacc.storage.oraclecloud.com --mediaserver brhost3
--username test.user@oracle.com -querypassphrase
--container mycont clodevice

```

```

ob> lsdev -l clodevice
clodevice:
  Device type:          cloud storage
  In service:          yes
  Debug mode:          no
  Capacity:            (not set)
  Consumption:         0
  Free space goal:     (system default)
  Concurrent jobs:     1
  Blocking factor:     (default)
  Max blocking factor: (default)
  UUID:                59824a0c-0b88-1035-bebf-0021f618cfbf
  Attachment 1:
    Host:              brhost3
  Staging:             no
  Username:            test.user@oracle.com
  Container:           mycont
  Storage Class:       object
  Segment size:        20
  Stream per job:      8
  Number of Objects:   0
  Bytes used:          0

```

3.1.4 mkds

Purpose

Use the `mkds` command to make a [dataset file](#) or [dataset directory](#).



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkds` command.

Syntax

```
mkds::=
```

```
mkds [ --nq ] [ --dir/-d ] [ --nocheck/-C ] [ --noedit/-E ] [ --input/-i ]
dataset-name...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--dir/-d

Creates a dataset directory called `dataset-name`.

A dataset directory is a directory that contains dataset files. Dataset directories can have a hierarchy of nested subdirectories that is up to 10 levels deep.

--nocheck/-C

Disables syntactic checking of a dataset file for errors.

--noedit/-E

Prevents a default editor window (as defined by your `EDITOR` environment variable) from opening when creating a dataset file.

--input/-i

Lets you to input the contents of a dataset file.

dataset-name

Specifies the name of the dataset directory or dataset file. The `mkds` command creates the dataset file or directory relative to the directory indicated by the `pwdds` (page 3-77) command. Refer to "[dataset-name](#) (page 4-8)" for a description of the `dataset-name` placeholder.

Usage Notes

- When you create a dataset file, be aware that the Oracle Secure Backup dataset statement, `exclude`, does not support exclusion of the NDMP backup type `zfs`.

However, Oracle Secure Backup does support the ability to send NDMP environmental variables to the Oracle ZFS Storage Appliance (ZFSSA) filer. The dataset statement `setenv NDMP` can be used to send exclude directives to the filer.

The `exclude` statement is only supported for ZFS dump type backups. It is not supported for ZFS type backups because the `exclude` statement is file-based and ZFS is block-based.

In a ZFSSA dump type backup, if you want to exclude a directory or file name (for example, `file-or-dirname`) then you must include the following statement before or after the `include path` line in the dataset description file:

```
setenv NDMP:EXCLUDE file-or-dirname
```

The following example shows the statement after the `include path` statement:

```
include host storabcknfs8
  include path /export/nfs7-restore-test
  setenv NDMP:EXCLUDE file-or-dirname
```

The `EXCLUDE` variable can contain one or more matching patterns, separated by commas, for files that should be excluded from the backup. The exclusion is recursive. The following rules are supported:

c	Any non-special character matches itself
?	Match any character
ab	Character a followed by character b
S	Any string of non-special characters
AB	String A followed by string B
*	Any string, including the empty string

Examples

Example 3-8 Creating a Dataset

This example creates a dataset directory called `mydatasets1` and then creates a dataset file called `test.ds` in this directory.

```
ob> pwdds
/ (top level dataset directory)
ob> mkds --dir mydatasets1
ob> mkds --nq --input mydatasets1/test.ds
Input the new dataset contents. Terminate with an EOF or a line
containing just a dot (".").
include host brhost2
include path /home
.
ob> lsds --recursive
Top level dataset directory:
mydatasets1/
mydatasets1/test.ds
```

Example 3-9 Creating a Dataset Subdirectory

This example creates a `not_used` subdirectory in the `mydatasets1` directory.

```
ob> pwdds
/mydatasets1
ob> mkds --dir not_used
ob> cdds ..
ob> pwdds
/ (top level dataset directory)
ob> lsds --recursive
Top level dataset directory:
mydatasets1/
mydatasets1/not_used/
mydatasets1/test.ds
```

Example 3-10 Creating a Dataset for a Windows Host

This example creates a dataset file named `c-winhost1.ds`. This file specifies the backup of drive `C:\` on a Windows host named `winhost1`.

```
ob> pwdds
/ (top level dataset directory)
ob> mkds --nq --input c-winhost1.ds
Input the new dataset contents. Terminate with an EOF or a line
containing just a dot (".").
include host winhost1
include path "C:\" {
exclude name *.log
}
.
ob> lsds
NEWCLIENTS
c-winhost1.ds
```

 **Notes:**

- Remote file systems that are mapped to drive letters on PCs cannot be backed up by Oracle Secure Backup.
- Because mapped drives are user-specific on Windows XP systems and Oracle Secure Backup runs as a service with its own security context, it cannot access drives mapped by any other users on the system. To work around this problem, back up the system that contains the mapped files directly, rather than trying to back them up from a system that maps them.

3.1.5 mkdup

Purpose

Create a [volume](#) duplication policy.

 **See Also:**

["Volume Duplication Commands \(page 1-22\)"](#)

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkdup` command.

Syntax

`mkdup::=`

```

mkdup
[ --comment/-c commentstring] [ --inputcomment/-i ]
[ --trigger/-e dupevent:duration ]
[ --restrict/-r restriction[,restriction]... ]
[ --migrate/-m { yes | no } ]
{ --rule/-u duplicationrule[,duplicationrule...] }
policyname...

```

Semantics

--comment/-c *commentstring*

A descriptive comment, displayed when using `lsdup`.

--inputcomment/-i

Prompt the backup administrator to enter a descriptive comment. After you run `mkdup --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--trigger/-e *dupevent:duration*

Specifies when a volume becomes eligible for duplication. The *duration* placeholder specifies how long after *dupevent* the volume becomes eligible for duplication.

--restrict/-r restriction...

Restricts duplication to specific devices within the [administrative domain](#). You can select [media server](#) hosts or specific devices on these hosts. You must have the `duplicateovernetwork` policy set to `yes` to duplicate a volume to a different media server than the one containing the [original volume](#) being duplicated. Oracle Secure Backup does not duplicate between devices attached to different media servers by default, because it requires heavy use of network bandwidth.

If you have set `duplicateovernetwork` to `yes` and do not specify a restriction (default), then this volume duplication policy has no device restrictions, and can use any available device on any media server at the discretion of the Oracle Secure Backup scheduling system.

 **See Also:**

- "[dupevent](#) (page 4-12)" for a description of the `dupevent` placeholder
- "[duration](#) (page 4-14)" for a description of the `duration` placeholder
- "[restriction](#) (page 4-25)" for a description of the `restriction` placeholder
- "[duplicateovernetwork](#) (page 7-17)" for more information on the `duplicateovernetwork` policy

--migrate/-m {yes|no}

Specifies volume to be migrated. If this option is set to `yes`, then only one rule can be specified for this volume duplication policy. If you do not specify the `--migrate` option, then the volume is not migrated.

--rule/-u duplicationrule

Specifies a duplication rule, in the form `media-family:number`.

Example**Example 3-11 Creating a Volume Duplication Policy**

This example creates a volume duplication policy with the trigger for the duplication event as the `firstwrite` and its duration as `forever`. This volume will not be migrated. It is restricted to the host `brhost3` and 2 duplicates will be created to the `RMAN-DEFAULT` media family.

```
ob> mkdup --trigger firstwrite:forever --migrate no --restrict @brhost3 --rule RMAN-
DEFAULT:2 voldup1
ob> lsdup --long voldup1
voldup1:
  Migrate:                no
  Trigger:                firstwrite : forever
  Restriction 1:         @brhost3
  Rule 1:                 RMAN-DEFAULT : 2
  UUID:                  db4bfd64-18af-1031-b040-00163e527899
```

3.1.6 mkhost

Purpose

Use the `mkhost` command to add a host to an [administrative domain](#). The host must run Oracle Secure Backup locally or be accessible to Oracle Secure Backup with [Network Data Management Protocol \(NDMP\)](#).



See Also:

"[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `mkhost` command.

Usage Notes

If your Windows host is protected by a [firewall](#), then the firewall must be configured to permit Oracle Secure Backup [daemons](#) on the host to communicate with the other hosts in your administrative domain. Windows XP Service Pack 2 and Windows Server 2003 contain a built-in Windows firewall which, in the default configuration, blocks inbound traffic on ports used by Oracle Secure Backup. Refer to *Oracle Secure Backup Installation and Configuration Guide* for more information.

Syntax 1

Use the following syntax to add a host that runs Oracle Secure Backup locally to an administrative domain.

`mkhost::=`

```
mkhost
[ --access/-a ob ]
[ --inservice/-o | --notinservice/-O ]
[ --encryption/-e { required | allowed } ]
[ --disablerds/-d { yes | no | systemdefault } ]
[ --algorithm/-l { AES128 | AES192 | AES256 } ]
[ --keytype/-t { passphrase | transparent } ]
[ --rekeyfrequency/-g duration ]
[ --passphrase/-s string ]
[ --querypassphrase/-Q ]
[ --tcpbufsize/-c bufsize ]
[ --ndmpauth/-A authtype ]
[ --roles/-r role[,role]... ]
[ --ip/-i ipname[,ipname]... ]
[ --nocomm/-N ]
[ --certkeysize/-k cert-key-size ]
[ --compression/-K {off | low | medium | basic | high} ]
hostname...
```

Semantics 1

Use these options if the host has Oracle Secure Backup installed and uses the Oracle Secure Backup internal communications protocol to communicate.

--access/-a ob

Specifies that the host accesses a local installation of Oracle Secure Backup. By default `obtool` determines dynamically whether the computer is accessed through the Oracle Secure Backup RPC protocol (plus NDMP) or solely through NDMP.

--encryption/-e {required | allowed}

Specifies whether encryption is required or allowed. If set to `required`, then all backups from this host are encrypted. If set to `allowed`, then encryption is determined by the global encryption policy and encryption settings specific to the [backup job](#). Default is `required`.

--disablerds/-d { yes | no | systemdefault }

Specifies whether Reliable Datagram Socket (RDS) over Infiniband is used for data transfer between clients and the media server. The valid values are:

- `yes`
Oracle Secure Backup does not use RDS for over Infiniband for data transfer between the host and media server.
- `no`
Oracle Secure Backup uses RDS over Infiniband for data transfer between the host and media server.
- `systemdefault`
This is the default setting. Oracle Secure Backup uses the setting made at the administrative domain level to decide if RDS must be used for data transfer. You use the operations policy `disablerds` to specify RDS usage at the administrative level. Therefore, if the `disablerds` operations policy is set to `no`, and the value of `--disablerds` for the host is set to `systemdefault`, the host uses RDS for data transfer.

The `--disablerds` setting at the host level overrides the setting that you made at the administrative domain level by using the `disablerds` operations policy. Therefore, if you set the operations policy `disablerds` to `no`, and, for a particular host, you set the `--disablerds` option of the `chost` command to `yes`, RDS is not used for data transfer host.

--algorithm/-l {AES128 | AES192 | AES256}

Specifies encryption algorithm used. Default is `AES192`.

--keytype/-t [passphrase | transparent]

Specifies how the encryption keys are generated. Values are:

- `passphrase`
The backup administrator supplies a passphrase, which is then used to generate encryption keys. The keys generated using a passphrase are not stored in the Oracle [wallet](#). If the passphrase is lost, then these backups cannot be restored.
- `transparent`

The encryption keys are generated automatically and stored in the Oracle wallet.

Default is `transparent`.

--rekeyfrequency/-g {disabled | *N duration* | systemdefault | perbackup}

Specifies how often a key is generated. Values are:

- `disabled`
Never generate a key
- `Nduration` (page 4-14)
Generate keys at the time interval specified. If *N* is 0, then Oracle Secure Backup never generates a key. The minimum duration is one day.
- `systemdefault`
Generate keys according to the global [rekeyfrequency](#) (page 7-6) policy.
- `perbackup`
Generate keys for each backup.

The default is `30days`.

--passphrase/-s

Specifies a passphrase used in generation of the encryption key.

The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the [Oracle Secure Backup user](#) be prompted for the password.

--querypassphrase/-Q

Queries for the passphrase used in generation of the encryption key.

--tcpbufsize/-c *bufsize*

Specifies [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#) buffer size. The default value is `not set`, in which case global policy `operations/tcpbufsize` applies. The maximum TCP/IP buffer size is 4GB, and the minimum TCP/IP buffer size is 1 KB. If Oracle Secure Backup cannot set TCP/IP buffer size as specified, then it returns a warning. This can happen when the operating system kernel limit is smaller than the specified TCP/IP buffer size.

Increasing TCP/IP buffer size also increases TCP/IP advertised window. So to tune backup over a wide area network (WAN), this parameter must be set to a value bigger than the bandwidth times round-trip time.

--inservice/-o

Specifies that the host is logically available to Oracle Secure Backup.

--notinservice/-O

Specifies that the host is not logically available to Oracle Secure Backup.

--roles/-r *role[,role]...*

Assigns one or more [roles](#) to the host. Refer to "[role](#) (page 4-25)" for a description of the `role` placeholder.

--ipl/-i *ipname[,ipname]...*

Indicates the IP address of the host computer. IP addresses are represented as a series of four numbers separated by periods. You can also use host names for IP

addresses. In this case, the host name is resolved by the underlying operating system to an IP address.

If you specify *ipname*, then Oracle Secure Backup never uses the user-assigned host name to obtain the host IP address; instead, it considers each specified *ipname* until it finds one that resolves to a working IP address. If you specified a [PNI \(Preferred Network Interface\)](#) for this host with the `mkpni` (page 3-40) command, then Oracle Secure Backup considers the PNI address first.

 **Note:**

The use of DHCP to assign IP addresses is not supported for hosts that participate in an Oracle Secure Backup administrative domain. You must assign static IP addresses to all hosts. If you cannot use static IP addresses, then ensure that the DHCP server guarantees that a given host is always assigned the same IP address.

If you do not specify *ipname*, then Oracle Secure Backup tries to resolve the specified *hostname* to obtain the IP address.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--nocomm/-N

Suppresses communication with the host computer. You can use this option to add a host to the domain when the host is not yet connected to the network.

--certkeysize/-k *cert-key-size*

Sets the size (in bits) of the [public key/private key](#) pair used for the [identity certificate](#) of this host. By default Oracle Secure Backup uses the value in the [certkeysize](#) (page 7-43) security policy. If you specify `--certkeysize`, then the specified value overrides the key size in the security policy. The key size set with `--certkeysize` applies only to this host and does not affect the key size of any other current or future hosts.

Because larger key sizes require more computation time to generate the key pair than smaller key sizes, the key size setting can affect the processing time of the `mkhost` command. While the `mkhost` command is running, `obtool` might display a status message every 5 seconds (see [Example 3-13](#) (page 3-33)). `obtool` displays a command prompt when the process has completed.

--compression/-K {off | low | medium | basic | high}

Specifies the compression option to use for all file system backups in this Oracle Secure Backup client where it is not set at the job level.

The possible values are as follows:

off

Software compression is not used for the backup regardless of global and client level policy

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the `medium` option. It is slower than the `low` and `medium` options, but faster than the `high` option.

high

Compresses data as much as possible, using extensive CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

The default value is that no compression option is set.

The compression option is available only to hosts running Oracle Secure Backup locally (`--access ob`).

Syntax 2

Use the following syntax to add a host that Oracle Secure Backup accesses with NDMP, such as a [filer](#), to an administrative domain.

`mkhost::=`

```
mkhost --access/-a ndmp [ --inservice/-o | --notinservice/-O ]
[ --encryption/-e { required | allowed } ]
[ --algorithm/-l { AES128 | AES192 | AES256 } ]
[ --keytype/-t { passphrase | transparent } ]
[ --rekeyfrequency/-g duration ]
[ --passphrase/-s string ]
[ --querypassphrase/-Q ]
[ --role/-r role[,role]... ] [ --ip/-i ipname[,ipname]... ]
[ --ndmpauth/-A authtype ]
[ { --ndmppass/-p ndmp-password } | --queryndmppass/-q | --dfndmppass/-D ]
[ --ndmpport/-n portnumber ] [ --ndmppver/-v protover ]
[ --ndmpuser/-u ndmp-username ] [ --nocomm/-N ]
[ --ndmpbackuptype/-B ndmp-backup-type ]
[ --backupev/-w evariable-name=variable-value ]...
[ --restoreev/-y evariable-name=variable-value ]...
hostname...
```

 **Note:**

For NDMP hosts, the following `mkhost` command options are only available starting with Oracle Secure Backup 10.3.0.2.0:

- encryption
- algorithm
- keytype
- rekeyfrequency
- passphrase
- querypassphrase

Semantics 2

Use these options if the host does not have Oracle Secure Backup installed (for example, a filer or [Network Attached Storage \(NAS\)](#) device) and uses NDMP to communicate.

--access/-a ndmp

Specifies that the host uses [Network Data Management Protocol \(NDMP\)](#) to communicate. An NDMP host is a storage appliance from third-party vendors such as NetApp, Mirapoint, or DynaStore. An NDMP host implements the NDMP protocol and employs NDMP daemons (rather than Oracle Secure Backup daemons) to back up and restore file systems.

--algorithm/-l {AES128 | AES192 | AES256}

Specifies encryption algorithm used. Default is AES192.

--encryption/-e {required | allowed}

Specifies encryption algorithm used. Default is AES192.

--rekeyfrequency/-g {disabled | *N duration* | systemdefault | perbackup}

Specifies how often a key is generated. Values are:

- disabled
Never generate a key
- *N duration* ([page 4-14](#))
Generate keys at the time interval specified. If *N* is 0, then never generate a key. The minimum duration is one day.
- systemdefault
Generate keys according to the global [rekeyfrequency](#) ([page 7-6](#)) policy.
- perbackup
Generate keys for each backup.

Default is 30days.

--keytype/-t {passphrase | transparent}

Specifies how the encryption keys are generated. Values are:

- passphrase
The backup administrator supplies a passphrase, which is then used to generate encryption keys.
- transparent
The encryption keys are generated automatically and stored in the Oracle Wallet.

--inservice/-o

Specifies that the host is logically available to Oracle Secure Backup.

--notinservice/-O

Specifies that the host is not logically available to Oracle Secure Backup.

--role/-r *role[,role]...*

Assigns a role to the host. Refer to "[role](#) ([page 4-25](#))" for a description of the *role* placeholder.

--ipl-i *ipname*[,*ipname*]...

Indicates the IP address of the host computer. The use of DHCP to assign IP addresses is not supported for hosts that participate in an Oracle Secure Backup administrative domain. You must assign static IP addresses to all hosts. If you cannot use static IP addresses, then ensure that the DHCP server guarantees that a given host is always assigned the same IP address.

**Note:**

You can use host names for IP addresses. In this case, the host name is resolved by the underlying operating system to an IP address.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.

--ndmpauth/-A *authtype*

Provides an authorization type. Refer to "[authtype](#) (page 4-3)" for a description of the *authtype* placeholder.

The authorization type is the mode in which Oracle Secure Backup authenticates itself to the NDMP server. Typically, you should use the *negotiated* default setting. You can change the setting if necessary; for example, if you have a malfunctioning NDMP server.

--ndmppass/-p *ndmp-password*

Specifies an NDMP password. The password is used to authenticate Oracle Secure Backup to this NDMP server. If you do not specify this option, and if you do not specify `--queryndmppass`, then Oracle Secure Backup uses the default NDMP password defined in the `ndmp/password` (page 7-29) policy.

--queryndmppass/-q

Prompts you for the NDMP password.

--dftndmppass/-D

Uses the default NDMP password defined in the `ndmp/password` (page 7-29) policy.

--ndmpport/-n *portnumber*

Specifies a TCP port number for use with NDMP. Typically, the port 10000 is used. You can specify another port if this server uses a port other than the default.

--ndmppver/-v *protover*

Specifies a protocol version. Refer to "[protover](#) (page 4-24)" for a description of the *protover* placeholder. The default is null (""), which means "as proposed by server."

--ndmpuser/-u *ndmp-username*

Specifies a user name. The user name is used to authenticate Oracle Secure Backup to this NDMP server. If left blank, then the user name value in the `ndmp/username` (page 7-31) policy is used.

--nocomm/-N

Suppresses communication with the host computer. You can use this option to add a host to the domain when the host is not yet connected to the network.

--ndmpbackuptype/-B *ndmp-backup-type*

Specifies a default NDMP backup format. The default is defined by the NDMP [data service](#) running on the client. Refer to "[ndmp-backup-type](#) (page 4-20)" for a description of the *ndmp-backup-type* placeholder.

--backupevl-w *evariable-name=variable-value*

Declares NDMP backup environment variables that are passed to the host's NDMP Data Service for a backup.

--restoreevl-y *evariable-name=variable-value*

Declares NDMP restore environment variables that are passed to the host's NDMP Data Service for a restore.

hostname

Specifies name of the host to be added to the administrative domain. Note that you cannot specify multiple hosts if you specify an IP address with the `--ip` option. Host names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Examples**Example 3-12 Adding a Host Running Oracle Secure Backup Locally**

This example adds host `sfserver1`, which runs Oracle Secure Backup locally, to the administrative domain.

```
ob> lshost
brhost2          client                      (via OB)  in service
brhost3          mediaserver,client              (via OB)  in service
osbsvr1          admin,mediaserver,client          (via OB)  in service
ob> mkhost --access ob --inservice --roles mediaserver,client --nocomm sfserver1
ob> lshost
brhost2          client                      (via OB)  in service
brhost3          mediaserver,client              (via OB)  in service
sfserver1        mediaserver,client              (via OB)  in service
osbsvr1          admin,mediaserver,client          (via OB)  in service
```

Example 3-13 Adding a Host with a Large Key Size

This example adds a host with a [certificate](#) key size of 4096. The sample output shows the periodic status message.

```
ob> mkhost --inservice --role client --certkeysize 4096 osbsvr2
Info: waiting for host to update certification status...
ob> lshost osbsvr2
osbsvr2          client                      (via OB)  in service
```

Example 3-14 Adding an NDMP Host

This example adds a host that Oracle Secure Backup accesses with NDMP. Due to space constraints the sample command has been reformatted to fit on the page.

```
ob> mkhost --nocomm --access ndmp --ip 192.0.2.151 --inservice --roles client
--ndmpauth none --ndmpuser jim --ndmppass mypassword --ndmppver "" ndmphost1
ob> lshost
```

brhost2	client	(via OB)	in service
brhost3	mediaserver,client	(via OB)	in service
sfserver1	mediaserver,client	(via OB)	in service
ndmphost1	client	(via NDMP)	in service
osbsvr1	admin,mediaserver,client	(via OB)	in service

3.1.7 mkloc

Purpose

Create a [location](#) object.

Note:

The `mkloc` command can only be used to create a [storage location](#). Oracle Secure Backup automatically creates an [active location](#) corresponding to each [tape library](#) and [tape drive](#) in the [administrative domain](#).

See Also:

"[Location Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkloc` command.

Syntax

`mkloc::=`

```
mkloc
  [ --inputcomment/-i | --comment/-c comment ]
  [ --mailto/-m email-target[,email-target]... ]
  [ --customerid/-I customerid ]
  [ --notification/-n ntype ]
  [ --recalltime/-R duration ]
  locationname...
```

Semantics

--inputcomment/-i

Allows input of an optional comment for the location. After you run `mkloc --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--comment/-c *commentstring*

Specifies a descriptive comment for the location.

--customerid/-I *idstring*

A customer ID string. Note: Only valid for storage locations.

--mailto/-m *email-target*[,*email-target*]...

The e-mail addresses specified here receive the pick or distribution reports for media movement involving volumes at the specified location. An e-mail system must be operational on the [administrative server](#) for this feature to operate. Separate multiple entries with a comma.

--notification/-n *ntype*

The `--notification ntype` option enables you to specify a type of electronic notification to be sent to the offsite vault vendor when media are moved from or to a storage location. The `ntype` value is either `none` or `imftp` (Iron Mountain FTP file).

---recalltime/-R *duration*

The `--recalltime` option enables you to specify the time taken to recall a [volume](#) from this storage location to the data center. This setting is disabled for an [active location](#) and is valid only for offsite storage locations. You can use this setting to determine whether to fail a restore request initiated by [Recovery Manager \(RMAN\)](#) that requires use of tape volumes that cannot be supplied within the specified resource wait time period. This parameter can also be used by the volume cloning feature to determine which volume to recall for a restore operation when multiple copies are available at multiple offsite locations.

locationname

The name of the storage location.

 **Note:**

`all` is a reserved word and cannot be used as a location name.

Example**Example 3-15 Creating a Location Object**

This example creates the location object `testloc`. The email target for this location is `john.doe@oracle.com` and its recall time is 1 year. No notifications will be provided for any media movement in this storage location.

```
ob> mkloc --mailto john.doe@oracle.com --recalltime 1y --notification none testloc
ob> lsloc --long
Media_Recycle_Bin:
  Comment:          OSB-generated location
  Recalltime:       disabled
  UUID:             632c3c50-0e77-1031-8e47-00163e527899
testloc:
  Recalltime:       1 year
  Mail to:          john.doe@oracle.com
  UUID:             3331c846-18c0-1031-b040-00163e527899
vlib1:
  Associated device: vlib1 (library)
  Comment:          OSB-generated location for library vlib1
  Recalltime:       disabled
  UUID:             712a478e-0e77-1031-b040-00163e527899
```

3.1.8 mkmf

Purpose

Use the `mkmf` command to create a [media family](#), which is a named classification of backup volumes. A media family ensures that volumes created at different times have similar characteristics. For example, you can create a media family for backups with a six-month [retention period](#). If you specify this family on successive [backup](#) (page 2-4) commands, then all created volumes have a six-month retention period.

A media family has either of the following types of mutually exclusive expiration policies: content-managed (default) or time-managed. In a content-managed policy, volumes expire only when every [backup piece](#) recorded on a [volume](#) has been marked as deleted. In a time-managed policy, volumes expire when they reach the expiration time, which is calculated as the sum of the `--writewindow` time, the `--retain` time, and the [volume creation time](#).



See Also:

"[Media Family Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkmf` command.

Syntax

`mkmf::=`

```
mkmf [ --writewindow/-w duration ] [ --retain/-r duration ]
[ [ --vidunique/-u ] |
  [ --vidfile/-F vid-pathname ] |
  [ --viddefault/-d ] |
  [ --vidfamily/-f media-family-name ] ]
[ [ --inputcomment/-i |
  [ --comment/-c comment ] ]
[ --contentmanaged/-C ] [ --append/-a ] [ --noappend/-A ]
[ --rotationpolicy/-R polycyname ]
[ --duplicationpolicy/-D polycyname ]
[ --acsscratchid/-d acsscratch_id ]
media-family-name...
```

Semantics

`--writewindow/-w duration`

Specifies a write-allowed time period for the media family. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default is `disabled`, which means that Oracle Secure Backup does not consider the [write window](#) when computing the [volume expiration time](#).

A write window is the period for which a [volume set](#) remains open for updates, usually by appending backup image instances. All volumes in the family are considered part

of the same volume set. The write window opens when Oracle Secure Backup writes the first file to the first volume in the set and closes after the specified period elapses. When the write window closes, Oracle Secure Backup disallows further updates to the volume set until one of the following conditions is met:

- It expires.
- It is relabeled.
- It is reused.
- It is unlabeled.
- It is forcibly overwritten.

Oracle Secure Backup continues using the volume set for backup operations until the write window closes.

Note that if you select `forever` or `disabled` as a *duration*, then you cannot enter a number. For example, you can set the write window as `14days` or specify `forever` to make the volume set eligible to be updated indefinitely. All volume sets that are members of the media family remain open for updates for the same time period. This option has no effect for media families used for automated tape duplication.

--retain/-r *duration*

Specifies the retention period, which is amount of time to retain the volumes in the volume set. By specifying this option, you indicate that this media family is time-managed rather than content-managed. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

The volume expiration time is the date and time on which a volume expires. Oracle Secure Backup computes this time by adding the write window duration (`--writewindow`), if it is specified, to the time at which it wrote [backup image file](#) number 1 to a volume, and then adding the volume retention time (`--retain`).

The retention period prevents you from overwriting any volume included as a member of this media family until the end of the specified time period. If one volume becomes full, and if Oracle Secure Backup continues the backup onto subsequent volumes, then it assigns each volume in the volume set the same retention time.

You can make [Recovery Manager \(RMAN\)](#) backups to time-managed volumes. Thus, volumes with a [time-managed expiration policy](#) can contain a mixture of file-system and RMAN backup pieces.

Note:

If you make RMAN backups to time-managed volumes, then it is possible for a volume to expire and be recycled while the RMAN repository reports the backup pieces as available. In this case, you must use the `CROSSCHECK` command in RMAN to resolve the discrepancy.

You can change a media family from time-managed to content-managed by specifying `--contentmanaged` on the [chmf](#) (page 2-52) command.

Media families used for automated tape duplication must have the same [expiration policy](#) as the associated original volumes. If the [original volume](#) has a time-managed expiration policy, then the duplicate volumes must be time-managed as well.

--vidunique/-u

Creates a [volume ID](#) unique to this media family. The volume ID begins with the string *media-family-name-000001* and increments the [volume sequence number](#) each time it is used. For example, *MYVOLUME-000001* would be the volume ID for the first volume in the *MYVOLUME* media family, *MYVOLUME-000002* would be the ID for the second volume, and so forth.

--vidfile/-F vid-pathname

Specifies the name of the [volume sequence file](#) for the media family that you are creating. Specify either a relative filename, in which case the file is created in the administrative directory on the [administrative server](#), or an absolute filename. Because Oracle Secure Backup does not create this file automatically, you must create it manually. If you select the `--vidfile` option, then use a text editor to customize the *vid-* prefix. Enter the first volume ID to be assigned to the media family as a single line of text, for example, *MYVOLUME-000001*.

**Note:**

You must create the volume ID file before specifying the `--vidfile` option.

--viddefault/-d

Specifies the system default, that is, Oracle Secure Backup uses the same volume ID sequencing that it would use if no media family were assigned. The default volume ID begins at *VOL000001* and increments each time it is used.

--vidfamily/-f media-family-name

Uses the same volume ID sequencing as is used for the media family identified by *media-family-name*.

--inputcomment/-i

Allows input of an optional comment for the media family. After you run `mkmf --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--comment/-c comment

Specifies information to store with the media family. To include white space in the *comment*, surround the text with quotes.

--contentmanaged/-C

Specifies that volumes in this media family are content-managed rather than time-managed. Volumes that use this expiration policy are intended for RMAN backups: you cannot write a [file-system backup](#) to a content-managed volume. A content-managed volume is eligible to be overwritten when all backup image sections have been marked as deleted. You can delete backup pieces through RMAN or through the [rmpiece](#) (page 3-123) command in `obtool`. A volume in a content-managed volume set can expire even though other volumes in the same set are not expired.

You can change a media family from content-managed to time-managed by specifying `--retain` on the [chmf](#) (page 2-52) command.

Media families used for automated tape duplication must have the same expiration policy as the associated original volumes. If the original volume has a [content-managed expiration policy](#), then the duplicate volumes must be content-managed as well.

--append/-a

Specifies that additional backup image instances can be appended to volumes in the media family (default). This option has no effect for media families used for automated tape duplication.

Although a volume might be unexpired and have tape remaining, Oracle Secure Backup does not write to a volume that is lower than the most recent volume sequence number for the media family. Every backup tries to append to the most recent volume in the media family. If this volume is full, then it writes to a different volume.

--noappend/-A

Specifies that additional backup image instances cannot be appended to volumes in the media family. This option ensures that a volume set contains only a single backup image instance, which is useful if you perform a [full backup](#) and then use the tapes to re-create the original file system.

--rotationpolicy/-R

Specifies the [rotation policy](#) for the media family.

This option has no effect for media families used for automated tape duplication. To clear the rotation policy, specify an empty string ("") for the policy name.

--duplicationpolicy/-D

Specifies the duplication policy for the media family.

To clear the duplication policy, specify an empty string ("") for the policy name.

--acsscratchid/-d *acsscratch_id*

For ACSLS libraries this option defines the scratch pool ID from which volumes are pulled. For non-ACSLs libraries this option has no effect. When a volume is unlabeled it is placed back into the scratch pool ID that is defined by the media family it belonged to when it was unlabeled.

media-family-name

Specifies the name of the media family to create. Media family names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 24 characters.

Examples**Example 3-16 Creating a Time-Managed Media Family**

This example creates a time-managed media family called `time-man-family`. Volumes in the volume set are available for update for 7 days. Because the retention period is 28 days, a volume in the media family expires 35 days after Oracle Secure Backup first writes to it.

```
ob> mkmf --vidunique --writewindow 7days --retain 28days time-man-family
```

Example 3-17 Creating a Content-Managed Media Family

This example creates a content-managed media family called `content-man-family`. Because the write window is `forever`, volumes in this family are eligible for update indefinitely. Volumes only expire when RMAN shows the status of all backup pieces on the volumes as `DELETED`.

```
ob> mkmf --vidunique --writewindow forever content-man-family
```

3.1.9 mkpni

Purpose

Use the `mkpni` command to define a **PNI (Preferred Network Interface)** for an existing host. A network can have multiple physical connections between a **client** and the server performing a backup or restore on behalf of that client. The `mkpni` command is used to configure an outbound interface for a host and a preferred inbound interface for incoming connections from a set of hosts.

A PNI for inbound connections enables you to specify which of the host's network interfaces is used when a remote host connects to this host. The number of PNIs for an inbound connection depends on the number of interfaces available on the host. A PNI for outbound connections specifies the network and interface that must be used when the host connects to a remote host. The number of PNIs for outbound connections depends on the number of networks to which the host is connected.



See Also:

"Preferred Network Interface Commands (page 1-19)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkpni` command.

Syntax

```
mkpni::=
```

```
mkpni
[ --interface/-i ipname
{ --client/-c client-hostname[,client-hostname]... } ]
[ {--network/-n network/prefix,ipaddr .../ {--useonly/-o ipaddr} ]
hostname
```

Semantics

--interface/-i *ipname*

Specifies the IP address or the DNS host name that the specified clients should use when communicating with the host specified by *hostname*. Use this option to configure an interface for inbound connections to a particular host.

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), mixed IPv4/IPv6 environments on all platforms that support IPv6, and RDS/RDMA (Reliable Datagram Socket/Remote Direct Access Memory) if the client supports RDS/RDMA.

--client/-c *client-hostname*[,*client-hostname*]...

Specifies one or more clients that should use the *ipname* when communicating with *hostname*. The *client-hostname* specifies the host name or internet address of the client as seen from the server. The *hostname* must be a host name that you created with the `mkhost` (page 3-26) command.

You cannot use this option with the `--network` or `--useonly` options in a single `mkpni` command.

`--network/-n network/prefix, ipaddr`

Specifies the network that must be used for all outbound connections from the host specified by *hostname*. Optionally, you can specify a bind address for the network. Oracle Secure Backup binds the specified address for outgoing connections. When no bind address is specified, the operating system determines the bind address. *network/prefix* represents the network address with the prefix length. *ipaddr* represents the IP address to bind for outbound connection and this address must exist in the host object. Multiple outbound networks can be configured for a host. However, for each network, you can specify only one bind address. You can use this option to select RDS as the outbound connection.

If the host to which a connection must be created does not belong to any of the configured PNI networks, you can specify that any available network path can be used to establish a connection to that host. Use the following network addresses to configure any available network for outgoing connections:

- 0.0.0.0/0 for IPv4 connections
- 0::0/0 for IPv6 connections
- 0/0 for IPv4 or IPv6 connections

`--useonly/-o ipaddr`

Specifies that only the interface represented by *ipaddr* must be used for all outbound connections from the host *hostname*. *ipaddr* must exist in the host object. You can configure one interface for each address family (IPv4 and IPv6). You must not use this option for RDS connections.

hostname

Specifies the name of the host for which PNI is being configured.

Example

Example 3-18 Defining a PNI

This example defines a PNI that specifies that the client hosts `osbsvr1` and `brhost3` should use the IP address `192.0.2.1` when communicating with server `brhost2`.

```
ob> mkpni --interface 192.0.2.1 --client osbsvr1, brhost3 brhost2
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        osbsvr1, brhost3
```

Example 3-19 Configuring a Single Interface for Outbound Connections

This example configures a PNI for all outbound connections from the host `brhost2`. Including the `--useonly` option indicates that the specified network must be used for all outbound connections.

```
ob> mkpni --useonly 192.0.2.25 brhost2
ob> lspni
brhost2:
  UNI 1:
    useonly: 192.0.2.25
```

Example 3-20 Configuring a Network for Outbound Connections

This example configures a PNI for outbound connections from the host `brhost3`. The following two networks are configured as PNI: `192.51.100.0/24` and `203.0.113.0/24`. When making outbound connections from `brhost3`, Oracle Secure Backup checks the ipnames in the remote host object. The first ipname in the remote host object that matches any specified outbound network, `192.51.100.0/24` or `203.0.113.0/24`, is used. For example, if the remote host has ipname `203.0.113.4`, and it appears before `192.51.100.33` in the list of ipnames in the host object, then `203.0.113.4` is used for the outbound connection.

```
ob> mkpni --network 192.51.100.0/24,192.51.100.11 --network 203.0.113.0/24 brhost3
ob> lspni
brhost3:
  ONI 1:
    network: 192.51.100.0/24
    interface: 192.51.100.11
  ONI 2:
    network: 203.0.113.0/24
```

Example 3-21 Using Any Network to Establish and Outbound Connection

This example configures a PNI for outbound connections from the host `brhost3`.

When creating an outbound connection from `brhost3`, Oracle Secure Backup checks the ipnames in the remote host object. If the ipname on the remote host is part of the network `192.51.100.0/24`, then this ipname is used and the outbound connection binds to the interface `192.51.100.11`. If the ipname on the remote host is not part of the same subnet, then no binding is performed.

```
ob> mkpni --network 192.51.100.0/24,192.51.100.11 --network 0.0.0.0/24 brhost3
ob> lspni
brhost3:
  ONI 1:
    network: 192.51.100.0/24
    interface: 192.51.100.11
  ONI 2:
    network: 0.0.0.0/0
```

3.1.10 mkrot

Purpose

Create a [rotation policy](#).



See Also:

["Rotation Policy Commands \(page 1-20\)"](#)

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkrot` command.

Syntax

mkrot::=

```
mkrot [ --comment/-c commentstring | --inputcomment/-i commentstring ]
--rule/-u rotation-rule[,rotation-rule]. . .
policyname. . .
```

Semantics

--comment/-c *commentstring*

A descriptive comment, displayed when using `lsrot`. You can specify either `--comment` or `--inputcomment`, but not both.

--inputcomment/-i

Allows input of an optional comment. After you run `mkrot --inputcomment`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself. You can specify either `--comment` or `--inputcomment`, but not both.

--rule/-u *rotation-rule*

Specifies a set of rotation rules to be applied to the rotation policy.

The *rotationrule* argument is of the form *locationname[:event[:duration]]*, where

- *locationname* is either the name of an existing [location](#) object or a wildcard (*).

If an existing location object is specified as the first *locationname* in a rotation rule, then the rotation rule is constrained to that location. If a wildcard (*) is specified as the first location in a rotation rule, then the rotation rule can apply to any active location. A wildcard is permitted only for the first *locationname* in a rotation rule.

A location can appear only once in a rotation policy. An attempt to include a location more than once in the entire set of location/duration tuples for the rotation policy results in an error message and failure of the command.

- *event* is the volume-specific event that triggers the point at which the duration specified in this tuple begins to count. The event value can be one of the following:

— `firstwrite`

This is the point at which the first write to a [volume](#) occurs. This value is valid only for an [active location](#).

— `lastwrite`

This is the point at which the last write to a volume occurs. This value is valid only for an active location.

— `windowclosed`

This is the point at which the [write window](#) closes. This value is valid only for an active location.

— `nonwritable`

This is the point at which a volume can no longer be written to, either because the write window has closed or because the volume is full. This value is valid only for an active location.

- `arrival`
This is the point at which the volume arrived at this location. This value is valid only for a [storage location](#).
- `expiration`
This is the point at which the volume expires. This value is valid only for a storage location.
- `duration`
This is the length of time media remain at the location specified in this tuple. It is expressed in standard Oracle Secure Backup time duration syntax.

The duration value must be specified for all locations except a buffer location. The duration value is expressed as an integer `n` followed by seconds, minutes, hours, days, weeks, months, or years. Examples of valid values are `14days`, `3weeks`, and `2months`.

If you specify `DISABLED` as the duration value, then the volume remains at the associated location forever. The `DISABLED` value is allowed only for the final location in a rotation policy.

policyname

Specifies the name for a rotation policy, which can be 1-31 characters.

3.1.11 mksched

Purpose

Use the `mksched` command to create a backup, vaulting scan, duplication scan, or stage scan schedule.

A schedule contains 0 or more triggers. A [trigger](#) is a user-defined set of days (`--day`) and times (`--time`) when the [scheduled backup](#), vaulting scan, or duplication scan should run. At the beginning of the day, Oracle Secure Backup inspects the triggers in each enabled schedule.

You can use the [chsched](#) (page 2-58) command to add, change, or remove triggers in an existing schedule.

**See Also:**

"[Schedule Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mksched` command.

To use the `--user` option, you must have the following rights: Perform file system backups as privileged user, Modify any backup, regardless of its owner, and Modify any job, regardless of its owner.

Syntax 1

Use the following syntax to create a [backup schedule](#), which describes what, when, and how Oracle Secure Backup should back up. The backup schedule contains the name of each [dataset](#) and its associated [media family](#).

For each trigger that fires on a particular day, Oracle Secure Backup creates one [backup job](#) for each dataset listed in the schedule. Unlike on-demand (one-time-only) backups created with the [backup](#) (page 2-4) command, the [scheduler](#) creates jobs directly and does not first create a [backup request](#).

mksched::=

```
mksched
  [ --type/-Y backup ]
  [ --dataset/-D dataset-name[,dataset-name]... ]
  [ --comment/-c comment | --inputcomment/-i ]
  [ --priority/-p schedule-priority ]
  [ --restrict/-r restriction[,restriction]... ]
  [ --enabled/-z | --disabled/-Z ]
  [ --encryption/-e { yes | no } ]
  [ [ --day/-d day-date ] [ --time/-t time ]
    [ --level/-l backup-level ][ --family/-f media-family-name ]
    [ --expires/-x duration ] ]...
  [--user/-u user-name]
  [ --compression/-K {off | low | medium | basic | high}]
  schedulename ...
```

Semantics 1

--type/-Y schedule-type

Specifies the type of schedule to create. Valid values are `backup`, `duplicationscan`, `vaultingscan`, and `stagescan`.

--dataset/-D dataset-name

Specifies the dataset to include in the backup job.

If no datasets are specified in the schedule, then Oracle Secure Backup does not initiate backups based on the schedule. You can add a dataset to an existing schedule by using the [chsched](#) (page 2-58) command.

--comment/-c comment

Adds a comment to the schedule.

--inputcomment/-i

Prompts for a comment. After you run `mksched`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--priority/-p schedule-priority

Assigns a schedule priority to a backup. Refer to "[schedule-priority](#) (page 4-26)" for a description of the `schedule-priority` placeholder.

--restrict/-r restriction

Restricts the backup to specific devices within an [administrative domain](#). You can select [media server](#) hosts or specific devices on these hosts. If you do not specify a restriction (default), then the current schedule has no device restrictions and can use any available device on any media server at the discretion of the Oracle Secure

Backup scheduling system. Refer to "[restriction](#) (page 4-25)" for a description of the *restriction* placeholder.

--enabled/-z

Specifies that the backup schedule be enabled when created. If you do not specify either `--enabled/-z` or `--disabled/-Z`, then the schedule is enabled when created.

--disabled/-Z

Specifies that the backup schedule be disabled when created. If you specify this option, then you can later enable the backup schedule with a `chsched` command.



See Also:

"[chsched](#) (page 2-58)"

--encryption/-e {yes | no}

Specifies encryption flags for the backup schedule or job. Valid values are:

- `yes`
Backups for these scheduled jobs are always encrypted, regardless of settings for the global or host-specific encryption policies.
- `no`
If the global or host-specific encryption policies are set to `allowed`, then backups created for these jobs are not encrypted. This is the default.
If both global and host-specific encryption policies are set to `allowed`, then backups created for these jobs are not encrypted.
If either the global encryption policy or the host-specific encryption policy is set to `required`, then that policy overrides this setting and backups are always encrypted. The encryption algorithm and keys are determined by the policies of each [client](#) host.

--day/-d *day-date*

Specifies the day on which Oracle Secure Backup triggers the scheduled backup. If you do not specify a day or time, then Oracle Secure Backup does not run backup jobs based on the schedule. If you specify a day but no time, then the time defaults to 00:00. Refer to "[day-date](#) (page 4-9)" for a description of the *day-date* placeholder.

--time/-t *time*

Specifies the time at which Oracle Secure Backup triggers the scheduled backup. You cannot specify a time without a day. Refer to "[time](#) (page 4-29)" for a description of the *time* placeholder.

--level/-l *backup-level*

Identifies a [backup level](#). The default is `full`. Refer to "[backup-level](#) (page 4-4)" for a description of the *backup-level* placeholder.

--family/-f *media-family-name*

Specifies the name of the media family to which the data of this scheduled backup should be assigned. The default is the `null` media family.

--expires/-x *duration*

Specifies an expiration time period. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder. Specifying this option expires the backup, vaulting scan, or duplication scan if it is not processed by *duration* after the trigger time.

--user/-u *username*

Specifies the name of the Oracle Secure Backup user who owns the created backups.

schedulename

Specifies the name of the schedule to create. Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

--compression/-K {*off* | *low* | *medium* | *basic* | *high*}

Specifies the compression option to use for the backup schedule job that overrides any global and client-level compression options already set.

The possible values are as follows:

off

Software compression is not used for the backup regardless of global and client level policy

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the *medium* option. It is slower than the *low* and *medium* options, but faster than the *high* option.

high

Compresses data as much as possible, using extensive CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

The default value is that no compression option is set.

If compression is not specified as part of the `mksched` command, then the client host setting for compression is used. If the client host compression setting is not set, then the domain-level policy is used. If the domain-level policy is also not set, then no software compression is performed for this job.

Syntax 2

Use the following syntax to create a vaulting scan schedule, which describes the time or times when Oracle Secure Backup scans the volumes [catalog](#) to determine which volumes are eligible for vaulting. Vaulting schedules have the `--type` option set to `vaultingscan`. Vaulting scan control job types are queued for processing by the media manager component of Oracle Secure Backup at the time or times specified in the schedule.

The scan occurs on a location-by-location basis. Scheduled vaulting jobs run in specified vaulting windows and when resources are available.

mksched::=

```
mksched
[ --type/-Y vaultingscan ]
[ --comment/-c comment|--inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --restrict/-r vault_restriction[,vault_restriction]... ]
[ --location/-L location_name[,location_name]... ]
[ --enabled/-z | --disabled/-Z ]
[ --select/-S select_criterion[,select_criterion]... ]
[ [ --day/-d day-date ] [ --time/-t time ] [ --expires/-x duration ] ]...
schedulename...
```

Semantics 2

--type/-Y *schedule-type*

Specifies the type of schedule to create. Valid values are `backup`, `duplicationscan`, `vaultingscan`, and `stagescan`.

--comment/-c *comment*

Adds a comment to the schedule.

--inputcomment/-i

Prompts for a comment. After you run `mksched`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--priority/-p *schedule-priority*

Assigns a schedule priority to a vaulting scan. Refer to "[schedule-priority](#) (page 4-26)" for a description of the `schedule-priority` placeholder.

--restrict/-r *vault_restriction*[,*vault_restriction*]...

Restricts a vaulting scan to one or more locations. The locations can be specified in any of the following forms:

- `location_name@cap_name`
The `location_name` is the location that is scanned during a scan job for volumes eligible to be moved. The cartridge access port (CAP) name can be specified only if the location is an ACSLS library.
- `location_name`
If `location_name` is an ACSLS library and no CAP name is specified, then Oracle Secure Backup selects the largest available CAP.
- `@cap_name`
If no location name is specified, then the location of the specified CAP is scanned. This form applies only to ACSLS libraries.

If the ejection type for the library is set to `automatic` or `ondemand`, then Oracle Secure Backup exports volumes to the specified CAP during a media movement job.

--location/-L *locationname*

Specifies one or more locations to be applied to the vaulting scan schedule. If no location is specified, then the schedule applies to all locations.

 **Note:**

The `--location` option is deprecated for vaulting scan schedules in this release, but it is supported for backward compatibility. Oracle recommends that you use the `--restrict` option to limit vaulting scans to particular locations.

--enabled/-z

Specifies that the vaulting scan schedule be enabled when created. If you do not specify either `--enabled/-z` or `--disabled/-Z`, then the schedule is enabled when created by default.

--disabled/-Z

Specifies that the vaulting scan schedule be disabled when created. If you specify this option, then you can later enable the backup schedule with a `chsched` command.

 **See Also:**

"[chsched](#) (page 2-58)"

--select/-S *select_criterion*

Restricts a vaulting scan to one or more media families.

--day/-d *day-date*

Specifies the day on which Oracle Secure Backup triggers the scheduled vaulting scan. If you do not specify a day or time, then Oracle Secure Backup does not run vaulting scan jobs based on the schedule. If you specify a day but no time, then the time defaults to 00:00. Refer to "[day-date](#) (page 4-9)" for a description of the *day-date* placeholder.

--time/-t *time*

Specifies the time at which Oracle Secure Backup triggers the scheduled vaulting scan. You cannot specify a time without a day. Refer to "[time](#) (page 4-29)" for a description of the *time* placeholder.

--expires/-x *duration*

Specifies an expiration time period. Specifying this option expires the vaulting scan if it is not processed by *duration* after the trigger time.

See "[duration](#) (page 4-14)" for more information on the *duration* placeholder.

schedulename

Specifies the name of the schedule to create. Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Syntax 3

Use the following syntax to create a duplication schedule, which describes the time or times when Oracle Secure Backup scans the volumes [catalog](#) to determine which volumes are eligible for duplication. Duplication schedules have the `--type` option set to `duplicationscan`. Duplication scan control job types are queued for processing by

the media manager component of Oracle Secure Backup at the time or times specified in the schedule.

The scan occurs on a location-by-location basis. Scheduled duplication jobs run in specified duplication windows and when resources are available.

mksched::=

```
mksched
[ --type/-Y duplicationscan ]
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ --location/-L locationname[,locationname]... ]
[ [ --day/-d day-date ] [ --time/-t time ] [ --expires/-x duration ] ]...
schedulename...
```

Semantics 3

--type/-Y *schedule-type*

Specifies the type of schedule to create. Valid values are `backup`, `duplicationscan`, `vaultingscan`, and `stagescan`.

--comment/-c *comment*

Adds a comment to the schedule.

--inputcomment/-i

Prompts for a comment. After you run `mksched`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--priority/-p *schedule-priority*

Assigns a schedule priority to a duplication scan. Refer to "[schedule-priority](#) (page 4-26)" for a description of the `schedule-priority` placeholder.

--day/-d *day-date*

Specifies the day on which Oracle Secure Backup triggers the scheduled duplication scan. If you do not specify a day or time, then Oracle Secure Backup does not run duplication scan jobs based on the schedule. If you specify a day but no time, then the time defaults to 00:00. Refer to "[day-date](#) (page 4-9)" for a description of the `day-date` placeholder.

--time/-t *time*

Specifies the time at which Oracle Secure Backup triggers the scheduled duplication scan. You cannot specify a time without a day. Refer to "[time](#) (page 4-29)" for a description of the `time` placeholder.

--expires/-x *duration*

Specifies an expiration time period. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. Specifying this option expires the duplication scan if it is not processed by `duration` after the trigger time.

--enabled/-z

Specifies that the duplication scan schedule be enabled when created. If you do not specify either `--enabled/-z` or `--disabled/-Z`, then the schedule is enabled when created by default.

--disabled/-Z

Specifies that the duplication scan schedule be disabled when created. If you specify this option, then you can later enable the backup schedule with a `chsched` command.

 **See Also:**

"[chsched](#) (page 2-58)"

--location/-L *locationname*

Specifies one or more locations to be applied to the duplication schedule. Only an [active location](#) can be specified in a duplication schedule. If no location is specified, then the schedule applies to all locations.

schedulename

Specifies the name of the schedule to create. Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Syntax 4

Use the following syntax to create a stagescan schedule.

The name of the scan job schedule can be added to a stage rule. If the stage rule is added to a disk pool device and staging is enabled, then the stagescan job launched by this schedule creates `copyfromstage` jobs for all backup image instances in the disk pool that match attributes of the stage rule.

You can create multiple stagescan schedules. However, it is best to create only a few because scanning all instances in a disk pool is a CPU-intensive operation.

```
mksched::=
```

```
mksched
[ --type/-Y stagescan ]
[ --comment/-c comment | --inputcomment/-i ]
[ --priority/-p schedule-priority ]
[ --enabled/-z | --disabled/-Z ]
[ [ --day/-d day-date ] [ --time/-t time ]
schedulename...
```

Semantics 4**--type/-Y *schedule-type***

Specifies the type of schedule to create. Valid values are `backup`, `duplicationscan`, `vaultingscan`, and `stagescan`.

When the schedule type is `stagescan` and no `--priority` value is specified, the priority is set to the `staging/defaultscanjobpriority` policy value.

--comment/-c *comment*

Adds a comment to the schedule.

--inputcomment/-i

Prompts for a comment. After you run `mksched`, `obtool` prompts you to enter the comment. End the comment with a period (.) on a line by itself.

--priority/-p *schedule-priority*

Assigns a schedule priority to a duplication scan. Refer to "[schedule-priority](#) (page 4-26)" for a description of the *schedule-priority* placeholder.

--day/-d *day-date*

Specifies the day on which Oracle Secure Backup triggers the scheduled duplication scan. If you do not specify a day or time, then Oracle Secure Backup does not run duplication scan jobs based on the schedule. If you specify a day but no time, then the time defaults to 00:00. Refer to "[day-date](#) (page 4-9)" for a description of the *day-date* placeholder.

--time/-t *time*

Specifies the time at which Oracle Secure Backup triggers the scheduled duplication scan. You cannot specify a time without a day. Refer to "[time](#) (page 4-29)" for a description of the *time* placeholder.

--enabled/-z

Specifies that the duplication scan schedule be enabled when created. If you do not specify either `--enabled/-z` or `--disabled/-Z`, then the schedule is enabled when created by default.

--disabled/-Z

Specifies that the duplication scan schedule be disabled when created. If you specify this option, then you can later enable the backup schedule with a `chsched` command.

**See Also:**

"[chsched](#) (page 2-58)"

schedulename

Specifies the name of the schedule to create. Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example**Example 3-22 Scheduling a Weekly Backup**

This example schedules a backup every Thursday at 9:00 p.m.

```
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:                backup
  Dataset:             OSB-CATALOG-DS
  Priority:             50
  Encryption:         no
  Comment:             catalog backup schedule
ob> mksched --priority 5 --dataset datadir.ds --day thursday --time 21:00 datadir
ob> lssched --long
OSB-CATALOG-SCHED:
  Type:                backup
  Dataset:             OSB-CATALOG-DS
  Priority:             50
  Encryption:         no
  Comment:             catalog backup schedule
```

```

datadir:
  Type:                backup
  Dataset:             datadir.ds
  Priority:             5
  Encryption:          no
  Trigger 1:
    Day/date:          thursdays
    At:                 21:00
    Backup level:       full
    Media family:       (null)
ob> lsjob --pending
Job ID      Sched time  Contents                               State
-----
3           10/06.21:00 dataset datadir.ds                     future work

```

3.1.12 mksnap

Purpose

Use the `mksnap` command to create a [snapshot](#). A snapshot is a consistent copy of a volume or a file system. Snapshots are supported only for a Network Appliance [filer](#) running Data ONTAP 6.4 or later.



See Also:

"[Snapshot Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `mksnap` command.

Syntax

```
mksnap::=
```

```

mksnap [ --host/-h hostname ] [ --fs/-f filesystem-name ]
[ --nowait/-n ] snapshot-name...

```

Semantics

--host/-h *hostname*

Specifies the name of a [Network Data Management Protocol \(NDMP\)](#) host. If you do not specify a host name, then Oracle Secure Backup uses the value from the [host](#) (page 5-3) variable.

--fs/-f *filesystem-name*

Specifies the name of an NDMP file system. If you do not specify the `--fs` option, then the `fs` variable must be set.

--nowait/-n

Does not wait for the snapshot operation to complete.

snapshot-name

Specifies the name to give the snapshot. Snapshot names must conform to the filename rules in effect where the snapshot is created.

Example**Example 3-23 Creating a Snapshot**

This example creates a snapshot of the file system `/vol/vol0` on the NDMP host named `lucy`.

```
ob> mksnap --host lucy --fs /vol/vol0 lucy_snap
ob> lssnap --long lucy_snap
File system /vol/vol0:
  Max snapshots:          255
  Reserved space:        44.8 GB
  % reserved space:      30
  Snapshot:              lucy_snap
  Of:                    /vol/vol0
  Taken at:              2013/03/28.20:52
  Used %:                0
  Total %:               0
  Busy:                  no
  Dependency:            no
```

3.1.13 mkssel

Purpose

Use the `mkssel` command to create a [database backup storage selector](#). Oracle Secure Backup uses the information encapsulated in storage selectors for a [backup job](#) when interacting with [Recovery Manager \(RMAN\)](#). You can modify the storage selector with the `chssel` (page 2-65) command.

See Also:

- ["Database Backup Storage Selector Commands \(page 1-14\)"](#) for related commands
- ["Database Backup Storage Selectors and RMAN Media Management Parameters \(page C-1\)"](#) for an explanation of how storage selectors interact with RMAN media management parameters
- *Oracle Secure Backup Administrator's Guide* for a conceptual explanation of storage selectors

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mkssel` command.

Syntax

```
mkssel::=
```

```

mkssel
{ --dbname/-d { * | dbname[,dbname]... } | --dbid/-i { * | dbid[,dbid]... } }
{ --host/-h { * | hostname[,hostname]... } }
{ --family/-f media-family }
[ --content/-c { * | content[,content]... } ]
[ --restrict/-r restriction[,restriction]... ]
[ --copynum/-n { * | 1 | 2 | 3 | 4 } ]
[ --encryption/-e {off|on|forcedoff|swencryption}]
[ --waittime/-w duration ] [--name/-N name-format]
[--priority/-p default | schedule-priority ]
sselname

```

Semantics

See "[chssel](#) (page 2-65)" for options that are not described in this section.

--dbname/-d *dbname*

Specifies the names of the databases to which this storage selector object applies. Specifying an asterisk (*) indicates that the storage selector applies to all database names. You cannot combine the asterisk character (*) with individual database names.

You must specify either `--dbname`, `--dbid`, or both. If you specify a database name but not a [database ID \(DBID\)](#), then the DBID defaults to all (*).

--dbid/-i *dbid*

Specifies the DBIDs of the databases to which this storage selector object applies. Specifying an asterisk (*) indicates that the storage selector applies to all DBIDs. You cannot combine the asterisk character (*) with individual DBIDs.

You must specify either `--dbname`, `--dbid`, or both. If you specify a DBID but not a database name, then the database name defaults to all (*).

--host/-h *hostname*

Specifies the names of the database hosts to which this storage selector applies. Specifying an asterisk character (*) indicates that the storage selector applies to all database hosts. You cannot combine the asterisk character (*) with individual hosts. You must specify at least one host name.

--family/-f *media-family*

Specifies the name of the [media family](#) to be used for backups under the control of this storage selector object. You can specify a media family that uses either a [content-managed expiration policy](#) or [time-managed expiration policy](#). You create media families with the [mkmf](#) (page 3-36) command.

--content/-c *content*

Specifies the backup contents to which this storage selector applies. Refer to "[content](#) (page 4-5)" for a description of the `content` placeholder. Specify an asterisk (*) to indicate all content types.

--restrict/-r *restriction*

Specifies the names of devices to which backups controlled by this storage selector are restricted. By default, Oracle Secure Backup uses device polling to find any available device for use in backup operations. Refer to "[restriction](#) (page 4-25)" for a description of the `restriction` placeholder.

--copynumber/-n * | 1 | 2 | 3 | 4

Specifies the copy number to which this storage selector applies. The copy number must be an integer in the range of 1 to 4. Specify an asterisk (*) to indicate that the storage selector applies to any copy number (default).

--waittime/-w *duration*

Specifies how long to wait for the availability of resources required by backups under the control of this storage selector. The default wait time is 1 hour. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

--name/-N *name-format*

Specifies the name assigned to the backup image created by this backup job. You can explicitly specify a name, specify one or more name format variables, or use a combination of name format variable and static values that you specify.

See "[name-format](#) (page 4-19)" for a description of the *name-format* placeholder.

sselname

Specifies the name of the database backup storage selector. Storage selector names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

--encryption/-e {off | on | forcedoff | swencryption}

Specifies whether backups should be encrypted. In all cases, if the data has been encrypted by RMAN, then Oracle Secure Backup performs no further encryption. Set one of the following options for encryption:

- **ON:** Oracle Secure Backup encrypts the backup data unless it has already been encrypted by RMAN.
- **OFF:** Oracle Secure Backup does not encrypt the backup data unless either the host or global policy is set to required. OFF is equivalent to specifying no value for encryption.
- **FORCEDOFF:** Oracle Secure Backup does not encrypt the database backup, overriding any host-specific encryption settings. The FORCEDOFF setting does not affect RMAN, which can still encrypt the backup data.
- **SWENCRYPTION:** Oracle Secure Backup uses software encryption instead of hardware encryption. This option is provided in case you do not want hardware encryption used in some situations.

 **Note:**

The `encryption` option is only available starting with Oracle Secure Backup 10.3.0.2.0.

—priority/-p *job priority*

Specifies a positive integer value that sets the priority for an RMAN backup or RMAN restore job. You can set the job priority value between 1 and 2147483647, with 1 being the highest priority. The default schedule-priority value is 100.

**See Also:**[About Setting the Job Priority for RMAN Operations](#) (page C-2)**Example****Example 3-24 Creating a Database Backup Storage Selector**

This example creates a storage selector named `ssel_full`. The storage selector applies to the database with a DBID of 1557185567 on host `brhost2`.

```
ob> mkssel --dbid 1557185567 --host brhost2 --content full --family f1 ssel_full
```

3.1.14 mkstage

Purpose

The `mkstage` command creates a stage rule.

Prerequisites

You must have the modify administrative domain's configuration right to use the `mkstage` command.

Syntax

`mkstage::=`

```
mkstage [--comment/-c comment]
        [--schedule/-T schedulename]
        [--matchfamily/-f media-family-name[,media-family-name]...]
        {[--dbname/-d { * | dbname[,dbname]...} |
        [--dbid/-i { * | dbid [,dbid]...} |
        [--fshost/-h { * | fshostname[,fshostname]...}]}
        [--mincopysize/-s size-spec]
        [--mincopyage/-a duration]
        {--targetfamily/-t target-media-family-name}
        [--restrict/-r restriction[,restriction]...]
        [--encryption/-e {yes | no | forcedoff}]
        [--algorithm/-L enc-algorithm]
        [--priority/-p {schedule-priority | default}]
        [--migrate/-m {yes | no}]
        stage-rule-name
```

Semantics**--comment/-c *comment***

Specifies a comment that is shown when using the long form of the `lsstage` command.

--schedule/-T *schedulename*

Specifies a stagescan schedule that specifies the time that a stagescan job will run. If the `--schedule` option is not set, then it defaults to the empty string (`""`). If a stage rule contains the empty string it matches all stagescan schedules; otherwise, the rule matches the named stagescan schedule. You can explicitly specify the empty string.

While an empty schedule specification does match all schedules during a scan, it does not cause the pool to be scanned for all schedules. A disk pool device is only scanned during the schedules referenced in the stage rules that were added to the disk pool device.

--matchfamily/-f *media-family-name*

Specifies the media families for backup instances that will be staged by this rule. If no match media family is specified, then this option defaults to an asterisk (*) so that all media families match the rule.

--dbname/-d *dbname*

Specifies one or more database names. A backup that has any of the specified database names matches this rule.

--dbid/-i *dbid*

Specifies one or more database identifiers. A backup that has any of the specified database identifiers matches this rule.

--fshost/-h *fshostname*

Specifies one or more Oracle Secure Backup client host names. A backup image instance for any file-system backup for any specified client host in the list of hosts matches this rule. An asterisk (*) matches all hosts. The default is the empty string so that no hosts match the stage rule.

--mincopysize/-s *size-spec*

The total size of all backup image instances that match the rule must be at least the minimum copy size or the staging job will not run. If the minimum copy size option is not specified or the size is set to 0, then this option is ignored. The minimum copy size defaults to the value 0.

--mincopyage/-a *duration*

Specifies the minimum age of a backup image instance before it is eligible to be copied. This option can be used separately or with the `-schedule` option. If the `--schedule` option is specified, then the copyfromstage job runs at the specified day and time. The minimum copy age value defaults to the value 0.

--targetfamily/-t *target-media-family-name*

Specifies the media family used with the target device when backup images that match this rule are staged. This option must be specified. If any media family specified using `--matchfamily` is time-managed, then the target media family must also be a time-managed media family.

--restrict/-r *restriction*

Restricts the copyfromstage job to specific devices within an administrative domain. You can select media server hosts or specific devices on these hosts. If you do not specify a restriction (default), then the current schedule has no device restrictions and can use any available device on the media server that hosts the disk pool, or if no tape device is available there, then on any media server. A restriction has the following form:

```
restriction ::= devicename | @hostname | devicename@hostname
```

 **See Also:**

- [restriction](#) (page 4-25)
for a description of the `restriction` placeholder

If the restriction list contains a disk pool device, then the rule cannot be added to the set of stage rules for that disk pool device. This prevents backup image instances from being copied back into the same disk pool stage device where the backup images already reside.

If there are any configured tape devices, then using an empty restriction list lets any tape device in the system become the target device for the copy, and a disk pool is never used. However, if there are no configured tape devices, then any disk pool can be chosen. Note that this can prevent the removal of the last configured tape device, because the empty restriction list could cause a stage loop by allowing an earlier source pool to become a potential target device for the copy.

The restriction list cannot contain both cloud devices and non-cloud devices. The default stage rule restriction list cannot be set to a cloud device.

--encryption/-e {yes | no} | forcedoff

Specifies encryption flags for the `copyfromstage` job. Valid values are:

- `yes`
Use encryption for the `copyfromstage` job. If the backup image instance is not encrypted, then the encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `no`
Do not use encryption for the `copyfromstage` job. This is the default. If the global backup policy or client backup policy is set to required, then those policies supersede this value and encryption is used. If encryption is used, then the encryption algorithm and keys used are determined by the current global and client policy settings that apply to each host.
- `forcedoff`
Do not use encryption for the `copyfromstage` job, regardless of global or client backup policy.

--algorithm/-L *enc-algorithm*

Specifies the encryption algorithm the `copyfromstage` jobs uses. Values include AES128, AES192, and AES256. The default algorithm is AES192.

--priority/-p *schedule-priority*

The scheduler priority value for the `copyfromstage` job. This is a value between 1 and 2147483647. A lower priority value designates a higher priority job.

If this option is not specified, then the `copyinstance/defaultpriority` policy value is used. That policy defaults to a priority value of 150. Using `--priority default` unsets any existing priority value so that the policy value is used (this is typically only used with the `chstage` (page 2-69) command).

--migrate/-m {yes | no}

The `yes` option causes all backup image instances that were successfully copied to the destination container by a `copyfromstage` job to be deleted from the source stage

device immediately after being copied. Even content-managed backup image instances are deleted.

RMAN content-managed backup image instances that are not migrated remain in the stage disk pool until RMAN deletes the database piece associated with the backup image instance.

If the migrate option is set to `yes`, then even a content managed backup image instance is deleted from the staging disk pool immediately after being stage-copied.

stage-rule-name

The name of the Oracle Secure Backup stage rule. A stage rule name must be no more than 31 characters long and must start with a letter. Other characters in the name come from the set of letters, decimal digits, and an underscore character. The name is case-sensitive. The name must be unique within the Oracle Secure Backup domain.

Examples

Example 3-25 Generating Stage Rules That Match RMAN Backup Images

This example generates a stage rule that matches any RMAN database backup image instance that was created with one of two specific media families. A `copyfromstage` job schedule runs every Monday at 4:00 PM. After the backup image instances are copied, they are immediately deleted from the stage disk pool device.

```
ob> mkstage --targetfamily tmf --matchfamily mymf1,mymf2 --dbname * --schedule
sscanmonat4pm --migrate yes mydbrule
```

Example 3-26 Generating Stage Rules That Match RMAN Backup Images of a Specified Age

This example generates a stage rule that matches the same rule options as in the previous example, but only copies backup image instances that are at least 10 days old at the specified schedule time.

```
ob> mkstage --targetfamily tmf --matchfamily mymf1,mymf2 --dbname * --schedule
sscanmonat4pm --mincopyage 10day --migrate yes mydbrule2
```

Example 3-27 Staging File-system Backups for Two Hosts

The following example causes file-system backup image instances with media family `mymf` for either host `sys1` or `sys2` to be staged. The instances are staged immediately because the schedule is an empty string (`""`), which is the default value when the schedule name is omitted. The time-managed backup image instances are deleted when they reach their expiration time.

```
ob> mkstage --targetfamily tmf --matchfamily mymf --fshosts sys1,sys2 myfsrule
```

Example 3-28 Staging File-system Backups for a Single Host That Are at Least 4TB Size Total

The following stage rule matches backup image instances with a media family of `mymf` and host `sys3`. If all of the backup image instances that match this rule have a cumulative size of at least 4TB, then the instances are copied.

```
ob> mkstage --targetfamily tmf --matchfamily mymf --fshosts sys3 --mincopysize 4TB
mysizerule1
```

Example 3-29 Copying Backup Image Instances With Any Media Family Containing Database Pieces

The following stage rule copies backup image instances with any media family that contain database pieces for the database with id 12345, and where the instances add up to a total size of at least 4TB. Either `dev1` or `dev2` will be the destination device.

```
ob> mkstage --targetfamily tmf --dbid 12345 --mincopysize 4TB --restrict dev1,dev2 --
schedule sscandaily mysizerule2
```

3.1.15 mksum

Purpose

Use the `mksum` command to create a [job summary schedule](#). The schedule indicates when and in what circumstances Oracle Secure Backup should generate a backup, restore, or duplication [job summary](#), which is a text file report that indicates whether the job was successful.

 **See Also:**

"[Summary Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `mksum` command.

Syntax

`mksum::=`

```
mksum [--days/-d produce-days[,produce-days]...]
      [--reporttime/-t time]
      [--mailto/-m email-target[,email-target]...]
      [--host/-h hostname[,hostname]...]
      [ [--covers/-c duration] |
        [--since/-s "summary-start-day [ time" ] ]
      [--backup/-B {yes | no}] [--restore/-R {yes | no}]
      [--orabackup/-b {yes | no}] [--orarestore/-e {yes | no}]
      [--scheduled/-S {yes | no}] [--user/-U {yes | no}]
      [--subjobs/-J {yes | no}] [--superseded/-D {yes | no}]
      [--duplication/-P {yes | no}] [--mediamovement/-M {yes | no}]
      [--catimport/-I {yes | no}] [--catalog/-C {yes | no}]
      [--copyinstance/-p {yes | no}] [--copyfromstage/-E {yes | no}]
      summary-name...
```

Semantics

--days/-d *produce-days*

Specifies the days of the week on which to generate a job summary. Refer to "[produce-days](#) (page 4-24)" for a description of the `produce-days` placeholder.

--reporttime/-t *time*

Specifies the time at which to generate a job summary. Refer to "[time](#) (page 4-29)" for a description of the *time* placeholder.

--mailto/-m *email-target[,email-target]...*

Specifies email addresses of users who receive job summaries. An email system must be operational on the [administrative server](#) for this feature to operate. Separate multiple entries with a comma.

--host/-h *hostname*

Generates reports only for the specified host.

--covers/-c *duration*

Specifies the time frame covered by the report. Refer to "[duration](#) (page 4-14)" for a description of the *duration* placeholder.

--since/-s "*summary-start-day time*"

Specifies the starting point of the time period that the report covers. Refer to "[summary-start-day](#) (page 4-28)" for a description of the *summary-start-day* placeholder. Refer to "[time](#) (page 4-29)" for a description of the *time* placeholder.

--backup/-B {*yes* | *no*}

Specifies whether backup jobs should be included in the report. The default is *yes*.

--restore/-R {*yes* | *no*}

Specifies whether restore jobs should be included in the report. The default is *yes*.

--orabackup/-b {*yes* | *no*}

Specifies whether [Recovery Manager \(RMAN\)](#) backup jobs should be included in the report. The default is *yes*.

--orarestore/-e {*yes* | *no*}

Specifies whether RMAN restore jobs should be included in the report. The default is *yes*.

--scheduled/-S {*yes* | *no*}

Specifies whether all jobs waiting to be processed in the [scheduler](#) should be included in the report. A scheduled job is a job that has yet to be run. The default is *yes*.

--user/-U {*yes* | *no*}

Specifies whether the report should include user-initiated jobs. The default is *yes*. If it is set to *no*, then the summary only shows scheduled jobs.

--subjobs/-J {*yes* | *no*}

Specifies whether the report should include subordinate jobs. The default is *yes*.

--superseded/-D {*yes* | *no*}

Specifies whether the report should include all jobs that have identical criteria. The default is *no*.

A job is superseded when an identical job was scheduled after the initial job had a chance to run. For example, suppose you schedule an [incremental backup](#) scheduled every night at 9 p.m. On Wednesday morning you discover that the Tuesday night backup did not run because no tapes were available in the [tape library](#). The incremental backup scheduled for Wednesday supersedes the backup from the previous night.

--duplication/-P {yes | no}

Specifies whether **volume** duplication jobs should be included in the report. The default is *yes*.

--catalog/-C {yes | no}

Specifies that the report should include information about **catalog** backups, including:

- The **volume ID** and **barcode** for each catalog backup
- The file number for the catalog backup
- Results of the verification step when the **backup job** was run

 **Note:**

Catalog backups are also listed in summary reports that include information on backup jobs. However, they are mixed in with other backups and not marked specifically as catalog backups. The `--catalog` option is intended to help monitor the status of catalog backups independently of other backup jobs.

--mediamovement/-M {yes | no}

Specifies whether to include media movement jobs in the report. The default is *yes*.

--copyinstance/-p {yes|no}

Specifies whether copy instance jobs must be included in the summary report. The default is *yes*.

--catimport/-I {yes | no}

Specifies whether catalog import jobs must be included in the summary report. The default is *yes*.

copyfromstage/-E {yes | no}

Controls whether `copyfromstage` jobs appear in the OSB summary report.

summary-name

Specifies the name of the job summary schedule. Names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 127 characters.

Examples**Example 3-30 Scheduling a Job Summary**

This example schedules a backup summary named `weekly_report`.

```
ob> mksum --days wed --reporttime 12:00 --mailto lance@example.com weekly_report
ob> lssum --long
weekly_report:
  Produce on:           Wed at 12:00
  Mail to:              lance@example.com
  In the report, include:
    Backup jobs:        no
    Restore jobs:       no
    Oracle backup jobs: no
    Oracle restore jobs: no
    Duplication jobs:   no
    Scheduled jobs:     yes
```

```

User jobs:           yes
Subordinate jobs:   yes
Superseded jobs:    no
Catalog backup jobs: yes
Media movement jobs: no
Catalog import jobs: no
Copy instance jobs: yes
Copy from stage jobs: yes

```

```
ob>
```

Example 3-31 Sample Job Summary

This example shows parts of a sample summary. Note that the sample output has been reformatted to fit on the page.

I. Pending jobs.

None.

II. Ready and running jobs.

None.

III. Successful jobs.

Job ID	Scheduled or *Introduced at	Completed at	Content	Backup Size	File Volume IDs # (Barcodes)
admin/1	*2013/03/24.09:52	2013/03/24.09:52	dataset tbrset/entire_backup		
admin/1.1	*2013/03/24.09:52	2013/03/24.09:52	host brhost2	3.5 MB	1 VOL000001 (ADE202)
admin/2	*2013/03/24.09:52	2013/03/24.09:52	restore to brhost2		

IV. Unsuccessful jobs.

Job ID	Scheduled or *Introduced at	Content	Status
admin/7	*2013/03/24.16:41	dataset homedir.ds	failed - host isn't administrative domain member (OB job mgr)
admin/7.1	*2013/03/24.16:41	host brhost4(DELETED)	failed - host isn't administrative domain member (OB job mgr)

3.1.16 mkuser

Purpose

Use the `mkuser` command to define an [Oracle Secure Backup user](#). Each Oracle Secure Backup user account belongs to exactly one [class](#), which defines the [rights](#) of the Oracle Secure Backup user.

See Also:

- "[User Commands](#) (page 1-22)" for related commands
- "[Class Commands](#) (page 1-13)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to run the `mkuser` command.

Usage Notes

When an Oracle Secure Backup user performs a [backup](#) (page 2-4) or [restore](#) (page 3-99) operation on a host with the default `--unprivileged` option, the host is accessed with an operating system identity.

If a Linux or UNIX host is backed up or restored, then Oracle Secure Backup uses the `--unixname` and `--unixgroup` values for the operating system identity.

If a Windows host is backed up or restored, then Oracle Secure Backup begins with the first domain triplet in the list—skipping any with a [wildcard](#) (*) for the domain name—and checks whether the domain and username allows access to the host.

Note:

Oracle Secure Backup uses the `LookupAccountName` system call to determine whether access is allowed. No attempt at logging on actually occurs during the check, nor is there any attempt to enumerate all the valid Windows domains.

If access is allowed, then Oracle Secure Backup uses this logon information to run the job. If access is not allowed, then Oracle Secure Backup proceeds to the next domain triplet in the list. If Oracle Secure Backup does not find a triplet that allows access to the host, then it checks whether a triplet exists with a wildcard (*) as domain name.

Syntax

`mkuser::=`

```
mkuser --class/-c userclass
[ --password/-p password | --querypassword/-q ]
[ --pwdlifetime ] [ --pwdgracetime ] [ --pwdreusetime ]
[ --unixname/-U unix-user ] [ --unixgroup/-G unix-group ]
[ --domain/-d { windows-domain | * },windows-account[,windows-password ] ]...
[ --ndmpuser/-N { yes | no } ]
[ --email/-e emailaddr ] [ --givenname/-g givenname ]
[ --preauth/-h preauth-spec[,preauth-spec]... ]
username
```

Semantics

--class/-c *userclass*

Specifies the name of the class to which the Oracle Secure Backup user should belong. [Table 8-1](#) (page 8-1) describes the predefined classes and rights.

--password/-p *password*

Specifies a password for the Oracle Secure Backup user when logging in to an [administrative domain](#). The maximum character length that you can enter is 16 characters. If you do not specify a password, then the password is null. Ensure that you enter the password enclosed in quotes.

The minimum password length is determined by the `minuserpasswordlen` security policy. Its default value is 0, which means a null password is permitted.



See Also:

"[minuserpasswordlen](#) (page 7-44)"

The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the Oracle Secure Backup user be prompted for the password.

--querypassword/-q

Specifies that you should be prompted for the password, which is not echoed.

--pwdlifetime

Specifies the lifetime of a user password, in number of days. This value must be greater than or equal to 1 day. The default lifetime of a password is set to 180 days. If the [password lifetime](#) is set to `disabled`, then the password never expires.

--pwdgracetime

Specifies the grace time of the password during which the user can continue using the current password even after it has expired. This value must be greater than or equal to 1 day. The default [password grace time](#) is set to 3 days. If the grace time is set to `disabled`, no grace time is provided and the user must change the password during the next login after the password expiration.

--pwdreusetime

Specifies the time period after which a user password that was previously used can be reused. This value must be greater than or equal to 1 day. The default [password reuse time](#) is set to 1 year. If the reuse time is set to `disabled`, the password can never be reused.

--unixname/-U *unix-user*

Specifies a user name for a Linux or UNIX host. The default user name is the first defined of `guest`, `nobody`, `none`, and `user`.

--unixgroup/-G *unix-group*

Specifies a group for a Linux or UNIX host. The default is `none`.

--domain/-d {*windows-domain* | *},*windows-account*[,*windows-password*]

Specifies a Windows domain name, user account, and password. If you do not enter the Windows password, then `obtool` prompts you for it. For *windows-domain*, enter an asterisk (*) if the *windows-account* and *windows-password* apply to all Windows domains. The `--domain` option has no default value.

Always enclose the Windows name, user account, and password string in quotes.

The Windows user account must have access to the following privileges so that `obtar` can run:

- `SeBackupPrivilege`
User right: Back up files and directories

- `SeRestorePrivilege`
User Right: Restore files and directories
- `SeChangeNotifyPrivilege`
User right: Bypass traverse checking

You must grant the preceding privileges to the user account when it is created or grant them afterward.

--ndmpuser/-N {yes | no}

Indicates whether the Oracle Secure Backup user is permitted to log in to an [Network Data Management Protocol \(NDMP\)](#) server. Specify `yes` to enable the Oracle Secure Backup user to access an NDMP server and `no` if you do not. The default is `no`. This login is achieved with an external client program.

--email/-e *emailaddr*

Specifies the email address for the Oracle Secure Backup user. When Oracle Secure Backup wants to communicate with this user, such as to deliver a [job summary](#) or notify the user of a pending input request, it sends email to this address.

--givenname/-g *givenname*

Specifies the given name of the Oracle Secure Backup user if different from the user name, for example, "Jim W. Smith" for user name `jsmith`.

--preauth/-h *preauth-spec*

Grants the specified operating system user preauthorized access to the administrative domain as the Oracle Secure Backup user. By default there is no [preauthorization](#). A preauthorization dictates how an operating system user can be automatically logged in to Oracle Secure Backup. Access is authorized only for the specified operating system user on the specified host. For each host within an Oracle Secure Backup administrative domain, you can declare one or more one-to-one mappings between operating system and Oracle Secure Backup user identities. For example, you can create a preauthorization so that UNIX user `bkpadmin` is automatically logged in to `obtool` as Oracle Secure Backup user `admin`.

Refer to "[preauth-spec](#) (page 4-23)" for a description of the `preauth-spec` placeholder. Duplicate preauthorizations are not permitted. Preauthorizations are considered to be duplicates if they have the same hostname, user ID, and domain.

username

Specifies a name for the Oracle Secure Backup user. User names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 127 characters.

The user name must be unique among all Oracle Secure Backup user names. Formally, it is unrelated to any other name used in your computing environment or the Oracle Secure Backup administrative domain.

Example**Example 3-32 Creating an Oracle Secure Backup User**

This example creates an administrative Oracle Secure Backup user named `janedoe`. This user runs [unprivileged backup](#) and restore operations on Linux and UNIX hosts under the `jdoh` operating system account. Because no Windows domains are specified, this user is not permitted to run backup or restore operations on Windows hosts. The `jdoh` operating system user is preauthorized to make [Recovery Manager \(RMAN\)](#) backups on host `osbsvr1`.

```

ob> lsuser
admin          admin
sbt           admin
tadmin        admin
ob> mkuser janedoe --class admin --password "x45y" --givenname "jane" --unixname
jdoe --unixgroup "dba" --preauth osbsvr1:jdoe+rman+cmdline --ndmpuser no
--email jane.doe@example.com
ob> lsuser
admin          admin
janedoe       admin
sbt           admin
tadmin        admin

```

Example 3-33 Creating an Oracle Backup User with Specific Password Settings

This example creates an administrative Oracle Secure Backup user `dave01` with the password being queried once the command is completed. The `-querypassword` clause strengthens user security as the password is not visible on the command line. The [password lifetime](#) is set to 80 days. Similarly, the [password grace time](#) is set to 2 days and the [password reuse time](#) is set to 120 days. The example also lists all the attributes of the user.

```

ob> mkuser dave01 --class admin --querypassword --pwdlifetime 80days --pwdgracetime
2days --pwdreusetime 120days --givenname "dave" --preauth brhost3:rman+cmdline --
ndmpuser no
Password:
Password (again):
ob> lsuser --long dave01
dave01:
  Password:                (set)
  Password last changed:   2012/10/30.02:33
  Password change required: no
  Password lifetime:       80 days
  Password grace time:     2 days
  Password reuse time:     120 days
  User class:              admin
  Given name:              dave
  UNIX name:               [none]
  UNIX group:              [none]
  Windows domain/acct:    [none]
  NDMP server user:       no
  Email address:          [none]
  UUID:                   7395a468-04dd-1030-93a4-00163e527899
  Preauthorized access:
    Hostname:              brhost3
    Username:              rman
    Windows domain:       [all]
    RMAN enabled:         no
    Cmdline enabled:      yes

```

Example 3-34 Creating an Oracle Secure Backup User with a Windows Domain

This example creates an administrative Oracle Secure Backup user named `winadmin` for a Windows domain. The Windows user account name for this user is `winuser1` and the Windows user password is `pwd`. The asterik (`*`) ensures that these Windows credentials apply to all Windows domains. This user can perform backup and restore operations on Windows hosts.

```

ob> mkuser winadmin --class admin --domain "*,\winuser1,pwd"
ob> lsuser --long winadmin

```

```

winadmin:
  Password: (not set)
  Password last changed: 2013/07/24.05:55
  Password change required: no
  Password lifetime: 180 days (system default)
  Password grace time: 3 days (system default)
  Password reuse time: 1 year (system default)
  User class: admin
  Given name: [none]
  UNIX name: [none]
  UNIX group: [none]
  Windows domain/acct: [all] winuser1
  NDMP server user: no
  Email address: [none]
  UUID: e4a96afa-d6c8-1030-9b32-00163e527899
  Preauthorized access: [none]

```

3.1.17 mountdev

Purpose

Use the `mountdev` command to mount a tape [volume](#) that was previously loaded into a [tape drive](#). When a volume is mounted in a tape drive, the Oracle Secure Backup [scheduler](#) is notified that the mounted volume is available for use. You can set the mode of use for the volume with the `mountdev` options.

You can use this command if the tape drive is not set to `automount`, which is the recommended, default setting. In special situations the `mountdev` and [unmountdev](#) (page 3-149) commands provide additional control over your tape drive.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `mountdev` command.

Syntax

```
mountdev :=
```

```

mountdev { --read/-r | --write/-w | --overwrite/-o }
[ --unmount/-u | --norewind/-R ] devicename ...

```

Semantics

--read/-r

Identifies the [mount mode](#) as read. In this mode, Oracle Secure Backup mounts the volume for reading only.

--write/-w

Identifies the mount mode as write. In this mode, Oracle Secure Backup mounts the volume so that it can append any backups to the end of the volume.

--overwrite/-o

Identifies the mount mode as overwrite. In this mode, Oracle Secure Backup mounts a volume on the device and positions it at the beginning of the tape so that the existing contents of the volume are overwritten. If you use this option, then you are granting permission to [overwrite](#) a volume even though its volume [expiration policy](#) might not deem it eligible to be overwritten. Specify this option only in situations that warrant or require overwriting unexpired volumes.

--unmount/-u

Unmounts the currently mounted tape before running the mount request. If a tape is mounted in the tape drive, and you do not first unmount the tape by specifying `--unmount`, then the `mountdev` command fails.

--norewind/-R

Specifies that the tape should not be rewound when Oracle Secure Backup finishes writing to it. This option enables Oracle Secure Backup to remain in position to write the next [backup image](#).

devicename

Specifies the device on which you want to mount a volume. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example**Example 3-35 Manually Mounting a Tape Volume**

This example manually unmounts a tape volume from tape drive `tape1`, which is automounted, and then manually mounts a tape in write mode. Note that the sample [lsdev](#) (page 2-133) output has been reformatted to fit on the page.

```
ob> lsdev --long tape1
tape1:
  Device type:          tape
  Model:                [none]
  Serial number:       [none]
  In service:          yes
  Library:             lib1
  DTE:                 1
  Automount:           yes
  Error rate:          8
  Position interval:   3145679KB (-1073791796 bytes) (from driver)
  Debug mode:          no
  Blocking factor:     (default)
  Max blocking factor: (default)
  Current tape:        1
  Use list:            all
  Drive usage:         14 seconds
  Cleaning required:   no
  UUID:                b7c3a1a8-74d0-1027-aac5-000cf1d9be50
  Attachment 1:
    Host:               brhost3
    Raw device:         /dev/obt0
ob> mountdev --unmount --write tape1
ob> lsdev --mount tape1
drive      tape1      in service      write      rbtar      VOL000003      ADE203
```

3.1.18 movevol

Purpose

Use the `movevol` command to move a [volume](#) from one element to another element within a [tape library](#). You can only move one volume at a time.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `movevol` command.

Syntax

```
movevol::=
```

```
movevol [ --library/-L libraryname | --drive/-D drivename ]
{ vol-spec | element-spec } element-spec
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library in which you want to move a volume. If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

--drive/-D *drivename*

Specifies the name of a [tape drive](#) in the tape library in which you want to move a volume.

If you do not specify `--library` or `--drive`, then Oracle Secure Backup uses the value of the [library](#) (page 5-3) or [drive](#) (page 5-1) variable. Oracle Secure Backup issues a warning if it can obtain neither the tape library nor tape drive setting.

vol-spec

Specifies the volume to be moved. Refer to "[vol-spec](#) (page 4-31)" for a description of the `vol-spec` placeholder.

element-spec

Specifies the number of a storage element, import/export location, or a tape drive. Refer to "[element-spec](#) (page 4-14)" for a description of the `element-spec` placeholder.

If you specify `vol-spec`, then `element-spec` represents the [location](#) to which the volume should be moved. If you specify `element-spec` twice, then the first represents the location from which the volume should be moved and the second represents the location to which the volume should be moved.

Example

Example 3-36 Moving a Volume

This example moves the volume in storage element 3 to the import/export element `iee3`. Note that the sample output has been reformatted to fit on the page.

```
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            vacant
  in  2:            volume VOL000001, barcode ADE201, oid 102, 48319392 kb remaining
  in  3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
                    remaining, content manages reuse
  in  4:            vacant
  in  iee1:         barcode ADE203, oid 114, 47725344 kb remaining, lastse 4
  in  iee2:         volume VOL000002, barcode ADE204, oid 110, 47670368 kb remaining, lastse 1
  in  iee3:         vacant
  in  dte:          vacant
ob> movevol --library lib1 3 iee3
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            vacant
  in  2:            volume VOL000001, barcode ADE201, oid 102, 48319392 kb remaining
  in  3:            vacant
  in  4:            vacant
  in  iee1:         barcode ADE203, oid 114, 47725344 kb remaining, lastse 4
  in  iee2:         volume VOL000002, barcode ADE204, oid 110, 47670368 kb remaining, lastse 1
  in  iee3:         volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
                    remaining, content manages reuse, lastse 3
  in  dte:          vacant
```

3.1.19 opendoor

Purpose

Use the `opendoor` command to open the import/export door of a [tape library](#). This command only works for libraries that support it.

The import/export door is a mechanism that an [operator](#) uses to transfer tapes into and out of the tape library. You can then run the [importvol](#) (page 2-102) command to move volumes to internal slots in the tape library and the [exportvol](#) (page 2-94) command to move volumes out of the tape library. Because the tape library itself is not opened during this process, a reinventory is not required.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `opendoor` command.

Syntax

```
opendoor::=
```

```
opendoor [ --library/-L libraryname ]
```

Semantics

--library/-L *libraryname*

Specifies the name of the tape library on which you want to open the import/export door. If you do not specify a tape library name, then the [library](#) (page 5-3) variable must be set.

Example

Example 3-37 Opening an Import/Export Door

This example opens the import/export door in tape library `lib1`.

```
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            vacant
  in  2:            volume VOL000001, barcode ADE201, oid 102, 48319392 kb remaining
  in  3:            vacant
  in  4:            vacant
  in  iee1:         barcode ADE203, oid 114, 47725344 kb remaining, lastse 4
  in  iee2:         volume VOL000002, barcode ADE204, oid 110, 47670368 kb remaining, lastse 1
  in  iee3:         volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
                    remaining, content manages reuse, lastse 3
  in  dte:          vacant
ob> opendoor --library lib1
```

3.1.20 pingdev

Purpose

Use the `pingdev` command to determine whether a device is accessible to Oracle Secure Backup with all configured attachments.

For each [attachment](#) defined for the device, Oracle Secure Backup performs the following steps:

1. Establishes a connection to the device
2. Queries the device's identity by using the [Small Computer System Interface \(SCSI\) inquiry](#) command
3. Closes the connection

For each attachment that is remote from the host running `obtool`, Oracle Secure Backup establishes a [Network Data Management Protocol \(NDMP\)](#) session with the remote [media server](#) to test the attachment. When the `pingdev` command is issued for a cloud storage device, the accessibility of Oracle Cloud services through all attached media servers is verified.

**See Also:**

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `pingdev` command.

Syntax

`pingdev::=`

```
pingdev [ --nohierarchy/-H ] [ --quiet/-q | --verbose/-v ]
[ --host/-h hostname ]... { --all/-a | devicename ... }
```

Semantics**--nohierarchy/-H**

Suppresses access to each [tape drive](#) contained in a [tape library](#). By default, `obtool` pings each tape drive contained in the tape library.

--quiet/-q

Suppresses output. By default, `obtool` displays the output shown in [Example 3-38](#) (page 3-74).

--verbose/-v

Displays verbose output as shown in the following sample output:

```
ob> pingdev --verbose lib1
Info: pinging library lib1.
Info: library    lib1          accessible.
Info: pinging drive tape1.
Info:  drive 1 tape1          accessible.
```

By default, `obtool` displays the output shown in [Example 3-38](#) (page 3-74).

--host/-h *hostname*

Specifies the name of the host computer whose attached devices you are pinging.

--all/-a

Pings all defined devices.

devicename

Specifies the name of the device to ping. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example**Example 3-38 Pinging a Tape Drive with Multiple Attachments**

This example pings the tape drive called `tape3`. The [tape device](#) has attachments to multiple hosts.

```
ob> pingdev tape3
Info: drive      tape3          via host osbsvr1 accessible.
Info: drive      tape3          via host brhost3 accessible.
```

```
ob> pingdev --host brhost3 tape3
Info: drive      tape3          via host brhost3 accessible.
```

3.1.21 pinghost

Purpose

Use the `pinghost` command to determine whether a host in an [administrative domain](#) is responsive to requests from Oracle Secure Backup. This operation is useful for ensuring that a host is responsive on all of its configured IP addresses.



See Also:

"[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `pinghost` command.

Usage Notes

This command attempts to establish a TCP connection to the host on each of the IP addresses that you have configured for it. For hosts that use the Oracle Secure Backup protocol, the command connects through TCP port 400; for hosts using [Network Data Management Protocol \(NDMP\)](#), it connects through the configured NDMP TCP port, usually 10000. Oracle Secure Backup reports the status of each connection attempt and immediately closes each connection that was established successfully.

Syntax

```
pinghost::=
```

```
pinghost [ --quiet/-q | --verbose/-v ] hostname...
```

Semantics

--quiet/-q

Suppresses output.

--verbose/-v

Displays output. This option is the default.

hostname

Specifies the name of the host computer to ping.

Example

Example 3-39 Pinging a Host

This example queries the hosts in the administrative domain and then pings host `brhost2`.

```
ob> lshost
brhost2          client                      (via OB)  in service
brhost3          mediaserver,client          (via OB)  in service
sfserver1       client                      (via OB)  in service
ndmphost1       client                      (via NDMP) in service
osbsvr1         admin,mediaserver,client    (via OB)  in service
ob> pinghost brhost2
brhost2 (address 192.0.2.1): Oracle Secure Backup and NDMP services are available
```

3.1.22 pwd

Purpose

Use the `pwd` command to display the name of the directory in the Oracle Secure Backup [catalog](#) that you are browsing.



See Also:

"[Browser Commands](#) (page 1-12)" for related commands

Prerequisites

The [rights](#) needed to use the `pwd` command depend on the [browse backup catalogs with this access](#) (page 8-3) setting for the [class](#).

Syntax

```
pwd::=
```

```
pwd [ --short/-s | --long/-l ] [ --noescape/-B ]
```

Semantics

--short/-s

Displays data in short form.

--long/-l

Displays data in long form.

--noescape/-B

Does not escape non-displayable characters in path name. Specify `--noescape` if you want path names that include an ampersand character (&) to display normally.

Example

Example 3-40 Displaying the Current Directory

This example displays the path information for `brhost2`.

```
ob> cd --host brhost2
ob> pwd --long
Browsemode:      catalog
Host:           brhost2
Data selector:   latest
Viewmode:       inclusive
Pathname:       <super-dir>
```

3.1.23 pwdds

Purpose

Use the `pwdds` command to show the name of the current directory in the [dataset directory](#) tree.



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `pwdds` command.

Syntax

```
pwdds::=
```

```
pwdds
```

Example

Example 3-41 Displaying the Current Directory

This example shows the current directory, changes into a different directory, and then shows the current directory again.

```
ob> pwdds
/ (top level dataset directory)
ob> lsds
Top level dataset directory:
mydatasets1/
mydatasets/
admin_domain.ds
ob> cdds mydatasets
ob> pwdds
/mydatasets
```

3.1.24 pwdp

Purpose

Use the `pwdp` command to display the identity of the current policy.

The policy data is represented as a directory tree with `/` as the root. You can use [cdp](#) (page 2-27) to navigate the tree and [lsp](#) (page 2-157) and `pwdp` to display data.

 **See Also:**

- "Policy Commands (page 1-18)" for related commands
- Defaults and Policies (page 7-1) for a complete list of policies and policy classes

Prerequisites

You must have the [display administrative domain's configuration](#) (page 8-4) right to use the `pwdp` command.

Syntax

```
pwdp::=
```

```
pwdp
```

Example**Example 3-42 Displaying the Current Directory in the Policy Tree**

This example uses `cdp` (page 2-27) to browse the policies and `pwdp` to display the current directory in the policy directory tree.

```
ob> pwdp
/
ob> lsp
daemons          daemon and service control policies
devices          device management policies
index            index catalog generation and management policies
local            Oracle Secure Backup configuration data for the local machine
logs            log and history management policies
media            general media management policies
naming           WINS host name resolution server identification
ndmp            NDMP Data Management Agent (DMA) defaults
operations       policies for backup, restore and related operations
scheduler       Oracle Secure Backup backup scheduler policies
security        security-related policies
testing         controls for Oracle Secure Backup's test and debug tools
ob> cdp daemons/auditlogins
ob> pwdp
/daemons/auditlogins
ob> lsp
auditlogins      no          [default]
ob> cdp ../..
ob> pwdp
/
ob> lsp
daemons          daemon and service control policies
devices          device management policies
index            index catalog generation and management policies
local            Oracle Secure Backup configuration data for the local machine
logs            log and history management policies
media            general media management policies
naming           WINS host name resolution server identification
ndmp            NDMP Data Management Agent (DMA) defaults
operations       policies for backup, restore and related operations
```

scheduler	Oracle Secure Backup backup scheduler policies
security	security-related policies
testing	controls for Oracle Secure Backup's test and debug tools

3.1.25 quit

Purpose

Use the `quit` command to exit `obtool`. This command is identical in functionality to the `exit` (page 2-93) command.



See Also:

"[Miscellaneous Commands](#) (page 1-18)" for related commands

Syntax

```
quit::=
```

```
quit [ --force/-f ]
```

Semantics

--force/-f

Exits `obtool` even if there are pending backup or restore requests. Specifying `--force` means that pending backup and restore requests are lost.

Normally, you cannot quit `obtool` when there are pending requests. You should submit pending requests to the [scheduler](#) by specifying `--go` on the [backup](#) (page 2-4) or [restore](#) (page 3-99) commands.

Example

Example 3-43 Quitting `obtool`

This example uses the `--force` option to quit `obtool` when a [backup job](#) is pending.

```
ob> backup --dataset fullbackup.ds
ob> quit
Error: one or more backup requests are pending. Use "quit --force" to
      quit now, or send the requests to the scheduler with "backup --go".
ob> quit --force
```

3.1.26 recallvol

Purpose

Recalls a tape [volume](#) from an offsite [storage location](#).



See Also:

"[Volume Rotation Commands](#) (page 1-22)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `recallvol` command.

Usage Notes

If you specify a volume ID that matches multiple volumes in the Oracle Secure Backup volumes catalog, then Oracle Secure Backup asks which volume or volumes you want to recall. You can select one or more of the volumes, all of them, or none of them. The default selection is all volumes.

If you specify a volume ID and the volume belongs to a volume set, then Oracle Secure Backup lists all volumes in the volume set. You can select all or none of them, but you cannot select individual members of the volume set. The default selection is `quit`, which means that no volumes are selected.



See Also:

"[chvol](#) (page 2-75)" for a pair of examples illustrating volume ID matching

Syntax

```
recallvol::=
```

```
recallvol
  [ --immediate/-I ]
  [ --piece/-p piecename | vol-spec ]
  [ --tolocation/-t locationname ]
```

Semantics

--immediate/-I

Creates a media movement job immediately.

--piece/-p *piecename*

Recall the volume or volumes containing the specified [backup piece](#). The `--piece` and `vol-spec` options are mutually exclusive.

vol-spec

The [volume ID](#) or the [barcode](#) value of the volume. The `--piece` and `vol-spec` options are mutually exclusive.

--tolocation/-t *locationname*

Specifies the [location](#) to which the volumes should be recalled. If the `--tolocation` option is not specified for the `recallvolume` command, then the volume are recalled to the [originating location](#).

3.1.27 releasevol

Purpose

Releases recalled volumes, for return to the [location](#) dictated by their rotation policies.

 **See Also:**

"[Volume Rotation Commands](#) (page 1-22)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `releasevolume` command.

Usage Notes

If you specify a volume ID that matches multiple volumes in the Oracle Secure Backup volumes catalog, then Oracle Secure Backup asks which volume or volumes you want to release. You can select one or more of the volumes, all of them, or none of them. The default selection is all volumes.

If you specify a volume ID and the volume belongs to a volume set, then Oracle Secure Backup lists all volumes in the volume set. You can select all or none of them, but you cannot select individual members of the volume set. The default selection is quit.

 **See Also:**

"[chvol](#) (page 2-75)" for a pair of examples illustrating volume ID matching

Syntax

```
releasevolume::=
releasevol
  { --all/-a | vol-spec }
```

Semantics**--all/-a**

Releases all volumes currently in the recalled state.

vol-spec

The [volume ID](#) or the [barcode](#) value of the [volume](#) to be released.

3.1.28 renbkup

Purpose

Use the `renbkup` command to modify the externally-visible name of a backup image. When you rename a backup image, Oracle Secure Backup renames the backup image instances associated with this backup image to reflect the changed name.

Prerequisites

You must have the [modify any backup, regardless of its owner](#) (page 8-5) or [modify any backups owned by user](#) (page 8-5) class right to use the `renbkup` command.

Syntax

renbkup::=

```
renbkup
[--nq] {old-backup-image-name new-backup-image-name}...
```

Semantics

--nq

Does not ask for confirmation before modifying the backup image name.

old-backup-image-name

Specifies the name of the existing backup image that needs to be modified.

new-backup-image-name

Specifies the new name for the backup image. If the name specified already exists, then the `renbkup` command fails.

Examples

Example 3-44 Renaming Backup Images

This example renames the backup image `my_bi_fs` to `new_bi_fs`. Notice that when you rename the backup image, the corresponding backup image instance name is also modified to match the new backup image name.

```
ob> lsbkup --long --instances my_bi_fs
Backup image name:  my_bi_fs
  Type:                file system
  Client:              brhost2
  Backup level:       0
  Size:               128.0 KB
  Backup owner:      admin
  Owner class:       admin
  Backup date and time: 2013/04/23.04:20
  Created by job:    admin/12.1
  UUID:              7123076c-8e70-1030-84cd-00163e359724
  Instance name:     my_bi_fs.1
    Container:        dp2
    Encryption:      off
    Created:         2013/04/23.04:20
    Expires:        2013/12/31.01:00
    Created by job:  admin/12.1
    UUID:           7123078a-8e70-1030-84cd-00163e359724
```

```
ob> renbkup --nq my_bi_fs new_bi_fs
```

```
ob> ob> lsbkup --long --instances new_bi_fs
Backup image name:  new_bi_fs
  Type:                file system
  Client:              brhost2
  Backup level:       0
  Size:               128.0 KB
  Backup owner:      admin
  Owner class:       admin
  Backup date and time: 2013/04/23.04:20
  Created by job:    admin/12.1
  UUID:              7123076c-8e70-1030-84cd-00163e359724
  Instance name:     new_bi_fs.1
```

```
Container:          dp2
Encryption:        off
Created:           2013/04/23.04:20
Expires:           2013/12/31.01:00
Created by job:    admin/12.1
UUID:              7123078a-8e70-1030-84cd-00163e359724
```

3.1.29 renclass

Purpose

Use the `renclass` command to rename an [Oracle Secure Backup user class](#).

See Also:

- ["Class Commands \(page 1-13\)"](#) for related commands
- [Classes and Rights \(page 8-1\)](#) for a descriptions of the default Oracle Secure Backup classes and [rights](#)

Prerequisites

You must have the [modify administrative domain's configuration \(page 8-4\)](#) right to use the `renclass` command.

Syntax

```
renclass ::=
renclass [ --nq ] { old-classname new-classname }...
```

Semantics

--nq

Does not display a confirmation message. Without this option, the command displays a confirmation message. ["obtool Interactive Mode \(page 1-3\)"](#) describes the confirmation message.

old-classname new-classname

Renames *old-classname* to *new-classname*. Class names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example

Example 3-45 Renaming a Class

This example renames class `backup_admin` to `bkup_admin`.

```
ob> renclass backup_admin bkup_admin
rename class backup_admin? (a, n, q, y, ?) [y]: a
ob> lsclass bkup_admin
bkup_admin
```

3.1.30 rendev

Purpose

Use the `rendev` command to rename a configured device.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rendev` command.

Syntax

```
rendev::=
```

```
rendev [ --nq ] { old-devicename new-devicename }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-devicename

Specifies the name of the existing device. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

new-devicename

Specifies the name for the device. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

If the device name specified already exists in the administrative domain, the command fails.

Example

Example 3-46 Renaming a Device

This example renames two tape devices.

```
ob> lsdev
library    lib1                in service
  drive 1  tape1                in service
library    lib2                in service
  drive 1  tape2                in service
ob> rendev tape1 t1 tape2 t2
rename device tape1? (a, n, q, y, ?) [y]: y
rename device tape2? (a, n, q, y, ?) [y]: y
ob> lsdev
library    lib1                in service
```

```
drive 1 t1          in service
library lib2       in service
drive 1 t2          in service
```

3.1.31 rends

Purpose

Use the `rends` command to rename a [dataset file](#) or [dataset directory](#). For example, the following command renames `old_file` to `new_file` and moves it from `old_dir` to `new_dir`:

```
ob> rends old_dir/old_file new_dir/new_file
```

The following command creates `new_file` in the current directory:

```
ob> rends old_dir/old_file new_file
```



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rends` command.

Syntax

```
rends::=
```

```
rends [ --nq ] { old-dataset-name new-dataset-name }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-dataset-name

Specifies the name of the existing dataset file or directory to rename. Refer to "[dataset-name](#) (page 4-8)" for a descriptions of the `dataset-name` placeholder.

new-dataset-name

Specifies a name for the dataset file or directory. Note that you can use `new-dataset-name` to specify a [dataset](#) path. Refer to "[dataset-name](#) (page 4-8)" for a descriptions of the `dataset-name` placeholder.

Example

Example 3-47 Renaming a Dataset

This example renames dataset `datadir.ds` in the top-level directory to `tbrset/ddir.ds`.

```

ob> lsds
Top level dataset directory:
tbrset/
datadir.ds
ob> rends --nq datadir.ds tbrset/mdir.ds
ob> cdds tbrset
ob> lsds
Dataset directory tbrset:
mdir.ds
entire_backup
tiny_backup

```

3.1.32 rendup

Purpose

Renames duplication policies.



See Also:

"[Volume Duplication Commands](#) (page 1-22)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rendup` command.

Syntax

`rendup` (page 3-86)::=

```

rendup [ --nq/--noquery ] { oldpolicyname newpolicyname }
[ oldpolicyname newpolicyname... ]

```

Semantics

--nq/--noquery

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

oldpolicyname newpolicyname

For each pair of duplication policy names, the policy with the first name in the pair is renamed to the second name in the pair

Example

Example 3-48 Renaming a Volume Duplication Policy

This example renames the `voldup1` duplication policy to `voldup`.

```

ob> lsdup --long voldup1
voldup1:
  Migrate:                no
  Trigger:                lastwrite : forever
  Rule 1:                 RMAN-DEFAULT : 3

```

```

        UUID:                db4bfd64-18af-1031-b040-00163e527899
ob> rendup --nq voldup1 voldup
ob> lsdup
voldup

```

3.1.33 renhost

Purpose

Use the `renhost` command to rename a configured Oracle Secure Backup host.

See Also:

"[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renhost` command.

Syntax

```

renhost::=
renhost [ --nq ] [ --nocomm/-N ] { old-hostname new-hostname }...

```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--nocomm/-N

Suppresses communication with the host computer. Use this option to rename a computer that is not connected to the network.

old-hostname

Specifies the name of the existing host to rename.

new-hostname

Specifies the name for the host. Host names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example

Example 3-49 Renaming a Host

[Example 3-49](#) (page 3-87) displays configured hosts and then renames `ndmhost1` to `ndmhost`.

```

ob> lshost
brhost2          client                (via OB)   in service
brhost3          mediaserver,client    (via OB)   in service

```

```

sfsver1      client                (via OB)  in service
ndmhost1    client                (via NDMP) in service
osbsvr1     admin,mediaserver,client (via OB)  in service
ob> renhost --nq ndmhost1 ndmhost
ob> lshost
brhost2     client                (via OB)  in service
brhost3     mediaserver,client    (via OB)  in service
sfsver1     client                (via OB)  in service
ndmhost     client                (via NDMP) in service
osbsvr1     admin,mediaserver,client (via OB)  in service

```

3.1.34 renloc

Purpose

Renames a [storage location](#).



See Also:

"[Location Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renloc` command.

Syntax

`renloc` (page 3-88)::=

```
renloc [ --nq ] oldlocationname newlocationname
[ oldlocationname newlocationname... ]
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

oldlocationname newlocationname

For each pair of location name arguments, the [location](#) with the first name in the pair is renamed to the second name in the pair.

3.1.35 renmf

Purpose

Use the `renmf` command to rename a [media family](#).

 **See Also:**

"[Media Family Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renmf` command.

Syntax

```
renmf::=
```

```
renmf [ --nq ] { old-media-family-name new-media-family-name }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-media-family-name

Specifies the name of the existing media family. Note that you cannot rename the `RMAN-DEFAULT` media family.

new-media-family-name

Specifies the name for the media family. Media family names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 31 characters.

Example

Example 3-50 Renaming a Media Family

This example renames media family `full_bkup` to `full_backup`.

```
ob> lsmf
RMAN-DEFAULT                content manages reuse
content-man-family write forever    content manages reuse
full_bkup      write 7 days        content manages reuse
time-man-family write 7 days        keep 28 days
ob> renmf full_bkup full_backup
rename media family full_bkup? (a, n, q, y, ?) [y]: y
ob> lsmf
RMAN-DEFAULT                content manages reuse
content-man-family write forever    content manages reuse
full_backup      write 7 days        content manages reuse
time-man-family  write 7 days        keep 28 days
```

3.1.36 renrot

Purpose

Renames rotation policies.

**See Also:**

"[Rotation Policy Commands](#) (page 1-20)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renrot` command.

Syntax

`renrot` (page 3-89)::=

```
renrot [ -nq ] oldpolicyname newpolicyname
[ oldpolicyname newpolicyname... ]
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

oldpolicyname newpolicyname

For each pair of policy names, the policy with the first name in the pair is renamed to the second name in the pair. Oracle Secure Backup [rotation policy](#) names must be 1-31 characters.

3.1.37 rensched

Purpose

Use the `rensched` command to rename a schedule. Run the [lssched](#) (page 2-167) command to display schedule names.

**See Also:**

"[Schedule Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rensched` command.

Syntax

`rensched`::=

```
rensched [ --nq ] { old-schedulename new-schedulename }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

old-schedulename

Specifies the name of an existing schedule.

new-schedulename

Specifies a name for the *old-schedulename* schedule. Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Example

Example 3-51 Renaming a Backup Schedule

[Example 3-51 \(page 3-91\)](#) renames schedule `full_backup` to `weekday_sunday_backup`.

```

ob> lssched
full_backup          sundays, weekdays          fullbackup.ds
ob> rensched --nq full_backup weekday_sunday_backup
ob> lssched
weekday_sunday_backup sundays, weekdays          fullbackup.ds

```

3.1.38 rensnap

Purpose

Use the `rensnap` command to rename a [snapshot](#).



See Also:

"[Snapshot Commands \(page 1-21\)](#)" for related commands

Prerequisites

You must have the right to [manage devices and change device state \(page 8-5\)](#) to use the `rensnap` command.

Syntax

`rensnap::=`

```

rensnap [ --nq ] [ --host/-h hostname ] [ --fs/-f filesystem-name ]
{ old-snapshot-name new-snapshot-name }...

```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--host/-h *hostname*

Specifies the name of the [Network Data Management Protocol \(NDMP\)](#) host computer where you want to rename the snapshot. If you do not specify a host name, then Oracle Secure Backup uses the value from the [host](#) (page 5-3) variable.

--fs/-f *filesystem-name*

Specifies the name of the file system included in the snapshot. If you do not specify the `--fs` option, then the `fs` variable must be set.

old-snapshot-name

Specifies the name of an existing snapshot.

new-snapshot-name

Specifies a name for *old-snapshot-name*.

Example

Example 3-52 Renaming a Snapshot

This example renames snapshot `lucy_snap` to `lucy.0`.

```
ob> lssnap --long lucy_snap
File system /vol/vol0:
  Max snapshots:          255
  Reserved space:         44.8 GB
  % reserved space:       30
  Snapshot:               lucy_snap
  Of:                     /vol/vol0
  Taken at:               2013/03/28.20:52
  Used %:                 0
  Total %:                0
  Busy:                   no
  Dependency:             no
ob> rensnap --nq --host lucy --fs /vol/vol0 lucy_snap lucy.0
ob> lssnap
File system /vol/vol0:
Snapshot Of              Taken at      %Used  %Total Snapshot Name
/vol/vol0                2013/03/28.21:00    0      0    hourly.0
/vol/vol0                2013/03/28.20:52    0      0    lucy.0
/vol/vol0                2013/03/28.17:00    0      0    hourly.1
/vol/vol0                2013/03/28.13:00    0      0    hourly.2
/vol/vol0                2013/03/28.05:00    0      0    nightly.0
/vol/vol0                2013/03/28.01:00    0      0    hourly.3
/vol/vol0                2013/03/27.21:00    0      0    hourly.4
/vol/vol0                2013/03/27.17:00    0      0    hourly.5
/vol/vol0                2013/03/27.05:00    0      0    nightly.1
/vol/vol0                2012/08/21.11:30   22     7    myhost_snap
```

3.1.39 renssel

Purpose

Use the `renssel` command to rename a [database backup storage selector](#).

See Also:

"[Database Backup Storage Selector Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renssel` command.

Syntax

```
renssel::=
```

```
renssel [ --nq ] { old-sselname new-sselname }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-sselname

Specifies the name of the existing database backup storage selector.

new-sselname

Specifies the name of a database backup storage selector.

Example

Example 3-53 Renaming a Database Backup Storage Selector

This example uses the [mkssel](#) (page 3-54) command to create a storage selector and specifies the content as full. The example uses the [chssel](#) (page 2-65) command to add archived logs to the content of the selector, then renames the selector from `ssel_full` to `ssel_full_arch`.

```
ob> mkssel --dbid 1557615826 --host brhost2 --content full --family f1 ssel_full
ob> chssel --addcontent archivelog ssel_full
ob> renssel ssel_full ssel_full_arch
rename ssel ssel_full? (a, n, q, y, ?) [y]: y
ob> lsssel --short
ssel_full_arch
```

3.1.40 renstage

Purpose

The `renstage` command renames one or more stage rules.

Prerequisites

Syntax

```
renstage::=
```

```
renstage [--nq] { old-stage-rule-name new-stage-rule-name } ...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-stage-rule-name

Specifies the name of an existing stage rule.

new-stage-rule-name

Specifies the new name for the stage rule. The name is case-sensitive and must be no more than 31 characters long and must start with a letter. The name must be unique within the Oracle Secure Backup domain.

Example

Example 3-54 Renaming a Stage Rule

```
ob> renstage --nq stageruleabc stagerulexyz
```

3.1.41 rensun

Purpose

Use the `rensun` command to rename a [job summary schedule](#).



See Also:

"[Summary Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rensun` command.

Syntax

```
rensun::=
```

```
rensum [ --nq ] { old-summary-name new-summary-name }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

old-summary-name

Specifies the name of an existing job summary schedule.

new-summary-name

Specifies the name of the job summary schedule. Names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 127 characters.

Example

Example 3-55 Renaming a Job Summary Schedule

This example renames schedule `weekly_report` to `wed_report`.

```
ob> lssum
weekly_report          Wed at 12:00
ob> rensum --nq weekly_report wed_report
ob> lssum
wed_report            Wed at 12:00
```

3.1.42 renuser

Purpose

Use the `renuser` command to rename an [Oracle Secure Backup user](#).



See Also:

"[User Commands](#) (page 1-22)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `renuser` command.

Syntax

```
renuser::=
```

```
renuser [ --nq ] { old-username new-username }...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

old-username

Specifies the current Oracle Secure Backup user name.

new-username

Specifies the name for the Oracle Secure Backup user. User names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain at most 127 characters.

Example

Example 3-56 Renaming an Oracle Secure Backup User

This example renames Oracle Secure Backup user `bkpadmin` to `backup_admin`.

```
ob> renuser --nq bkpadmin backup_admin
```

3.1.43 resdev

Purpose

Use the `resdev` command to reserve a [tape device](#) for your exclusive use. While you hold the reservation, no Oracle Secure Backup component accesses the device.



See Also:

"[Device Commands \(page 1-15\)](#)" for related commands

Prerequisites

You must have the right to [manage devices and change device state \(page 8-5\)](#) to use the `resdev` command.

Usage Notes

During normal operations, Oracle Secure Backup temporarily assigns exclusive use of shared resources to its processes and jobs. It assigns this use through a built-in resource reservation system managed by the service [daemons](#) on the [administrative server](#).

You might encounter situations in which you want exclusive and explicit use of a device. When such situations arise, you can direct Oracle Secure Backup to reserve a device for your use and, when you are finished, to release that reservation with the [unresdev \(page 3-150\)](#) command. While you hold the reservation, no Oracle Secure Backup component can access the device.

The `resdev` command fails with an error if you try to reserve a device that is reserved. The command also fails if you attempt to select a [tape drive](#) in a [tape library](#) but all devices are reserved or no tape drives are configured.

Syntax

```
resdev::=
```

```
resdev [ --nowarn/-W ] { --in/-i libraryname ... | devicename ... }
```

Semantics

--nowarn/-W

Does not warn about devices that are out of service.

--in/-i libraryname

Finds and reserves any reservable tape drive in the specified libraries.

devicename

Specifies either the name of a tape drive or a tape library to be reserved. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example

Example 3-57 Reserving a Device

This example reserves all tape drives in tape library `lib1`. In this example, `lib1` contains a single tape drive. The example shows the warnings that result from attempting to reserve a reserved tape drive.

```
ob> lsdev
library   lib1           in service
  drive 1  tapel        in service
library   lib2           in service
  drive 1  tape2        in service
ob> lsdev --reserved
ob> resdev --in lib1
Drive tapel reserved.
ob> resdev --in lib1
Error: no drive is available in library lib1.
ob> resdev tapel
Error: you already have drive tapel reserved.
```

3.1.44 resetp

Purpose

Use the `resetp` command to reset the value of a one or more policies to the default value.

The policy data is represented as a directory tree with `/` as the root. You can use [cdp](#) (page 2-27) to navigate the tree and [lsp](#) (page 2-157) and [pwd](#) (page 3-76) to display data.

 **See Also:**

- ["Policy Commands \(page 1-18\)"](#) for related commands
- [Defaults and Policies \(page 7-1\)](#) for a complete list of policies and policy classes

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `resetp` command.

Syntax

```
resetp::=
```

```
resetp [ --nq ] policy-name...
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

policy-name

Specifies the name of a policy or a class of policies.

Example**Example 3-58 Resetting Policies to Their Default Values**

This example resets the policies in the `logs` class to their defaults.

```
ob> lsp logs
adminlogevents          all
adminlogfile            /tmp/logs/adminevents.log
clientlogevents        (none)                  [default]
jobretaintime          60 days
logretaintime          14 days
transcriptretaintime   14 days
unixclientlogfile      (none)                  [default]
windowsclientlogfile   (none)                  [default]
ob> resetp logs
Really reset ALL logs policies [no]? y
ob>
```

Example 3-59 Resetting Password Policies to Their Default Values

This example resets all policies in the `security` class to their defaults.

```
ob> lsp security
autocertissue           yes                      [default]
certkeysize            1024                    [default]
certlifetime           3 years
certwarning            7 days
encryptdataintransit   no                       [default]
loginduration           forever
```

```

minuserpasswordlen          0
passwordgracetime           10 days
passwordlifetime            30 days
passwordreusetime          180 days
securecomms                 yes [default]
trustedhosts                yes [default]
webinactivitytimeout        15 minutes [default]
websessiontimeout           24 hours [default]
ob> resetp security
Really reset ALL security policies [no]? y
ob> lsp security
autocertissue               yes [default]
certkeysize                 1024 [default]
certlifetime                10 years [default]
certwarning                 14 days [default]
encryptdataintransit        no [default]
loginduration               15 minutes [default]
minuserpasswordlen          8 [default]
passwordgracetime           3 days [default]
passwordlifetime            180 days [default]
passwordreusetime           1 year [default]
securecomms                 yes [default]
trustedhosts                yes [default]
webinactivitytimeout        15 minutes [default]
websessiontimeout           24 hours [default]

```

3.1.45 restore

Purpose

Use the `restore` command to create a file-system restore request. File-system restore operations are distinct from database restore operations, which are initiated by [Recovery Manager \(RMAN\)](#).

You can use the `restore` command to perform catalog-based or raw restore operations. In a catalog-based restore, you browse the [catalog](#) for the objects to be restored. When you have located their names and selected the instances, you can restore the objects. In a raw restore, you must have independent knowledge of the secondary storage location ([volume ID](#) and [backup image file](#) number) of a backup. You can either restore all data in the backup or specify an individual file or directory.

A restore request is held locally in `obtool` until you run the `restore` command with the `--go`, `--gocatalog`, or `--goraw` option, at which time Oracle Secure Backup converts all restore requests into jobs and sends them to the Oracle Secure Backup [scheduler](#).



See Also:

"[Restore Commands](#) (page 1-19)" for related commands

Prerequisites

If you have specified that the restore run in privileged mode, or if you are restoring files to a host accessed through [Network Data Management Protocol \(NDMP\)](#), then you must have the right to [perform file system restores as privileged user](#) (page 8-6) to

use the `restore` command. Otherwise, you must have the right to [perform file system restores as self](#) (page 8-7).

Usage Notes

`obtool` uses the [host](#) (page 5-3) variable to determine the name of the host whose backups are being restored. The default value for `host` is the name of the host on which `obtool` is running. You can set the `host` variable with the [set](#) (page 3-140) or [cd](#) (page 2-25) command.

If you specify a volume ID that matches multiple volumes in the Oracle Secure Backup volumes catalog, then Oracle Secure Backup asks which volume or volumes you want to recall. You can select one or more of the volumes, all of them, or none of them. The default selection is all volumes.

If you specify a volume ID and the volume belongs to a volume set, then Oracle Secure Backup lists all volumes in the volume set. You can select all or none of them, but you cannot select individual members of the volume set. The default selection is quit.

You can use [Oracle Secure Backup wildcard pattern matching](#) while performing the restore operation.



See Also:

["chvol \(page 2-75\)"](#) for a pair of examples illustrating volume ID matching



See Also:

[find \(page 2-97\)](#) for a description on wildcard characters and pattern matching.

Syntax 1

Use the following syntax to restore data by browsing the Oracle Secure Backup catalog.

`restore::=`

```
restore
[ --tohost/-h hostname ]
[ --device/-d drivename ]
[ --privileged/-g | --unprivileged/-G ]
[ --replaceexisting/-e | --keepexisting/-E ]
[ --replaceinuse/-u | --keepinuse/-U ]
[ --incremental/-i ]
[ --noposition/-X ]
[ --priority/-p schedule-priority ]
[ --select/-s data-selector[,data-selector]... ]
[ --passphrase/-P string | --querypassphrase/-Q ]
[ --algorithm/-l enc_algorithm ]
[ --ignoremismatch/-w ]
[ --obtaropt/-o obtar-option ]... [--waitfor/-W <duration>]
[[ --recall/-r ] [--immediate/-I] | [--preview /-y] | --go | --gocatalog | --
```

```
goraw ]  
pathname [ --aspath/-a pathname ] ...
```

Semantics 1

--tohost/-h hostname

Specifies the name of the host computer to which you want to restore data.

--device/-d drivename

Specifies a [tape drive](#) used to perform the restore operation. The tape drive name must be a valid device name. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

--privileged/-g

Specifies that the restore operation should run in privileged mode.

On UNIX systems, a privileged restore job runs under the `root` user identity. On Windows systems, the job runs under the same account identity as the Oracle Secure Backup service on the Windows [client](#).

--unprivileged/-G

Specifies that the restore operation should run in unprivileged mode (default).

An unprivileged restore job runs under the UNIX user or Windows account identity specified in the [mkuser](#) (page 3-64) command. Access to file-system data is constrained by the rights of the UNIX user or Windows account having this identity.

--replaceexisting/-e

Overwrites existing files (default).

--keepexisting/-E

Does not [overwrite](#) existing files.

--replaceinuse/-u

Replaces in-use files with those from the backup image instance. Windows deletes each in-use file when the last user closes it. This option is available on Windows only.

--keepinuse/-U

Leaves in-use files unchanged (default). This option is available on Windows only.

--incremental/-i

Directs [Network Attached Storage \(NAS\)](#) data servers to apply incremental restore rules. This option applies only to NAS data servers that implement this feature. This option does not apply to a [file-system backup](#) created with [obtar](#).

Normally, restore operations are additive: each file and directory restored from a full or an [incremental backup](#) is added to its destination directory. If files have been added to a directory since the most recent Oracle Secure Backup backup, then a restore operation does not remove the newly added files.

When you specify `--incremental`, NAS data servers restore each directory to its state during the last incremental backup. Files that were deleted before the last incremental backup are deleted by the NAS [data service](#) when restoring this incremental backup. For example, assume you make an incremental backup of `/home`, which contains `file1` and `file2`. You delete `file1` and make another incremental backup of `/home`. After a normal restore of `/home`, the directory would contain `file1` and `file2`; after an NDMP incremental restore of `/home`, the directory would contain only `file2`.

--noposition/-X

Indicates that Oracle Secure Backup should not use available position data to speed the restore operation. You might use this option if position data is corrupted.

--priority/-p *schedule-priority*

A *schedule-priority* you assign to a restore.

See "[schedule-priority](#) (page 4-26)" for more information on the *schedule-priority* placeholder.

--select/-s *data-selector*

Filters data based on the specified *data-selector*.

See "[data-selector](#) (page 4-6)" for more information on the *data-selector* placeholder.

--passphrase/-p

Specifies a passphrase-generated decryption key for the entire backup [volume set](#) to be restored.

--querypassphrase/-Q

Queries the [operator](#) for a passphrase to use in generating decryption keys for the entire backup volume set to be restored.

--algorithm/-l

Specifies the backup algorithm to use for decryption during restore. Required if `--passphrase` is used.

--ignoremismatch/-w

Causes mismatches of the encryption algorithm or passphrase as supplied by the `--algorithm` or `--passphrase` options to be treated as warnings instead of failures. This option is targeted at the situation where the header on the tape has been corrupted, but you still want to recover as much of the encrypted data as possible.

Mismatched encryption parameters are processed at different times depending on the restore type. For a *raw* restore the mismatch is caught and handled after the job is created, the tape is loaded, and the header is read off the tape. The job transcript for the raw restore reflects the encryption parameter mismatch. For a *catalog-based* restore, however, the mismatch is caught immediately and the job is never created.

**Note:**

The risk with restoring data using the incorrect `--algorithm` or `--passphrase` is that the restored data will be garbled on the disk.

--obtaropt/-o *obtar-option*

Specifies *obtar* options. For example `-j` enables debug mode and provides more details in the restore transcript.

See "[obtar Options](#) (page B-14)" for more information on *obtar* options.

--waitfor/-W *duration*

Specifies the amount of time that Oracle Secure Backup waits for the restore job to complete. After the specified time duration is exceeded, Oracle Secure Backup exits from *obtool*.

See [duration](#) (page 4-14) for more information on the *duration* placeholder.

--preview/-y

Lists the volumes needed for a restore and gets their status as either `onsite` or `offsite`. An `onsite` status means that the volume is in a library or drive. An `offsite` status means that the volume is in a storage location and must be recalled. This option is available only for catalog restore operations. It is not supported for raw restore operations.

--recall/-r

Starts recalls for any volumes needed by a restore if the volumes are `offsite`. This option is available only for catalog restore operations. It is not supported for raw restore operations.

--go

Releases all queued restore requests to the Oracle Secure Backup scheduler.

--gocatalog

Releases queued restore requests from a backup catalog to the Oracle Secure Backup scheduler.

--goraw

Releases queued raw restore requests to the Oracle Secure Backup scheduler. A raw restore request does not use backup catalog data.

pathname

Specifies the path name obtained by browsing the backup catalog for files that you backed up. If you do not specify `--aspath`, then Oracle Secure Backup restores the backup to the same path. If *pathname* does not exist on the host to which you are restoring, then Oracle Secure Backup creates it.

For example, assume that you browse the backup catalog for `brhost2` and locate the `/home` directory, which you want to restore. The `restore /home` command restores the backup to the `/home` directory on `brhost2`.

`--aspath/-a pathname`

Specifies an alternative path name where Oracle Secure Backup can restore the files. For example, to restore a backup of `/home` to `/tmp/home`, specify `restore /home --aspath /tmp/home`.

Note that if *pathname* does not exist on the host to which you are restoring, then Oracle Secure Backup creates it.

Syntax 2

Use the following syntax for raw restore operations.

`restore::=`

```
restore --raw/-R [ --tohost/-h hostname ] [ --device/-d drivename ]
[ --privileged/-g | --unprivileged/-G ]
{ --filenumber/-F filename }
{ --vid/-v vid[,vid]... } [ --tag/-t tag[,tag]... ]
[ --replaceexisting/-e | --keepexisting/-E ]
[ --replaceinuse/-u | --keepinuse/-U ] [ --incremental/-i ]
[ --priority/-p schedule-priority ]
[ {--passphrase/-P <passphrase>} | --querypassphrase/-Q ]
[--algorithm/-l <enc-algorithm>] [--ignoremismatch/-w]
[ --obtaropt/-o obtar-option ]... [--waitfor/-W <duration>]
[ --go | --gocatalog | --goraw ]
{ --all/-A pathname | { [ --aspath/-a pathname ] [ --position/-x position ] ... } }
```

Semantics 2

This section describes additional options used in Syntax 2. Options that are also used with Syntax 1 are not described in this section.

--raw/-R

Specifies a raw restore operation, which is a restore operation that does not use an Oracle Secure Backup catalog. You must specify the identity (volume ID or [barcode](#)) of the tape volumes to which the file-system objects were backed up and the backup image instance file number in which they are stored.

--filenumber/-F *filenumber*

Specifies the file number on the tape where the backup is located. Refer to "[filenumber](#) (page 4-16)" for a description of the *filenumber* placeholder.

--vid/-v *vid*

Selects backups based on volume ID. Refer to "[vid](#) (page 4-30)" for a description of the *vid* placeholder.

--tag *tag*

Selects backups based on the [volume tag](#) (barcode).

--all/-A

Restores all data in the backup.

pathname

Specifies the absolute path name of the file or directory that you backed up. If you do not know the absolute path names for the files when they were backed up, then you can use `obtar -tvf` to find them or restore an entire backup image instance. If you do not specify `--aspath`, then Oracle Secure Backup restores the backup to the same path.

Oracle Secure Backup does not support the use of wildcard characters in restore path names. The following wildcard characters are supported for backup include paths: `*`, `?`, `[`, and `]`. If you have path names to restore that include any of these wildcard characters, then no special escaping is required for the `restore` command.

Note that if *pathname* does not exist on the host to which you are restoring, then Oracle Secure Backup creates it.

--aspath/-a *pathname*

Specifies an alternative path name where Oracle Secure Backup can restore the files. For example, to restore a backup of `/private/bkpadm` to `/tmp/private/bkpadm`, specify the following:

```
restore /private/bkpadm --aspath /tmp/private/bkpadm
```

Note that if *pathname* does not exist on the host to which you are restoring, then Oracle Secure Backup creates it.

--position/-x *position*

Specifies the position of the data on the tape.

Examples

Example 3-60 Performing a Raw Restore Operation Based on the Oracle Secure Backup Catalog

This example displays the latest backup image instance of the `/home/data` directory stored in the Oracle Secure Backup catalog. The `restore` command submits the request to the scheduler with priority 1. Oracle Secure Backup runs the job and restores the data.

```
ob> set host brhost2
ob> cd /home/data
ob> ls
bin/ c_files/ tree/
ob> lsbackup latest
      Backup      Backup Volume      Volume      File Sect Backup
      Date and Time      ID ID      Tag      # # Level
2013/03/28.11:17:02      2 VOL000003 ADE201      1 1 0
ob> restore --select latest --priority 1 --go /home/data
Info: 1 catalog restore request item submitted; job id is admin/16.
ob> lsjob admin/16
Job ID      Sched time Contents      State
-----
admin/16      none      restore 1 item to brhost2      completed successfully at
2013/03/29.16:34
```

Example 3-61 Performing a Raw Restore Operation

This example submits a raw restore request to the scheduler. The request specifies that the `/home/data` directory should be restored from volume `VOL000003`. Oracle Secure Backup runs the job and restores the data.

```
ob> restore --raw --filenumber 1 --vid VOL000003 /home/data
ob> restore --go
Info: raw restore request 1 submitted; job id is admin/76.
ob> lsjob admin/7
Job ID      Sched time Contents      State
-----
admin/7      none      restore 1 item to brhost2      completed successfully at
2013/03/29.17:00
```

Example 3-62 Performing a Catalog Based Restore using Oracle Secure Backup Wildcard Pattern Matching

```
restore --tohost brhost2 --select latest --incremental --priority 100 --go /tmp*
```

3.1.46 returndev

Purpose

Use the `returndev` command to return a [tape drive](#) that you borrowed with the [borrowdev](#) (page 2-12) command.

**See Also:**

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `returndev` command.

Syntax

```
returndev::=  
returndev { drivename... | --all/-a }
```

Semantics***drivename***

Specifies the name of the tape drive to return.

--all/-a

Returns all the tape drives that you currently have borrowed.

Example**Example 3-63 Returning Borrowed Devices**

This example returns all borrowed devices.

```
ob> returndev --all
```

3.1.47 reusevol

Purpose

Use the `reusevol` command to recycle selected volumes. Oracle Secure Backup loads the selected volumes and deletes their backup image instances.

Each [volume](#) has a [volume label](#) stored at Beginning of Tape (BOT). The label consists of the [volume ID](#), the [barcode](#) tag (if any), and other information about the volume. The `reusevol` command is similar to the [unlabelvol](#) (page 3-146) command, but `reusevol` directs Oracle Secure Backup to preserve the existing volume label.

**See Also:**

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `reusevol` command.

Syntax

reusevol::=

```
reusevol [ --drive/-D drivename ] [ --force/-f ]
[ --obtaropt/-o obtar-option ]... se-range
```

Semantics

--drive/-D drivename

Specifies the name of the [tape drive](#) to be used to relabel the volume. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--force/-f

Forces the reuse of a volume. Oracle Secure Backup disregards the expiration date, if any, found in the volume label. If the `--force` option is not employed and the volume is not expired, then `reusevol` fails.

--obtaropt/-o obtar-option

Specifies [obtar](#) options. For example `-J` enables debug mode and provides more details in backup and restore transcripts. See "[obtar Options](#) (page B-14)" for details on `obtar` options.

se-range

Specifies the range of [storage elements](#) holding the volumes to be reused. If omitted, then the volume currently loaded in the tape drive is reused. Refer to "[se-range](#) (page 4-27)" for a description of the `se-range` placeholder.

Example

Example 3-64 Reusing a Volume

This example displays information about the tape located in storage element 2 of tape library `lib1`. The volume in this storage element is not empty. The `reusevol` command forcibly reuses the volume, thereby deleting its contents and removing its volume ID. The barcode of the volume is retained. Note that the sample output has been reformatted to fit on the page.

```
ob> lsvol --long --library lib1
Inventory of library lib1:
  in  mte:          vacant
  in  1:            barcode ADE202, oid 117, 47447360 kb remaining, content manages reuse
  in  2:            volume VOL000004, barcode ADE204, oid 120, 47420448 kb remaining
  in  3:            barcode ADE201, oid 116, 47462976 kb remaining
  in  4:            volume VOL000001, barcode ADE200, oid 102, 47424064 kb remaining
  in  iee1:         barcode ADE203, oid 114, 47725344 kb remaining,
                    lastse 4
  in  iee2:         vacant
  in  iee3:         vacant
  in  dte:         vacant
ob> lsvol --barcode ADE204 --content
VOID Seq Volume ID          Barcode      Family          Created      Attributes
   120   1 VOL000004          ADE204      04/01.09:16 never closes
        BSOID File Sect Level Host          Created      Attributes
        172   1 1          0 brhost2      04/01.09:16
ob> reusevol --drive tapel --force 2
ob> lsvol --barcode ADE204 --content
VOID Seq Volume ID          Barcode      Family          Created      Attributes
   122                                ADE204
```

3.1.48 revhost

Purpose

Use the `revhost` command to revoke a host [identity certificate](#).

See Also:

- [Oracle Secure Backup Installation and Configuration Guide](#) for more information on revoking a host identity certificate
- "[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `revhost` command.

Syntax

```
revhost::=
```

```
revhost [ --nq ] hostname...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

hostname

The name of the host whose identity certificate is to be revoked.

3.1.49 rmbackup

Purpose

Use the `rmbackup` command to remove a [backup request](#), set of backup requests, or all backup requests that are queued in `obtool`. A backup request is held locally in `obtool` until you run the [backup](#) (page 2-4) command with the `--go` option, at which time Oracle Secure Backup makes each backup request into a [dataset backup job](#) and forwards it to the [scheduler](#).

See Also:

- "[Backup Commands](#) (page 1-10)" for related commands

Prerequisites

You must have the [perform file system backups as privileged user](#) (page 8-6) right if you specified the `--privileged` option when you requested the backup. Otherwise, you must have the [perform file system backups as self](#) (page 8-6) right.

Syntax

```
rmbbackup::=
```

```
rmbbackup { --all/-a | backup-item... }
```

Semantics

--all/-a

Removes all backup requests in the queue.

backup-item

Specifies an identifier assigned by obtool to a backup request created with the [backup](#) (page 2-4) command. The identifier is a small integer number. Run the [lsbackup](#) (page 2-117) command with the `--long` option to display backup identifiers.

Example

Example 3-65 Deleting a Backup Request

This example queries the backup requests awaiting delivery to the scheduler and deletes the backup request with the identifier 2.

```
ob> lsbackup --long
1:
  Dataset:          fullbackup.ds
  Media family:    (null)
  Backup level:    full
  Priority:         100
  Privileged op:   no
  Eligible to run: upon "backup --go"
  Job expires:     never
  Restriction:     any device
2:
  Dataset:          partialbackup.ds
  Media family:    (null)
  Backup level:    full
  Priority:         100
  Privileged op:   no
  Eligible to run: upon "backup --go"
  Job expires:     never
  Restriction:     any device
ob> rmbbackup 2
ob> lsbackup --long
1:
  Dataset:          fullbackup.ds
  Media family:    (null)
  Backup level:    full
  Priority:         100
  Privileged op:   no
  Eligible to run: upon "backup --go"
  Job expires:     never
  Restriction:     any device
```

3.1.50 rmbw

Purpose

Use the `rmbw` command to remove a [backup window](#) or specific time ranges. The command displays an error if no backup windows within the specified range exist.



See Also:

"[Backup Window Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmbw` command.

Syntax

```
rmbw::=
```

```
rmbw [ --times/-t time-range[,time-range]... ] day-specifier[,day-specifier]...
```

Semantics

--times/-t *time-range*

Defines a time-of-day range. Refer to "[time-range](#) (page 4-29)" for a description of the *time-range* placeholder.

day-specifier

Defines the day ranges for the backup window. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example

Example 3-66 Removing Backup Windows

This example removes the backup windows created by the [adbbw](#) (page 2-1) command in [Example 2-1](#) (page 2-1).

```
ob> rmbw --times 00:00-08:00 mon-friob> rmbw --times 20:00-24:00 mon-friob> rmbw --times 08:00-20:00 weekend
```

3.1.51 rmcheckpoint

Purpose

Use the `rmcheckpoint` command to remove checkpoint information for the specified jobs. When you issue this command, Oracle Secure Backup immediately removes all administrative-host resident checkpoint data for the specified job. It cleans up [filer](#)-resident data at the beginning of the next backup of this filer or within 24 hours, whichever comes first.

If no checkpoints exist, then `obtool` displays the following error message:

Error: no checkpoints matched the selection criteria.

 **See Also:**

"[Checkpoint Commands](#) (page 1-12)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `rmcheckpoint` command.

Syntax

`rmcheckpoint::=`

```
rmcheckpoint [ --nq ] { { --host/-h hostname[,hostname]... }... | --all/-a |  
job-id... }
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--host/-h *hostname*

Deletes all checkpoints describing the [client](#) host specified by *hostname*.

--all/-a

Deletes all checkpoints within the [administrative domain](#).

job-id

Deletes the checkpoint identified by job ID *job-id*.

Example

Example 3-67 Removing Checkpoints

This example removes two checkpoints: one specified by job ID and the other by host.

```
ob> rmcheckpoint 1660.3  
ob> rmcheckpoint --host brhost2,brhost3
```

3.1.52 rmclass

Purpose

Use the `rmclass` command to remove an [Oracle Secure Backup user class](#) from an [administrative domain](#).

 **See Also:**

- "[Class Commands](#) (page 1-13)" for related commands
- [Classes and Rights](#) (page 8-1) for a descriptions of the default Oracle Secure Backup classes and [rights](#)

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmclass` command. The class must be empty, that is, have no Oracle Secure Backup users, to be deleted.

Syntax

```
rmclass::=  
rmclass [ --nq ] classname...
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

classname

Specifies the name of the class to delete.

Example**Example 3-68 Removing a Class**

This example confirms that the `bkup_admin` class exists, deletes it, and then confirms that the class is deleted.

```
ob> lsclass bkup_admin  
bkup_admin  
ob> rmclass --nq bkup_admin  
ob> lsclass bkup_admin  
Error: class bkup_admin - name not found
```

3.1.53 rmdev

Purpose

Use the `rmdev` command to remove a device from an [administrative domain](#) or to move it from one location to another within the administrative domain. You can run the [mkdev](#) (page 3-6) command to reconfigure a device for use by Oracle Secure Backup.

 **See Also:**

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmdev` command.

Usage Notes

- When you remove a disk pool or cloud storage device, Oracle Secure Backup does not automatically delete its contents. The contents are deleted only if you specify the `--deletecontents` option. Regardless of whether its contents are deleted or not, all backup catalog data associated with backup image instances contained in the disk pool or cloud storage device is deleted from the backup catalog. The catalog data is deleted during the next regular catalog cycle as specified by the `index/indexcleanup` policy.

Syntax

`rmdev::=`

```
rmdev [ --nq ] [ --migrate/-m new_devicename ]
[ --deletecontents/-d ] [ --force/-f ]
devicename...
```

Semantics

--nq

Does not display a confirmation message before removing the device from the administrative domain. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--migrate/-m *new_devicename*

Logically migrates all volumes that have references to the location corresponding to *devicename* to the location corresponding to *new_devicename*. The `--migrate` option can specify only one device name at a time.

--deletecontents/-d

Deletes all content from a cloud storage device (and also removes the cloud container), or deletes all backup image instances stored in the disk pool. If the container contains unexpired backup image instances, then Oracle Secure Backup displays a message indicating that the `--force` option must be used to delete the contents.

--force/-f

Deletes all backup image instances, even if they are valid and not expired.

devicename

Specifies the name of the device to remove or move to a different location. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example

Example 3-69 Removing a Tape Drive

This example removes a [tape drive](#) from a [tape library](#).

```
ob> lsdev
library    lib1            in service
  drive 1  tape1            in service
library    lib2            in service
  drive 1  tape2            in service
  drive 2  tape2a           in service
ob> rmdev tape2a
Warning: removing a device to which a job is restricted will cause the job
        to become unusable.
remove device tape2a? (a, n, q, y, ?) [n]: y
ob> lsdev
library    lib1            in service
  drive 1  tape1            in service
library    lib2            in service
  drive 1  tape2            in service
```

Example 3-70 Removing a Disk Pool and Its Contents

This example removes a disk pool `dp2` and its contents. The `--force` option indicates that unexpired backup image instances must also be deleted.

```
ob> rmdev --deletecontents --force dp2
Warning: removing a device to which a job is restricted will cause the job
        to become unusable.
remove device dp2? (a, n, q, y, ?) [n]: y
```

3.1.54 rmds

Purpose

Use the `rmds` command to remove a [dataset file](#) or [dataset directory](#).



See Also:

"[Dataset Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmds` command.

Syntax

```
rmds::=
rmds [ --nq ] dataset-name...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

dataset-name

Specifies the name of the dataset directory or dataset file that you created with the [mkds](#) (page 3-21) or [rends](#) (page 3-85) command. Refer to "[dataset-name \(page 4-8\)](#)" for a description of the *dataset-name* placeholder.

Example

Example 3-71 Removing a Dataset

This example removes a dataset directory named `mydatasets` and a dataset file named `full_backup.ds`.

```
ob> lsds
Top level dataset directory:
mydatasets/
full_backup.ds
ob> rmds --nq mydatasets
ob> lsds
Top level dataset directory:
full_backup.ds
ob> rmds --nq full_backup.ds
ob> lsds
Top level dataset directory:
ob>
```

3.1.55 rmdup

Purpose

Removes one or more duplication policies.



See Also:

"[Volume Duplication Commands \(page 1-22\)](#)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmdup` command.

Syntax

`rmdup::=`

```
rmdup [ -nq/--noquery ] { polycyname } [ polycyname ]...
```

Semantics

-nq/--noquery

By default, the backup administrator is prompted before the duplication policy is removed. With `--nq`, no confirmation is requested.

policyname

The duplication policy with the specified name is removed.

Example

Example 3-72 Removing a Duplication Policy

This example removes the `voldup` duplication policy.

```
ob> lsdup
voldup
ob> rmdup --nq voldup
ob> lsdup
ob>
```

3.1.56 rmdw

Purpose

Use the `rmdw` command to remove a duplication window.



See Also:

["Duplication Window Commands \(page 1-15\)"](#) for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmdw` command.

Syntax

`rmdw::=`

```
rmdw { --times/-t time-range[,time-range]... }
      day-specifier[,day-specifier]...
```

Semantics

--times/-t *time-range*

Defines a time-of-day range for the duplication window. Refer to "[time-range](#) (page 4-29)" for a description of the `time-range` placeholder.

day-specifier

Defines the day ranges for the duplication window. Refer to "[day-specifier](#) (page 4-12)" for a description of the `day-specifier` placeholder.

Example

Example 3-73 Removing a Duplication Window

This example removes an existing duplication window.

```
ob> lsdw09/30 15:30-16:30:30weekend 10:00-21:00weekday 10:00-20:00b> rmdw --times
0900-0930 tuesday
ob> lsdw
09/30 15:30-16:30:30
weekend 10:00-21:00
Mon Wed-Fri 10:00-20:00
```

3.1.57 rmhost

Purpose

Use the `rmhost` command to remove a host from the Oracle Secure Backup [administrative domain](#). When you remove a host, Oracle Secure Backup destroys all information pertinent to the host, including:

- Configuration data
- Incremental backup state information
- Metadata in the backup [catalog](#)
- Device attachments
- [PNI \(Preferred Network Interface\)](#) references

Moreover, when you remove a UNIX or Windows host, Oracle Secure Backup contacts that host and directs it to delete the administrative domain membership information that it maintains locally. You can suppress this communication if the host is no longer accessible.



See Also:

["Host Commands \(page 1-16\)"](#) for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmhost` command.

Usage Notes

- The `rmhost` command fails if there are any stage rules that contain the Oracle Secure Backup host name. All stage rules that contain the Oracle Secure Backup host name are listed in the error message.
- If you attempt to delete a host that is contained in a stage rule, then the `rmhost` command fails with an error.

Syntax

```
rmhost::=
```

```
rmhost [ --nq ] [ --nocomm/-N ] hostname...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--nocomm/-N

Suppresses communication with the host computer. Use this option to remove a computer that is not connected to the network. This option does not apply to hosts accessible only through [Network Data Management Protocol \(NDMP\)](#).

hostname

Specifies the name of the host to remove.

Example

Example 3-74 Removing a Host

This example shows that `brhost4` is not in service and then removes `brhost4` from the administrative domain.

```
ob> lshost
brhost2      client                               (via OB)  in service
brhost3      mediaserver,client                   (via OB)  in service
brhost4      client                               (via OB)  not in service
sfserver1    client                               (via OB)  in service
osbsvr1      admin,mediaserver,client            (via OB)  in service
ob> rmhost --nq --nocomm brhost4
ob> lshost
brhost2      client                               (via OB)  in service
brhost3      mediaserver,client                   (via OB)  in service
sfserver1    client                               (via OB)  in service
osbsvr1      admin,mediaserver,client            (via OB)  in service
```

3.1.58 rminstance

Purpose

The `rminstance` command deletes backup image instances from disk pool and cloud storage devices.

Prerequisites

You must have the [modify any backup, regardless of its owner](#) (page 8-5) or [modify any backups owned by user](#) (page 8-5) class right to use the `rminstance` command.

Usage Notes

You can use the `rminstance` command only to delete backup image instances that are stored on disk pool or cloud storage devices. When you delete a backup image instance, Oracle Secure Backup removes the associated information from the backup catalog. If all the backup image instances associated with a particular backup image are stored on disk pool or cloud storage devices, then Oracle Secure Backup removes the backup image also when the last backup image instance is deleted.

If the backup image instance specified in the `rminstance` command is currently being used in another operation (for example, in a `cpinstance` command), then Oracle Secure Backup marks this instance for deletion and deletes it after the operation is completed.

Syntax

```
rminstance::=
```

```
rminstance [--nq] [--force/-f]
{ [--uuid/-u backup-instance-uuid]... | backup-instance-name... }
```

Semantics

--nq

Specifies that no confirmation is required before removing the backup image instance.

--force/-f

Forces a delete of the backup image instance even if it has not expired. Use this option to remove active backup image instances that are unexpired.

--uuid/-u *backup-instance-uuid*]... | *backup-instance-name*...

Specifies the UUID or name of the backup image instance that must be deleted. If the specified instance has not expired, then you cannot delete it unless you use the `--force` option.

Examples

This example deletes the backup image instance `bk_fs_test.3` that is stored on the disk pool `dp1`. The `--force` option is used because the backup image instance has not expired. Oracle Secure Backup asks for confirmation before deleting the backup image instance.

```
ob> rminstance --force bk_fs_test.3
Info: backup instance bk_fs_test.3 has not expired
delete backup instance bk_fs_test.3? (a, n, q, y, ?) [n]: y
```

3.1.59 rmjob

Purpose

Use the `rmjob` command to remove jobs. Removing a job has the effect of canceling it and deleting all record of the existence of the job and its subordinate jobs. You can remove a job only if it is not running. After removing a job, you cannot view its status.



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to remove the jobs of another [Oracle Secure Backup user](#), then you must have the right to [modify any job, regardless of its owner](#) (page 8-5). If you

are attempting to remove your own jobs, then you must have the right to [modify any jobs owned by user](#) (page 8-5).

Syntax

```
rmjob::=
```

```
rmjob [ --nq ] [ --keepxcr/-k ] [ --quiet/-q | --verbose/-v ] job-id...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--keepxcr/-k

Keeps the job transcript. The default is to delete the transcript of the job.

--quiet/-q

Removes the job quietly.

--verbose/-v

Displays verbose output about the job removal.

job-id

Specifies the job IDs of the jobs to remove.

Example

Example 3-75 Removing a Job

This example displays all active and pending jobs and removes them.

```
ob> lsjob
Job ID          Sched time  Contents                               State
-----
sbt/13          03/23.00:00 dataset fullbackup.ds                 future work
ob> rmjob --nq sbt/13
Info: removing job sbt/13.
ob> lsjob
ob>
```

3.1.60 rmloc

Purpose

Use the `rmloc` command to remove a [location](#).



See Also:

"[Location Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmloc` command.

Syntax

```
rmloc::=
```

```
rmloc [ --nq ] locationname...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

locationname

Specifies the location to remove, using its location name.

3.1.61 rmmf

Purpose

Use the `rmmf` command to remove a [media family](#).

Removing a media family does not affect the metadata on tapes that were originally written using that media family.



See Also:

"[Media Family Commands](#) (page 1-17)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmmf` command.

Usage Notes

- The `rmmf` command fails if any there are any stage rules that contain the media family. All stage rules that contain the media family are listed in the error message.

Syntax

```
rmmf::=
```

```
rmmf [ --nq ] media-family-name...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

media-family-name

Specifies the name of the media family you want to remove. Note that you cannot remove the `RMAN-DEFAULT` media family.

Example

Example 3-76 Removing Media Families

This example removes the media families named `content-man-family` and `time-man-family`.

```

ob> lsmf
RMAN-DEFAULT                               content manages reuse
content-man-family write forever             content manages reuse
full_backup      write 7 days                content manages reuse
time-man-family  write 7 days                keep 28 days
ob> rmmf --nq content-man-family time-man-family
ob> lsmf
RMAN-DEFAULT                               content manages reuse
full_backup      write 7 days                content manages reuse

```

3.1.62 rmp

Purpose

Use the `rmp` command to remove a variable name-value pair from a policy.

See Also:

- "[Policy Commands \(page 1-18\)](#)" for related commands
- [Defaults and Policies \(page 7-1\)](#) for a complete list of policies and policy classes

Prerequisites

You must have the [modify administrative domain's configuration \(page 8-4\)](#) right to use the `rmp` command.

Syntax

```
rmp::=
```

```
rmp policy-name member-name...
```

Semantics

policy-name

Specifies the name of a policy or a class of policies.

member-name

Specifies a user-assigned name of a policy, usually an environment variable name.

Example

Example 3-77 Enabling Verbose Output from the NDMP Data Service

This example uses the `rmp` command to unset the `VERBOSE` environment variable for an `ndmp/backupdev` policy. [Example 2-3](#) (page 2-3) shows how to set the variable for the policy.

```

ob> pwdp
/
ob> lsp ndmp/backupdev
backupdev          VERBOSE          y
ob> rmp ndmp/backupdev VERBOSE
ob> lsp ndmp/backupdev
backupdev          (none)          [default]

```

3.1.63 rmpiece

Purpose

Use the `rmpiece` command to delete a [Recovery Manager \(RMAN\) backup piece](#) from the Oracle Secure Backup catalog. This command scans the catalog and updates it to be in sync with the RMAN catalog. If a backup piece has been removed from the RMAN catalog, the `rmpiece` command ensures that the same backup piece and related database backup information is also removed from the Oracle Secure Backup catalog.

This command cannot be undone and therefore must be used sparingly. Using RMAN is the recommended method for managing backup pieces.



See Also:

["Backup Piece Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `rmpiece` command.

Syntax

```
rmpiece::=
```

```
rmpiece [ --nq ] [ --oid/-o oid-list ]... [ piename ]...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

--oid/-o *oid-list*

Specifies or more backup piece identifiers in the Oracle Secure Backup [catalog](#). Refer to "[oid \(page 4-21\)](#)" for a description of the *oid* placeholder.

piecename

Specifies the names of the backup pieces to which the listing applies. The name of a backup piece is indicated by the `Piece name` heading in the [lspiece](#) (page 2-160) output.

Example

Example 3-78 Removing Backup Pieces

This example displays information about two RMAN backup pieces and then deletes them.

```
ob> lspiece
      POID Database   Content      Copy Created      Host              Piece name
      104 ob          full         0 03/18.16:25    osbsvr1          05gfkmg9_1_1
      105 ob          archivelog   0 03/18.16:32    osbsvr1          06gfknh8_1_1
ob> rmpiece --oid 104,105
remove backup piece OID 104? (a, n, q, y, ?) [n]: y
remove backup piece OID 105? (a, n, q, y, ?) [n]: y
ob> lspiece
ob>
```

3.1.64 rmpni

Purpose

Use the `rmpni` command to remove [PNI \(Preferred Network Interface\)](#) definitions.



See Also:

["Preferred Network Interface Commands \(page 1-19\)"](#) for related commands

Prerequisites

You must have the [modify administrative domain's configuration \(page 8-4\)](#) right to use the `rmpni` command.

Syntax 1

Use the following syntax to remove all PNIs defined for a server.

```
rmpni::=
```

```
rmpni server-hostname...
```

Syntax 2

Use the following syntax to remove a [client](#) host from all PNI definitions.

```
rmpni::=  
rmpni [ --client/-c client-hostname[,client-hostname]... ]...
```

Syntax 3

Use the following syntax to remove all PNIs that use a specific interface on a server.

```
rmpni::=  
rmpni [ --interface/-i server-ipname[,server-ipname]... ]...
```

Syntax 4

Use the following syntax to remove a client host from the PNI defined for the specified server.

```
rmpni::=  
rmpni [ --client/-c client-hostname[,client-hostname]... ]...  
server-hostname...
```

Semantics

--client/c *client-hostname*[,*client-hostname*]...

Specifies one or more client hosts from which you want to remove PNIs.

--interface/-i *server-ipname*[,*server-ipname*]...

Specifies the IP address or the DNS name of the interface to be removed.

server-hostname

Specifies the name of the server computer.

Examples

Example 3-79 Removing All PNI Definitions for a Host

This example uses the syntax shown in Syntax 1 to remove all network interfaces for host `brhost3`.

```
ob> lspni  
brhost2:  
  PNI 1:  
    interface:      192.0.2.1  
    clients:        osbsvr1, brhost4, sfserver1  
brhost3:  
  PNI 1:  
    interface:      192.0.2.200  
    clients:        osbsvr1, brhost4, sfserver1  
ob> rmpni brhost3  
ob> lspni  
brhost2:  
  PNI 1:  
    interface:      192.0.2.1  
    clients:        osbsvr1, brhost3, sfserver1
```

Example 3-80 Removing a Client from All PNI Definitions

This example uses the syntax shown in Syntax 2 to remove the client hosts `sfserver1` and `osbsvr1` from all network interfaces definitions.

```
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        osbsvr1, brhost4, sfserver1
brhost3:
  PNI 1:
    interface:      192.0.2.200
    clients:        osbsvr1, brhost4, sfserver1
ob> rmpni --client sfserver1,osbsvr1
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        brhost4
brhost3:
  PNI 1:
    interface:      192.0.2.200
    clients:        brhost4
```

Example 3-81 Removing All PNI Definitions That Use a Specified Interface

This example uses the syntax shown in Syntax 3 to remove all PNIs that use interface `192.0.2.1` on a server.

```
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        osbsvr1, brhost4, sfserver1
brhost3:
  PNI 1:
    interface:      192.0.2.200
    clients:        osbsvr1, brhost4, sfserver1
ob> rmpni --interface 192.0.2.1
ob> lspni
brhost3:
  PNI 1:
    interface:      192.0.2.200
    clients:        osbsvr1, brhost4, sfserver1
```

Example 3-82 Removing Clients from a PNI Definition

This example uses the syntax shown in Syntax 4 to remove the clients `osbsvr1` and `sfserver1` from the PNI definition for server `brhost2`.

```
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        osbsvr1, brhost4, sfserver1
ob> rmpni --client osbsvr1,sfserver1 brhost2
ob> lspni
brhost2:
  PNI 1:
    interface:      192.0.2.1
    clients:        brhost4
```

3.1.65 rmrestore

Purpose

Use the `rmrestore` command to remove a restore request from the queue.

See Also:

"[Restore Commands](#) (page 1-19)" for related commands

Prerequisites

If you specified that the restore run in privileged mode, or if you are restoring files to a host accessed through [Network Data Management Protocol \(NDMP\)](#), then you must have the right to [perform file system restores as privileged user](#) (page 8-6) to use the `restore` command. Otherwise, you must have the right to [perform file system restores as self](#) (page 8-7).

Syntax

```
rmrestore::=
```

```
rmrestore { --all /-a | restores-item... }
```

Semantics

--all

Removes all restore requests.

restores-item

Specifies the item number of the restore request to remove. You can display the item numbers for restore requests by running the [lsrestore](#) (page 2-164) command.

Example

Example 3-83 Removing a Restore Request

This example removes a queued restore request by specifying its item number.

```
ob> lsrestore
Item      Restore data saved from...      To...
#         Host          Path                          Host          Path
1         brhost2      /home/data/backup             brhost2      (original location)
ob> rmrestore 1
ob> lsrestore
```

3.1.66 rmrot

Purpose

Removes rotation policies.

**See Also:**

"[Rotation Policy Commands](#) (page 1-20)"

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmdup` command.

Syntax

```
rmrot::=
```

```
rmrot  
  --noquery/-nq  
  rotationname [ rotationname... ]
```

Semantics**--noquery/-nq**

By default, the backup administrator is prompted before the policy is removed. With `--noquery`, no confirmation is requested.

rotationname

The name of the rotation policy to remove.

3.1.67 rmsched

Purpose

Use the `rmsched` command to remove a [backup schedule](#). Run the `lssched` (page 2-167) command to display backup schedules.

**See Also:**

"[Schedule Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmsched` command.

Syntax

```
rmsched::=
```

```
rmsched [ --nq ] schedulename...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

*schedule*name

Specifies the name of the schedule to remove.

Example

Example 3-84 Removing a Backup Schedule

[Example 3-84](#) (page 3-129) removes the backup schedule named `incremental`.

```

ob> lssched
full_backup          sundays          homedir.ds
incremental          mondays tuesdays wednesdays thursdays homedir.ds
ob> rmsched --nq incremental
ob> lsschedfull_backup          sundays          homedir.ds

```

3.1.68 rmsection

Purpose

Use the `rmsection` command to inform Oracle Secure Backup that a [backup section](#) is deleted. Oracle Secure Backup does not physically remove the section from the [volume](#), but indicates in its backup sections [catalog](#) that the section is removed. You can view the status of a section by running the [lsection](#) (page 2-170) command. Typically, you use `rmsection` only when the backup sections catalogs require manual update.

Note:

If you remove a backup section that contains a [Recovery Manager \(RMAN\) backup piece](#), then Oracle Secure Backup responds to RMAN queries concerning the backup piece by saying that it does not exist.

See Also:

"[Section Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `rmsection` command.

Syntax

```
rmsection::=
```

```
rmsection [ --nq ] [ --oid/-o oid-list ]...[ --vid/-v vid { --file/-f filenumber-
list }... ]
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--oid *oid-list*

Selects backup sections with the object identifiers matching those in *oid-list*. Refer to "[oid-list](#) (page 4-22)" for a description of the *oid-list* placeholder.

--vid *vid*

Selects backup sections contained on the volume specified by *vid*. Refer to "[vid](#) (page 4-30)" for a description of the *vid* placeholder.

--file/-f *filenumber-list*

Selects the backup sections with the file numbers specified in the list. Refer to "[filenumber-list](#) (page 4-16)" for a description of the *filenumber-list* placeholder.

Example

Example 3-85 Removing Backup Sections

This example deletes a section that contains an RMAN backup piece. A query of the backup sections catalog shows that the backup section has the attribute `deleted`.

```
ob> lssection --short
BSOID
 106
 107
ob> rmsection --nq --oid 107
ob> lssection --long
Backup section OID: 106
  Containing volume: VOL000003
  Containing volume OID: 110
  File: 1
  Section: 1
  Backup level: 0
  Client: brhost2
  Created: 2013/04/19.11:36
  Attributes: never expires
Backup section OID: 107
  Containing volume: RMAN-DEFAULT-000002
  Containing volume OID: 112
  File: 1
  Section: 1
  Backup level: 0
  Client: osbsvr1
  Created: 2013/04/19.11:37
  Attributes: deleted
```

3.1.69 rmsnap

Purpose

Use the `rmsnap` command to remove a [snapshot](#).

 **See Also:**

"[Snapshot Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `rmsnap` command.

Syntax

`rmsnap::=`

```
rmsnap [ --host/-h hostname ] [ --fs/-f filesystem-name ]
[ --nowait/-n ] snapshot-name...
```

Semantics

--host/-h *hostname*

Specifies the name of the [Network Data Management Protocol \(NDMP\)](#) host that contains the snapshot to remove. If you do not specify a host name, then Oracle Secure Backup uses the value from the [host](#) (page 5-3) variable.

--fs/-f *filesystem-name*

Specifies the name of the file system included in the snapshot. If you do not specify the `--fs` option, then the `fs` variable must be set.

--nowait/-n

Does not wait for the snapshot removal operation to complete.

snapshot-name

Specifies the name of the snapshot to remove.

Example

Example 3-86 Removing a Snapshot

This example creates a snapshot called `test` and then deletes it.

```
ob> set fs /vol/vol0
ob> mksnap --host lucy
ob> lssnap test
File system /vol/vol0:
Snapshot Of          Taken at          %Used  %Total  Snapshot Name
/vol/vol0            2013/03/28.21:11    0      0      test
ob> rmsnap test
ob> lssnap test
Warning: snapshot test not found on host lucy, file system /vol/vol0.
```

Example 3-87 Removing a Snapshot

This example deletes three snapshots from the host `storabcknfs4`.

```
ob> lssnap -h storabcknfs4
File system /vol/vol1:
Snapshot Of  Taken at          %Used  %Total  Snapshot Name
/vol/vol1   2010/08/18.04:00  0      0      nightly.0
/vol/vol1   2010/08/18.02:47  0      0      snapshot_for_backup.8204
```

```

/vol/voll 2010/08/18.00:00 0 0 hourly.0
/vol/voll 2010/08/17.20:00 0 0 hourly.1
/vol/voll 2010/08/17.16:00 0 0 hourly.2
/vol/voll 2010/08/17.12:00 0 0 hourly.3
/vol/voll 2010/08/17.04:00 0 0 nightly.1
/vol/voll 2010/08/16.04:00 0 0 weekly.0
/vol/voll 2010/08/15.04:00 0 0 nightly.2
/vol/voll 2010/08/14.04:00 1 0 nightly.3
/vol/voll 2010/08/13.04:00 0 0 nightly.4
/vol/voll 2010/08/09.04:00 9 5 weekly.1
ob> rmsnap -h storabcknfs4 -f/vol/voll hourly.3
ob> rmsnap -h storabcknfs4 -f/vol/voll nightly.4
ob> rmsnap -h storabcknfs4 -f/vol/voll nightly.3
ob> lssnap -h storabcknfs4
File system /vol/voll:
Snapshot Of Taken at %Used %Total Snapshot Name
/vol/voll 2010/08/18.04:00 0 0 nightly.0
/vol/voll 2010/08/18.02:47 0 0 snapshot_for_backup.8204
/vol/voll 2010/08/18.00:00 0 0 hourly.0
/vol/voll 2010/08/17.20:00 0 0 hourly.1
/vol/voll 2010/08/17.16:00 0 0 hourly.2
/vol/voll 2010/08/17.04:00 0 0 nightly.1
/vol/voll 2010/08/16.04:00 0 0 weekly.0
/vol/voll 2010/08/15.04:00 0 0 nightly.2
/vol/voll 2010/08/09.04:00 9 5 weekly.1

```

3.1.70 rmsssel

Purpose

Use the `rmsssel` command to remove a [database backup storage selector](#).



See Also:

"[Database Backup Storage Selector Commands](#) (page 1-14)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmsssel` command.

Syntax

```
rmsssel::=
```

```
rmsssel [ --nq ] sselname...
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

sselname

Specifies the names of the database backup storage selectors to remove.

Example**Example 3-88 Deleting a Database Backup Storage Selector**

This example deletes the storage selector named `ssel_full_arch`.

```
ob> lsssel --short
ssel_full_arch
ob> rmssel ssel_full_arch
remove ssel ssel_full_arch? (a, n, q, y, ?) [n]: y
ob> lsssel
ob>
```

3.1.71 rmstage

Purpose

The `rmstage` command deletes one or more stage rules.

Usage Notes

The `rmstage` command fails if any stage rule is currently set in a staging disk pool device, and all stage devices that contain the stage rule are listed in the error message.

Syntax

```
rmstage::=
```

```
rmstage [--nq ] stage-rule-name [stage-rule-name]...
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

stage-rule-name

Specifies the name of the stage rule to remove.

Example**Example 3-89 Example Title**

```
ob> rmstage --nq stagerulexyz
```

3.1.72 rmsum

Purpose

Use the `rmsum` command to remove a [job summary schedule](#).

**See Also:**

"[Summary Commands](#) (page 1-21)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmsum` command.

Syntax

```
rmsum::=
```

```
rmsum [ --nq ] summary-name...
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

summary-name

Specifies the name of the job summary schedule to remove.

Example**Example 3-90 Removing a Job Summary Schedule**

This example removes the job summary schedule named `weekly_report`.

```
ob> lssum
weekly_report          Wed at 12:00
ob> rmsum --nq weekly_report
ob> lssum
ob>
```

3.1.73 rmuser

Purpose

Use the `rmuser` command to remove an [Oracle Secure Backup user](#) from the [administrative domain](#).

**See Also:**

"[User Commands](#) (page 1-22)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `rmuser` command.

Syntax

```
rmuser::=
```

```
rmuser [ --nq ] username...
```

Semantics**--nq**

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the confirmation message.

username

Specifies the name of the Oracle Secure Backup user to remove.

Example**Example 3-91 Removing an Oracle Secure Backup User**

This example removes Oracle Secure Backup user `bkpadmin`.

```
ob> lsuser
admin          admin
bkpadmin       oracle
sbt            admin
tadmin        admin
ob> rmuser --nq bkpadmin
ob> lsuser
admin          admin
sbt            admin
tadmin        admin
```

3.1.74 rmvol

Purpose

Use the `rmvol` command to remove volume records from the Oracle Secure Backup catalog permanently. The only way to undo the removal is to import the volume again, so that the Oracle Secure Backup catalog is repopulated.

**See Also:**

"[Volume Rotation Commands \(page 1-22\)](#)" for related commands

Prerequisites

You must have the [modify catalog \(page 8-6\)](#) right to use the `rmvol` command.

Syntax

```
rmvol::=
```

```
rmvol [ --nq ] [ --force/-f ]
{ [ --vid/-v vol-spec[,vol-spec]... ]
```

```
[ --barcode/-b barcode_value[,barcode_value]... ]
[ --location/-l location_name[,location_name]... ]
}
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then you are prompted for confirmation before the volume is deleted. You can reply to the confirmation request with one of the following:

- a
Remove records for all volume selections. Enter this response when prompted for confirmation for the first volume in the selection.
- n
Remove no records.
- q
Remove no records and quit the command.
- y
Remove the record for this volume.
- ?
Repeat the prompt.

--force/-f

By default, you can only remove the records of expired volumes. You can specify `--force` to override this restriction and remove the records of unexpired volumes as well.

--vid/-v *vol-spec*

Specifies the volume ID of the volume whose record you want to remove. See "[vol-spec](#) (page 4-31)" for more information on the *vol-spec* placeholder.

--barcode/-b *barcode_value*

Specifies the barcode of the volume whose record you want to remove.

--location/-l *location_name*

Specifies the location of the volume or volumes whose records you want to remove. Oracle Secure Backup removes the records of all volumes at the specified location.



Note:

You must specify `--vid`, `--barcode`, or `--location`, but you can specify multiple options.

If the volumes database contains multiple entries matching a specified *vol-spec* or barcode, then Oracle Secure Backup displays a list of the matching volumes from which you can choose volumes to remove. The following example shows multiple matches for *vol-spec* `VOL000001`:

```
ob> rmvol -f -v VOL000001
Your vol-spec, "VOL000001", matched the following volumes:
```

	Volume ID	Barcode	Created
1	VOL000001	def5768a15b710295f7000423a5cbf4	
2	VOL000001	3f2e113415b7102a59e000423a5cbf4	06/05.15:28

Please select the volume(s) that you wish to modify (1, 2, ..., a(11), n(one), q(uit)):

3.1.75 rpyjob

Purpose

Use the `rpyjob` command to respond to a job that is prompting for input or assistance. You can display jobs of this type by specifying `--inputrequest` on the [lsjob](#) (page 2-149) command. You can determine what a job is requesting by performing a [catxcr](#) (page 2-22) command.



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to respond to the job prompts of another [Oracle Secure Backup user](#), then you must have the right to [modify any job, regardless of its owner](#) (page 8-5). If you are attempting to respond to your own job prompts, then you must have the right to [modify any jobs owned by user](#) (page 8-5).

Syntax

```
rpyjob::=
rpyjob --reply/-r text job-id...
```

Semantics

--reply/-r text

Specifies the textual reply to the prompt. To include white space in the value, surround the text with quotes.

job-id

Specifies the identifier of the job to which the reply is to be sent.

Example

Example 3-92 Displaying Information About a Job Requesting Assistance

This example uses [lsjob](#) (page 2-149) to display jobs that are requesting assistance and then runs [catxcr](#) (page 2-22) to display the transcript for job `admin/7.1`.

The transcript shows that the [tape library](#) does not contain a usable tape for the [backup job](#). Press the Enter key after running `catxcr` to return to the `obtool` prompt.

```
ob> lsjob --inputrequest --long
admin/7.1:
```

```

Type:                backup brhost2
Level:               full
Family:              (null)
Scheduled time:      none
State:               running since 2013/01/09.12:38
Priority:             100
Privileged op:       no
Run on host:         brhost2
Attempts:            1

ob> catxcr --tail 12 admin/7.1
End of tape has been reached. Please wait while I rewind and unload the tape.
The Volume ID of the next tape to be written is VOL000005.
The tape has been unloaded.
  obtar: couldn't perform auto-swap - can't find usable volume in library (OB device
mgr) Enter a command from the following list:
  load <n>          .. load the tape from element <n> into the drive
  unload <n>        .. unload the tape from the drive into element <n>
  help              .. display other commands to modify drive's database
  go                .. to use the tape you selected
  quit             .. to give up and abort this backup or restore
:

```

Example 3-93 Displaying Information About a Job Requesting Assistance

This example inserts a [volume](#) into the tape library and then uses `rpyjob` to reply with two commands: `load 3` and `go`. Specifying `--inputrequest` on `lsjob` generates a null response, which means that no jobs require input.

```

ob> insertvol --library lib2 unlabeled 3
ob> rpyjob --reply "load 3" admin/7.1
ob> rpyjob --reply "go" admin/7.1
ob> lsjob --inputrequest
ob>

```

3.1.76 runjob

Purpose

Use the `runjob` command to control how a job is processed. The command enables you to start a job in the following ways:

- Immediately
- In an order different from that of the [scheduler](#)
- On a specific device or a device from which the job was previously restricted



See Also:

"[Job Commands](#) (page 1-16)" for related commands

Prerequisites

If you are attempting to control jobs belonging to another [Oracle Secure Backup user](#) are processed, then you must have the right to [modify any job, regardless of its owner](#)

(page 8-5). If you are attempting to control the processing of your own jobs, then you must have the right to [modify any jobs owned by user](#) (page 8-5).

Syntax

runjob::=

```
runjob { --asap/-a | --now/-n | { --priority/-p schedule-priority } }
[ --device/-d device-name ] [ --mediamovement/-m ] [ --quiet/-q | --verbose/-v ]
job-id...
```

Semantics

--asap/-a

Starts the job as soon as possible by raising it to priority 1.

--now/-n

Starts the job now. If Oracle Secure Backup cannot start the job, then it generates an error message.

--priority/-p *schedule-priority*

Resets the job priority to *schedule-priority*. The default priority is 100. Refer to "[schedule-priority](#) (page 4-26)" for a description of the *schedule-priority* placeholder.

--device/-d *device-name*

Runs the job on the device specified by *device-name*, ignoring job requirements.

--mediamovement/-m

Enables the pending media movement job specified by *job-id*.

--quiet/-q

Runs the job in quiet mode. `--quiet` directs `obtool` to suppress status messages it would normally write to `stdout`. Note that Oracle Secure Backup never suppresses error messages.

--verbose/-v

Displays output when running the job.

job-id

Specifies the identification number of the job you want to run. Run the [lsjob](#) (page 2-149) command to display job IDs.

Example

Example 3-94 Running a Job Now

This example lists a pending job and runs it immediately.

```
ob> lsjob --pending
Job ID          Sched time  Contents                               State
-----
sbt/23          03/22.21:00 dataset workdata.ds                 future work
ob> runjob --device tape1 --now sbt/23
ob> lsjob --all sbt/23
Job ID          Sched time  Contents                               State
-----
sbt/23          03/22.21:00 dataset workdata.ds                 completed successfully
at 2013/03/22.18:09
```

3.1.77 set

Purpose

Use the `set` command to set or reset the value of an obtool variable in the current session.



See Also:

[obtool Variables](#) (page 5-1) for a complete list of obtool variables

Syntax

```
set::=
```

```
set [ variable-name [ variable-value ] ]
```

Semantics

variable-name

Specifies the name of the variable to set. If you do not specify a variable name, then `set` displays the variables that are currently set.

variable-value

Specifies the value to which *variable-name* should be set.

Example

Example 3-95 Setting a Variable

This example sets the `errors` variable to `long` so that errors include descriptive text and the obtool component name and then resets it to `short`.

```
ob> show errors
errors          (not set)
ob> set errors long
ob> show errors
errors          long
ob> set errors short
ob> show errors
errors          short
```

3.1.78 setbw

Purpose

Use the `setbw` command to change the settings of a [backup window](#). This command replaces an existing backup window, as opposed to the [addbw](#) (page 2-1) command, which adds a backup window.

 See Also:

"[Backup Window Commands](#) (page 1-11)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `setbw` command.

Syntax

```
setbw::=
```

```
setbw { --times/-t { none | time-range[,time-range]... } }  
day-specifier[,day-specifier]...
```

Semantics**--times/-t *time-range***

Defines a time-of-day range. Refer to "[time-range](#) (page 4-29)" for a description of the *time-range* placeholder.

day-specifier

Defines the day ranges for the backup window. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example**Example 3-96 Changing Backup Windows**

This example changes the settings of the backup windows created in [Example 2-1](#) (page 2-1). These backup windows allow backups from 7 a.m. until 9 p.m. on weekdays and any time during the weekend.

```
ob> setbw --times 00:00-07:00 mon-fri  
ob> setbw --times 21:00-24:00 mon-fri  
ob> setbw --times 00:00-24:00 weekend
```

3.1.79 setdw

Purpose

Use the `setdw` command to set a duplication window, which is a time and day range.

 See Also:

"[Duplication Window Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `setdw` command.

Syntax

setdw::=

```
setdw { --times/-t none | time-range[,time-range]... }
      day-specifier[,day-specifier]...
```

Semantics

--times/-t *time-range*

Defines a time-of-day range for the duplication window. Refer to "[time-range](#) (page 4-29)" for a description of the *time-range* placeholder.

day-specifier

Defines the day ranges for the duplication window. Refer to "[day-specifier](#) (page 4-12)" for a description of the *day-specifier* placeholder.

Example

Example 3-97 Setting a Duplication Window

This example sets a duplication window for 9 a.m. to 9:30 a.m. for Tuesdays.

```
ob> setdw -t 0900-0930 tuesday
ob> lsdw
09/30 15:30-16:30:30
weekend 10:00-21:00
Mon Wed-Fri 10:00-20:00
Tue 09:00-09:30
```

3.1.80 setp

Purpose

Use the `setp` command to set the value of a policy. Note that you can reset a value with the [resetp](#) (page 3-97) command.

The policy data is represented as a directory tree with `/` as the root. You can use [cdp](#) (page 2-27) to navigate the tree and [lsp](#) (page 2-157) and `pwdp` to display data.



See Also:

- "[Policy Commands](#) (page 1-18)" for related commands
- [Defaults and Policies](#) (page 7-1) for a complete list of policies and policy classes

When you use the `setp` command to set the port number for an NDMP daemon on Windows, in addition to specifying the port number, you must add an entry in the Windows services file. The Windows services file is called `services` and is located in the `C:\WINDOWS\system32\drivers\etc` directory. [Example 3-99](#) (page 3-143) describes how to set the port number for an NDMP daemon on Windows.

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `setp` command.

Syntax

```
setp::=
```

```
setp policy-name policy-value
```

Semantics

policy-name

Specifies the name of a policy or a class of policies.

policy-value

Specifies the policy value, which is dependent on the policy type.

Example

Example 3-98 Setting Policy Values

This example sets the Web server password to `pandora`, configures the Web server so that it starts automatically, and then sets the [Network Data Management Protocol \(NDMP\)](#) host password to `mehitibel`.

```
ob> pwdp
/
ob> lsp daemons/webpass
webpass (set)
ob> setp daemons/webpass pandora
ob> lsp --nodefault daemons/webauto
webautostart no
ob> setp daemons/webauto yes
ob> lsp --nodefault ndmp/password
password (not set)
ob> setp ndmp/password mehitibel
```

Example 3-99 Setting the Port Number for NDMP Daemons

This example sets the port number for an NDMP daemon on Windows to 9000. Setting the port number on Windows includes the following steps:

1. Set the port number for the NDMP daemon using the `setp` command.
2. Edit the Windows services file and add an entry for the port number.
3. Restart the `observed` daemon.

To set the port number using the `setp` command:

```
ob> setp ndmp/port 9000
ob> lsp -l ndmp/port
port 9000
Default port number via which to connect to an NDMP server
```

To add an entry for the port number in the Windows services file, edit the `C:\WINDOWS\system32\drivers\etc\services` file and include the following entry:

```
ndmp 9000/tcp
```

After changing the port number, you must restart the `observed` daemon using the following commands:

```
net stop observed
net start observed
```

Example 3-100 Setting the Password Lifetime Security Policy

This example sets the global `password lifetime` security policy to 30 days. This specifies that a user password will expire after 30 days. Per-User settings may differ from the global password security settings.

```
ob> setp security/passwordlifetime 30days
ob> lsp --nodefault security/passwordlifetime
passwordlifetime          30 days
```

Example 3-101 Setting the Policy to Cross Mount Points During a File-System Backup

This example sets the `backupoptions` policy and ensures that `obtar` crosses all mount points while performing a file-system backup. By default, `obtar` does not cross mount points.

```
ob> lsp operations/backupoptions
backupoptions             (none)                [default]
ob> setp operations/backupoptions -Xcrossmp
```

Example 3-102 Setting the Certificate Lifetime and Warning Policies

This example sets the `certlifetime` policy, to define the duration of validity of the signing certificates on the current domain, to 3 years. It also sets the `certwarning` policy, that defines the warning notification period before the certificate expires, to 7 days.

```
ob> setp security/certlifetime 3 years
ob> setp security/certlifetime 7 days
ob> lsp security
autocertissue             yes                    [default]
certkeysize               1024                  [default]
certlifetime              3 years
certwarning               7 days
encryptdataintransit     no                    [default]
loginduration             forever
minuserpasswordlen       0
passwordgracetime         10 days
passwordlifetime         30 days
passwordreusetime        180 days
securecomms               yes                    [default]
trustedhosts              yes                    [default]
webinactivitytimeout     15 minutes           [default]
websessiontimeout        24 hours              [default]
```

3.1.81 show

Purpose

Use the `show` command to display the value of one or more variables.

**See Also:**

[obtool Variables](#) (page 5-1) for a complete list of obtool variables

Syntax

```
show::=
```

```
show [ variable-name ]...
```

Semantics***variable-name***

Specifies the name of the variable whose value you want to display. If you do not specify a variable name, then `show` displays all variables that are currently set.

Example**Example 3-103 Showing the Value of a Variable**

This example sets the `drive` variable and then displays the `drive` and `host` variables.

```
ob> show
browsemode    catalog
escape        &
host          osbsvr1
viewmode      inclusive
ob> set drive  tape1
ob> show drive host
drive         tape1
host         osbsvr1
```

3.1.82 stagescan

Purpose

Use the `stagescan` command to run an on-demand stagescan job that will scan the specified device, and create `copyfromstage` jobs to copy backup image instances stored in the device.

Prerequisites**Usage Notes**

- The `stagescan` command will work with disk pool devices that do not have staging enabled.

Syntax

```
stagescan::=
```

```
stagescan {--device/-d devicename}
           {--stagerule/-r stage-rule-name[,stage-rule-name]...}
           [--noage/-a] [--nosize/-s] [--quiet/-q]
           [--priority/-p schedule-priority]
```

Semantics

--device/-d *devicename*

Starts an on-demand stagescan job for backup image instances in the specified stage device. The specified device must be a disk pool, but the disk pool does not have to have staging enabled

stage-rule-name

The name of the Oracle Secure Backup stage rule. An on-demand stagescan job is started that creates copyfromstage jobs for backup image instances that match a stage rule in the list of rules. The stage rules are scanned in the order in which they appear in the list. The default stage rule is not used automatically; it is only used if it appears in the specified list of stage rules.

--noage/-a

If this option is specified, then the minimum copy age (`--mincopyage`) filter value of a stage rule is ignored by this command, and all instances that match all other stage rule parameters are copied.

--nosize/-s

If this option is specified, then the minimum copy size (`--mincopysize`) filter value of a stage rule is ignored by this command, and all instances that match all other stage rule parameters are copied.

--quiet/-q

This option suppresses non-error output.

--priority/-p *schedule-priority*

This option is used to set the stagescan job schedule priority. If this option is not used, then the stagescan job priority defaults to the stagescan/defaultscanjobpriority policy value of 150.

Example

Example 3-104 Running an On-Demand Stagescan Job

The following command copies all instances that have not already been copied in the disk pool `mypool` that match the stage rule `host2rule`. The `mincopysize` and `mincopyage` values in the stage rule are ignored.

```
ob> stagescan --stagerule host2rule --device mypool --nosize --noage
```

3.1.83 unlabelvol

Purpose

Use the `unlabelvol` command to load selected volumes and physically remove the Oracle Secure Backup [volume label](#) and backup data from each of them.

Each [volume](#) has a volume label stored at Beginning of Tape (BOT). The label consists of the [volume ID](#), the [barcode](#) (if any), and other information about the volume. Typically, you use the `unlabelvol` command to remove all traces of a backup and its associated volume label from an unexpired tape and from the Oracle Secure Backup [catalog](#).

 **See Also:**

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `unlabelvol` command.

Syntax

`unlabelvol::=`

```
unlabelvol [ --drive/-D drivename ] [ --force/-f ]
[ --obtaropt/-o obtar-option ]... [ se-range ]
```

Semantics

--drive/-D *drivename*

Specifies the name of the [tape drive](#) to be used to unlabel the volume. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

--force/-f

Forces `obtool` to ignore the [expiration policy](#) for the volume. If the `--force` option is not used and the volume is not expired according to its expiration policy, then `unlabelvol` fails.

se-range

Specifies the range of [storage elements](#) holding the volumes to be unlabeled. If this option is omitted, then the volume currently loaded in the tape drive is unlabeled. Refer to "[se-range](#) (page 4-27)" for a description of the `se-range` placeholder.

Example

Example 3-105 Unlabeling a Volume

This example unlabeled the volume in storage element 1 of tape library `lib1`.

```
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            volume VOL000002, barcode ADE201, oid 110, 16962752 kb remaining
  in  2:            vacant
  in  3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 17017984 remaining,
                    content manages reuse
  in  4:            vacant
  in  iee1:         vacant
  in  iee2:         vacant
  in  iee3:         vacant
  in  dte:          vacant
ob> unlabelvol --force --drive tape1 1
ob> lsvol --library lib1 --long
Inventory of library lib1:
  in  mte:          vacant
  in  1:            unlabeled
  in  2:            vacant
  in  3:            volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 17017984 remaining,
```

```

content manages reuse
in 4:          vacant
in iee1:       vacant
in iee2:       vacant
in iee3:       vacant
in dte:        vacant

```

3.1.84 unloadvol

Purpose

Use the `unloadvol` command to unload a [volume](#) from a [tape drive](#). The unload operation rewinds the tape before moving it to its storage slot.



See Also:

"[Library Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `unloadvol` command.

Syntax

```
unloadvol::=
```

```
unloadvol [ --drive/-D drivename ] [ element-spec ]
```

Semantics

--drive/-D *drivename*

Specifies the name of the tape drive to be unloaded. If you do not specify a tape drive name, then the [drive](#) (page 5-1) variable must be set.

element-spec

Specifies the destination storage element for the volume to be unloaded. Refer to "[element-spec](#) (page 4-14)" for a description of the *element-spec* placeholder. You can specify `vacant` to make Oracle Secure Backup unload the volume to any vacant storage element. If *element-spec* is omitted, then the source (if known) of the volume is used. The source element of the volume in the `dte` is displayed after the string `lastse` when you run `lsvol` (page 2-182).

Example

Example 3-106 Unloading a Volume from a Tape Drive

This example unloads a volume from tape drive `tape1` and inserts it into the source element for the volume. The text `lastse 3` in the `dte` output indicates that the source for the volume is element 3. Note that the sample output has been formatted to fit on the page.

```

ob> lsvol --library lib1 --long
Inventory of library lib1:
in  mte:          vacant

```

```

in 1:          volume VOL000002, barcode ADE204, oid 110, 47670368 kb remaining
in 2:          volume VOL000001, barcode ADE201, oid 102, 48319392 kb remaining
in 3:          vacant
in 4:          vacant
in iee1:       barcode ADE203, oid 114, 47725344 kb remaining, lastse 4
in iee2:       vacant
in iee3:       vacant
in dte:        volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
              remaining, content manages reuse, lastse 3
ob> unloadvol --drive tapel
ob> lsvol --library lib1 --long
Inventory of library lib1:
in  mte:       vacant
in  1:          volume VOL000002, barcode ADE204, oid 110, 47670368 kb remaining
in  2:          volume VOL000001, barcode ADE201, oid 102, 48319392 kb remaining
in  3:          volume RMAN-DEFAULT-000002, barcode ADE202, oid 112, 47725600 kb
              remaining, content manages reuse
in  4:          vacant
in  iee1:       barcode ADE203, oid 114, 47725344 kb remaining, lastse 4
in  iee2:       vacant
in  iee3:       vacant
in  dte:        vacant

```

3.1.85 unmountdev

Purpose

Use the `unmountdev` command to unmount tape volumes manually. When a tape is unmounted, the tape is no longer in a mode in which Oracle Secure Backup can read or write to it. You can use the `mountdev` (page 3-69) command to mount an unmounted tape.

The `unmountdev` command is particularly useful when the `tape drive` is not set to `automount`, which is the recommended, default configuration setting. In special situations the `unmountdev` and `mountdev` (page 3-69) commands provide additional control over your tape drive.



See Also:

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `unmountdev` command.

Syntax

```
unmountdev::=
```

```
unmountdev [ --unload/-u | --norewind/-R ] devicename...
```

Semantics

--unload/-u

Unloads a [volume](#) from the tape drive.

--norewind/-R

Specifies that the tape should not be rewound when Oracle Secure Backup finishes writing to it.

devicename

Specifies the device from which you want to unmount a volume. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example

Example 3-107 Unmounting a Tape Volume

This example unmounts an automounted tape drive called `tape1`.

```

ob> lsdev --long tape1
tape1:
  Device type:          tape
  Model:                [none]
  Serial number:       [none]
  In service:          yes
  Library:             lib1
  DTE:                 1
  Automount:           yes
  Error rate:          8
  Position interval:   3145679KB (-1073791796 bytes) (from driver)
  Debug mode:          no
  Blocking factor:     (default)
  Max blocking factor: (default)
  Current tape:        1
  Use list:            all
  Drive usage:         14 seconds
  Cleaning required:   no
  UUID:                b7c3ala8-74d0-1027-aac5-000cf1d9be50
  Attachment 1:
    Host:               brhost3
    Raw device:         /dev/obt0
ob> unmountdev --norewind tape1
ob> lsdev --mount tape1
drive   tape1          in service
unmounted

```

3.1.86 unresdev

Purpose

Use the `unresdev` command to unreserve a device previously reserved with the [resdev](#) (page 3-96) command.

 **See Also:**

"[Device Commands](#) (page 1-15)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to run the `unmountdev` command.

Syntax

```
unresdev::=
```

```
unresdev { --all/-a | devicename... }
```

Semantics**--all/-a**

Unreserve all devices reserved by the current [Oracle Secure Backup user](#).

devicename

Specifies the name of the device to be unreserved. Refer to "[devicename](#) (page 4-12)" for the rules governing device names.

Example**Example 3-108 Unreserving a Device**

This example unreserves [tape drive](#) `tape1`.

```
ob> lsdev --reserved
   drive 1  tape1           in service
ob> unresdev tape1
ob> lsdev --reserved
ob>
```

3.1.87 unrmsection

Purpose

Use the `unrmsection` command to undo the effect of the [rmsection](#) (page 3-129) command. The command resets the deleted flag in the [backup section](#) records, which you can view by running the [lssection](#) (page 2-170) command.

The `unrmsection` command fails if the [volume](#) containing the selected backup sections has been recycled or unlabeled after all of the backup sections it contains were deleted.

 **See Also:**

"[Section Commands](#) (page 1-20)" for related commands

Prerequisites

You must have the right to [manage devices and change device state](#) (page 8-5) to use the `unrmsection` command.

Syntax

Syntax

`unrmsection::=`

```
unrmsection [ --nq ] [ --oid/-o oid-list ]...[ --vid/-v vid { --file/-f filenumber-list }... ]
```

Semantics

--nq

Does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode](#) (page 1-3)" describes the confirmation message.

--oid *oid-list*

Selects backup sections with the object identifiers matching those in *oid-list*. Refer to "[oid-list](#) (page 4-22)" for a description of the *oid-list* placeholder.

--vid *vid*

Selects backup sections contained on the volume specified by *vid*.

--file/-f *filenumber-list*

Selects the backup sections with the file numbers specified in the list. Refer to "[filenumber-list](#) (page 4-16)" for a description of the *filenumber-list* placeholder.

Example

Example 3-109 Undoing the Deletion of Backup Sections

This example undoes the deletion of two backup sections that have an attribute of deleted.

```
ob> lssection
BSOID Volume          File Sect  Level Client          Created      Attributes
 100 VOL000001          1 1        0 brhost2          03/24.09:52 never expires
 105 RMAN-DEFAULT-000002 1 1        0 osbsvr1          03/24.10:13 deleted
 106 VOL000002          1 1        0 brhost2          03/24.10:13 never expires
 107 VOL000003          1 1        0 brhost2          03/24.10:13 never expires
 108 RMAN-DEFAULT-000002 2 1        0 osbsvr1          03/24.10:14 deleted
 109 VOL000003          2 1        0 brhost2          03/24.11:27 never expires
 110 VOL000003          3 1        0 brhost2          03/24.11:27 never expires
ob> unrmsection --nq --oid 105,108
ob> lssection
BSOID Volume          File Sect  Level Client          Created      Attributes
 100 VOL000001          1 1        0 brhost2          03/24.09:52 never expires
 105 RMAN-DEFAULT-000002 1 1        0 osbsvr1          03/24.10:13 content manages reuse
 106 VOL000002          1 1        0 brhost2          03/24.10:13 never expires
 107 VOL000003          1 1        0 brhost2          03/24.10:13 never expires
 108 RMAN-DEFAULT-000002 2 1        0 osbsvr1          03/24.10:14 content manages reuse
 109 VOL000003          2 1        0 brhost2          03/24.11:27 never expires
 110 VOL000003          3 1        0 brhost2          03/24.11:27 never expires
```

3.1.88 unset

Purpose

Use the `unset` command to undefine a variable.



See Also:

[obtool Variables](#) (page 5-1) for a complete list of obtool variables

Syntax

```
unset::=  
unset variable-name...
```

Semantics

variable-name

Specifies the name of the variable to undefine.

Example

Example 3-110 Undefining a Variable

This example unsets the `drive` variable.

```
ob> show drive  
drive          tape1  
ob> unset drive  
ob> show drive  
drive          (not set)
```

3.1.89 updatehost

Purpose

Use the `updatehost` command to instruct Oracle Secure Backup to complete the inclusion of a host in the [administrative domain](#). Typically, you use this command when you initially configured a host when it was offline.

When you run the [mkhost](#) (page 3-26) or [chhost](#) (page 2-43) command for a host, Oracle Secure Backup exchanges messages with the host to inform it of its state. If you run `mkhost` or `chhost` with the `--nocomm` option because communication with the host is not possible, then the host contains out-of-date configuration information. When the host becomes available, use an `updatehost` command to synchronize the Oracle Secure Backup configuration information between the [administrative server](#) and the host.

**See Also:**

"[Host Commands](#) (page 1-16)" for related commands

Prerequisites

You must have the [modify administrative domain's configuration](#) (page 8-4) right to use the `updatehost` command.

Syntax

```
updatehost::=
```

```
updatehost [ --force/-f ] [--recertify/-r] hostname...
```

Semantics**--force/-f**

Forces an update. The `updatehost` command normally fails if the internal name (UUID) stored on the subject host disagrees with the internal name for the subject stored on the administrative server. This situation arises if the subject host is reassigned to this administrative domain from another domain. To update the subject host regardless of this situation, use `--force`.

--recertify/-r

Recertifies a client host that was earlier decertified and brings it back into the Oracle Secure Backup administrative domain, without destroying the restore catalog data of the client. The host could have been decertified either by using the `obcm decertify` command or by the reinstallation of Oracle Secure Backup. If you remove a client and then add it, the catalog restore data would be destroyed in the process.

**Note:**

The `recertify` option is only available starting with Oracle Secure Backup 10.3.0.2.0.

hostname

Specifies the name of the host to update. This command is useful only for hosts accessed with the Oracle Secure Backup protocol. NDMP hosts do not maintain any Oracle Secure Backup state data and are therefore not applicable to this function.

Examples**Example 3-111 Updating a Host**

This example updates a host that had been offline when it was added with `mkhost` (page 3-26).

```
ob> lshost
brhost2      client                               (via OB)  in service
brhost3      mediaserver,client                   (via OB)  in service
sfsrvr1     client                               (via OB)  not in service
osbsvr1     admin,mediaserver,client             (via OB)  in service
```

```
ob> updatehost sfserver1
ob> pinghost sfserver1
sfserver1: Oracle Secure Backup and NDMP services are available
```

Example 3-112 Recertifying a Host

This example recertifies the host `brhost46`, that was previously decertified using the `obcm decertify` command, and brings it back into the Oracle Secure Backup administrative domain. The commands are run using the `obtool` utility on the administrative server.

```
ob> updatehost --recertify brhost46
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
ob> pinghost brhost46
stadc46: Oracle Secure Backup and NDMP services are available
```

3.1.90 vault

Purpose

Use the `vault` command to perform a one-time on-demand vaulting scan.



See Also:

"[Volume Rotation Commands](#) (page 1-22)" for related commands

Syntax

`vault::=`

```
vault
[ --select/-S select_criterion[, select_criterion]...
[ --quiet/-q ]
[ --at/-a date-time ]
[ --priority/-p schedule-priority ]
[ --restrict/-r restriction[,restriction]... ]
[ --waitfor/-W duration ]
[ --expires/-x duration ] ]...
```

Semantics

--select/-S *select_criterion*

Restricts a vaulting scan to one or more media families.

--quiet/-q

Specifies that neither job ID nor status information is displayed when the vaulting scan job is dispatched to the [scheduler](#).

--at/-a *date-time*

Specifies a date and time to perform the vaulting scan. If a date and time is not specified, then the vaulting scan runs immediately.

See "[date-time](#) (page 4-9)" for more information on the `date-time` placeholder.

--priority/-p *schedule-priority*

Assigns a schedule priority to the vaulting scan.

See "[schedule-priority](#) (page 4-26)" for more information on the *schedule-priority* placeholder.

--restrict/-r *restriction*

Specifies locations to be scanned during the vaulting scan. If the location corresponds to an ACSLS library, then this option also specifies the cartridge access point to be used for media ejection. Restrictions can be specified in any of the following forms:

- *location*
- *location@capname*
- *@capname*

--waitfor/-W *duration*

Specifies the amount of time that Oracle Secure Backup waits for the vaulting job to complete. After the specified time duration is exceeded, Oracle Secure Backup exits from obtool.

See [duration](#) (page 4-14) for more information on the *duration* placeholder.

--expires/-x *duration*

Specifies an expiration time period. Specifying this option expires the vaulting scan if it is not processed by *duration* after the trigger time.

See "[duration](#) (page 4-14)" for more information on the *duration* placeholder.

Example**Example 3-113 Scheduling an On-Demand Vaulting Scan**

This example uses the `vault` command to schedule a one time vaulting scan on November 12 at 5:30 p.m.

```
ob> vault --quiet --at 11/12.5:30:00
ob> lsjob --pending
Job ID          Sched time  Contents                                     State
-----
admin/3         11/12.05:30 volume vaulting scan                       future work
```

3.1.91 vfylibs

Purpose

Use the `vfylibs` command to check the configuration of one or more libraries and drives. You specify which libraries to check, and `vfylibs` checks the drive ID of each tape drive in each of the specified libraries against a list of all defined libraries and drive IDs for all tape drives in those libraries.

Prerequisites

The drives can be open and in use when you run the `vfylibs` command, but `vfylibs` fails if an active robot process is associated with the library.

The `vfylibs` command is not supported for ACSLS libraries.

Usage Notes

For each specified library, `vfylibs` performs the following configuration checks:

1. The device ID (DVCID) for each tape drive in the library is obtained by a Read Element Status command with the DVCID bit set.

 **Note:**

Some libraries, particularly older models, do not support the DVCID bit. The accuracy of the `vfylibs` command is reduced when it encounters libraries of this type.

2. The drive object for each tape drive in the library is fetched.
3. For each attach point specified with this drive object, the drive is opened.
4. An ID for the drive is constructed using SCSI Inquiry commands.
5. The constructed ID is compared with the ID returned with the element status for the tape drive.

The `vfylibs` command checks for and reports the following configuration errors:

- There is no drive object for a library and tape drive number.
- The drive object for a library and tape drive is not in service.
- The drive object for a library and tape drive has no attach points.
- The host for an attach point could not be resolved (host object not found).
- The host for an attach point is not in service.
- The ID obtained through an attach point does not match the ID reported by the library.

 **Note:**

If `vfylibs` finds an ID mismatch, then it also searches the IDs of all drives to see if the incorrect ID matches the ID of a tape drive in some other library.

 **See Also:**

["Device Commands \(page 1-15\)"](#) for related commands

Syntax

`vfylibs::=`

```
vfylibs library_name [ [library_name]... | --all/-a ] [ --verbose/-v ]
```

Semantics

library_name

The name of the library whose configuration you want to check. You can specify multiple library names. Specifying no names at all, which is the same as specifying `--all`, requests verification of all libraries in your configuration.

--verbose/-v

Displays the serial number of the device. If the serial number of an IBM ULTRIUM-DT2 drive is 1110229581, for example, then `vfylibs` displays:

```
IBM      ULTRIUM-TD2      1110229581
```

Examples

Example 3-114 Checking the Configuration of a Tape Library

In this example, the `vfylibs` command runs successfully, and the IDs match:

```
ob> pingd l2
Info: library l2 accessible.
Error: drive l2_t1 is in use by obt on host bkpsrvr04, process 5487.
Error: drive l2_t2 is in use by obt on host bkpsrvr04, process 5513.

ob> vfylib -v l2

collecting dte info...
lib l2 ...
  dte 1: l2_t1 (IBM      ULTRIUM-TD2      1110229581)
  dte 2: l2_t2 (IBM      ULTRIUM-TD2      1110229610)

verifying dte definitions against drive objects...
lib l2 ...
  dte 1 l2_t1 (IBM      ULTRIUM-TD2      1110229581) ...
    att bkpsrvr04:/dev/sg3 ...
    id matches
  dte 2 l2_t2 (IBM      ULTRIUM-TD2      1110229610) ...
    att bkpsrvr04:/dev/sg4 ...
    id matches
0 errors found
```

Example 3-115 Running vftlibs When a Robot Process Is Active

In this example, the `vfylibs` command returns an error because an active robot process is associated with the library:

```
ob> pingd l2
Error: library l2 is in use by obt on host bkpsrvr04, process 5487.
Error: drive l2_t1 is in use by obt on host bkpsrvr04, process 5487.
Error: drive l2_t2 is in use by obt on host bkpsrvr04, process 5513.
ob> vfylib -v

collecting dte info...
Error: library l2 is in use by obt on host bkpsrvr04, process 5487.
0 errors found
```

Example 3-116 Running vfylibs When IDs Do Not Match

In this example, the `vfylibs` command runs successfully but the IDs do not match:

```
ob> vfylib l1 -v

collecting dte info...
  lib l1 ...
    dte 1 [not determined] ...
      getting DVCID: bad id type in DVCID
Error: the following requested library name(s) were not found:
  l1
1 error found
```

4

obtool Placeholders

This chapter describes placeholders shared by multiple obtool commands. A placeholder is italicized text in the syntax diagram for an obtool command that indicates user-specified data.

4.1.1 *aspec*

Description

The *aspec* placeholder represents a physical [attachment](#) for a [tape device](#). The attachment describes a data path between a host and the tape device or disk pool.

Syntax 1

The format for NDMP and SCSI devices is as follows:

aspec::=

```
hostname:rawdevicename[+scsidevice=altrawdevicename][+stdevice=stdevicename]\  
[+stcontroller=stcontroller][+sttarget=sttarget][+stlun=stlun]
```

Note that the backslash (\) is not a literal, but represents line continuation.

Syntax 2

The format for disk pools is as follows:

aspec::=

```
hostname:pathname
```

Syntax 3

The format for an ACSLS servers is as follows:

aspec::=

```
osb_mediaserver_hostname:acsls_server_hostname
```

Restrictions and Usage Notes

The settings other than *hostname* and *rawdevicename* are used only for [Network Data Management Protocol \(NDMP\)](#) servers that run protocol version 2. The requirements to set each of these options are server-specific.

Use the following guidelines when creating attachments:

- For tape devices connected to Linux and UNIX systems, the raw device name is the name of the [device special file](#) that was created when you set up tape devices for use by Oracle Secure Backup. The `installob` and `makedev` tools displayed each such name.

- For Windows systems, the raw device name is the Universal Naming Convention (UNC) name of the device.
- For [Network Attached Storage \(NAS\)](#) systems, the raw device name is a device name assigned by the host operating system (for example, Network Appliance Data ONTAP). You must choose a device name for which no ancillary tape operations, such as rewind or unload, occur either when the [tape drive](#) is opened or when it is closed. These names usually begin or end with the letter "n."

The basic raw device naming convention is `obln` for libraries and `obtn` for tape drives, where *n* is 0 for the first device and increments by one for each subsequent device. Note that the 1 character in `obln` is an alphabet letter and not the numeral 1. [Table 4-1](#) (page 4-2) shows raw device names for popular systems.

Table 4-1 Raw Device Names for Popular Systems

Operating System	Attachment for First Drive	Attachment for First Library
AIX	/dev/obt0	/dev/obl0
Quantum NDMP server	/dev/nst0	/dev/sg0
HP-UX	/dev/obt/0m	/dev/obl/0
Linux	/dev/obt0	/dev/obl0
SGI	/dev/obt2	/dev/obl0
Solaris	/dev/obt	/dev/obl0
Windows	\\./obt0	\\./obl0
Data ONTAP	nrst1a	mc2

Semantics 1

hostname

The name of the host computer to which the device is attached.

rawdevicename

A name assigned by the NDMP server implementer or operating system implementer to represent the device. A *rawdevicename* is the equivalent of a device special file name on UNIX (see [Table 4-1](#) (page 4-2)). Note that the name can include the notation "\$WWN" to refer to the worldwide name of the device.

alrawdevicename

The name of a separate [Small Computer System Interface \(SCSI\)](#) pass-through interface that Oracle Secure Backup must use to pass through SCSI operations to the tape device.

stdevicename

The equivalent device name used when Oracle Secure Backup issues an `NDMP_SCSI_SET_TARGET` message to the server. It specifies an operating system-specific string that identifies the SCSI host bus adapter (HBA) or device.

stcontroller

The SCSI controller index or channel number of the device when `NDMP_SCSI_SET_TARGET` is used.

sttarget

The SCSI bus target ID of the device when `NDMP_SCSI_SET_TARGET` is used.

stlun

The [SCSI LUN](#) of the device when `NDMP_SCSI_SET_TARGET` is used.

Semantics 2**hostname**

The name of the host computer that serves as a repository for backup image instances. The host must be an Oracle Secure Backup host that is configured as a media server. It must also support the NDMP file service extension protocol.

pathname

The name of the file-system directory on the specified host that stores the backups.

Semantics 3**osb_mediaserver_hostname**

The name of the host computer that is configured as a media server in the Oracle Secure Backup administrative domain.

acsls_server_hostname

The name of the host computer that is configured as the ACSLS server.

Example**Example 4-1 aspec**

Sample values for `aspec` include the following:

```
w0x0f:/dev/obt0    # a tape drive connected to Linux host w0x0f
darth:/dev/obl0   # a tape library connected to Solaris host darth
ethel:nrst0a      # a tape drive connected to NetApp filer ethel
winserv:\\.\obl0  # a tape library connected to Windows media server winserv
//winserv/obl0    # equivalent to the preceding aspec
```

4.1.2 authtype

The `authtype` placeholder specifies an authorization type, which is the mode in which Oracle Secure Backup authenticates itself to the [Network Data Management Protocol \(NDMP\)](#) server. Typically, you should use the `negotiated` default setting. You can change the setting if necessary; for example, if you have a malfunctioning NDMP server.

Syntax**authtype::=**

```
none | negotiated | text | md5
```

Semantics

none

Oracle Secure Backup sends the NDMP server an `authorize client` message specifying NDMP's `none` authentication mode. Most servers do not accept this type of authentication.

negotiated

Oracle Secure Backup determines (with the NDMP server) the best authentication mode to use. This is the default setting for the NDMP default and policies value.

text

Oracle Secure Backup uses plain, unencrypted text to authenticate.

md5

Oracle Secure Backup uses the MD5 digest algorithm to authenticate.

4.1.3 backup-container

Description

The `backup-container` placeholder specifies a backup container to store the backup images and backup image instances. This can be the volume ID of a tape volume or the name of a disk pool.

Syntax

backup-container::=

`backup-container`

Semantics

backup-container

Specifies the name of the backup container. This can be the name of a disk pool or tape volume.

4.1.4 backup-level

Description

The `backup-level` placeholder specifies the level of a backup created with the `backup` (page 2-4) command.

Syntax

backup-level::=

`full | incr_level | incr | offsite`

incr_level::=

`1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9`

Semantics

full

Specifies that Oracle Secure Backup should back up all files defined in a [dataset](#) regardless of when they were last backed up. This option is equivalent to level 0. This is the default value.

incr_level

Specifies an incremental level from 1 to 9 and backs up only those files that have changed since the last backup at a lower level.

incr

Specifies that Oracle Secure Backup should back up any file that has been modified since the last [incremental backup](#) at the same level or lower. The `incr` option is equivalent to level 10. This level is platform-dependent and is incompatible with some client operating systems such as the Netapp [filer](#) Data ONTAP.

offsite

Equivalent to a full (level 0) backup except that Oracle Secure Backup keeps a record of this backup in such a way that it does not affect the full or incremental [backup schedule](#). This option is useful when you want to create a [backup image](#) for offsite storage without disturbing your schedule of incremental backups.

4.1.5 concjobs

Description

Specifies the maximum number of jobs that can be run concurrently for a particular disk pool or cloud storage device.

Syntax

```
concjobs::=  
n | unlimited
```

Semantics

n

Specifies a number that is greater than or equal to 1.

unlimited

There is no limit on the number of concurrent jobs for a disk pool or cloud storage device.

4.1.6 content

Description

The `content` placeholder represents the type of backup content in a [database backup storage selector](#).

Syntax

content::=

archivelog | full | incremental | autobackup

Semantics

archivelog

Backs up or restores database archived redo logs.

full

Backs up or restores the database files, regardless of when they were last backed up. This option is identical to a level 0 backup.

incremental

Backs up or restores only data that has been modified since the last backup, regardless of the [backup level](#).

autobackup

Backs up or restores control files.

4.1.7 data-selector

Description

The *data-selector* placeholder represents Oracle Secure Backup [catalog](#) data that is selected based on user-specified values.

Syntax

data-selector::=

latest | earliest | all | *backup-id* | *date-time* | *date-range*

Semantics

latest

Most recent. If the following conditions are met, then Oracle Secure Backup includes all backups on which the incremental is dependent up to and including the preceding [full backup](#):

- The file-system object is a directory.
- The most recent instance is an [incremental backup](#).

earliest

Least recent. If the file-system object is a directory, then Oracle Secure Backup selects the instance of the directory and its contents found in the earliest full backup.

all

All instances.

backup-id

The specific instance contained in the [backup image](#) section identified by *backup-id*. The [backup ID](#) is a small integer assigned by obtool for reference purposes only.

date-time

The file-system object as it existed in a backup no later than the given *date-time* (see "[date-time](#) (page 4-9)"). If the file-system object is a directory, and if the most recent instance is an incremental backup, then Oracle Secure Backup includes all predicates (backups on which the incremental is dependent) up to and including the preceding full backup.

date-range

All objects backed up exactly between the two specified *date-time* values (see "[date-range](#) (page 4-8)"). Unlike the single *date-time* expression, Oracle Secure Backup gives no special consideration to incremental backups of directories.

4.1.8 dataset-dir-name

Description

The *dataset-dir-name* placeholder specifies the name of a [dataset directory](#). Like Windows and UNIX file systems, Oracle Secure Backup dataset files are organized in a naming tree on the [administrative server](#). A dataset directory is a directory that contains dataset files. Dataset directories can have a hierarchy of nested subdirectories that is up to 10 levels deep.

Syntax

dataset-dir-name::=

dataset-dir-name

Semantics**dataset-dir-name**

Specifies the name of a dataset directory. Dataset directory names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

Standard notation for directory paths applies to dataset directories. For example, a single period (.) specifies the current directory and two consecutive periods (..) specifies one level higher than the current directory.

4.1.9 dataset-file-name

Description

The *dataset-file-name* placeholder specifies the name of a [dataset file](#). As described in "[dataset-dir-name](#) (page 4-7)", dataset files are organized in a directory tree.

Syntax

dataset-file-name::=

dataset-file-name

Semantics

dataset-file-name

Specifies the name of a dataset file. Dataset file names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

4.1.10 dataset-name

Description

Specifies the name of a [dataset directory](#) or [dataset file](#).

Syntax

dataset-name::=

dataset-file-name | *dataset-dir-name*

Semantics

"[dataset-dir-name](#) (page 4-7)" describes the *dataset-dir-name* placeholder. "[dataset-file-name](#) (page 4-7)" describes the *dataset-file-name* placeholder.

4.1.11 date-range

Description

The *date-range* placeholder represents a range of dates in a *data-selector*.

Syntax

date-range::=

date-time-date-time

Semantics

Refer to "[date-range](#) (page 4-8)" for a description of the *date-time* placeholder. Note that the formats of the beginning and end of the *date-range* are not required to be parallel. For example, you can express the time in the beginning of the range and then omit the time in the end of the range.

Example

Sample values for *date-range* include the following:

```
2013/1/1-2013/1/31
5/25.08:00:00-5/25.08:30:00
2012/03/01-05/3/2.22:00:00
```

4.1.12 date-time

Description

The *date-time* placeholder represents a date and time.

Syntax

date-time::=

```
[year/]month/day[.hour][:minute][:second]
```

Semantics

year

Specifies a one-digit, two-digit, or four-digit year number. If *year* is absent, then the current year is assumed unless explicitly documented otherwise.

month

Specifies a one-digit or two-digit month number.

day

Specifies a one-digit or two-digit day number.

hour

Specifies a one-digit or two-digit hour number. Hours are represented in military format.

minute

Specifies a one-digit or two-digit minute number.

second

Specifies a one-digit or two-digit second number.

Example

Example 4-2 date-time

Sample values for *date-time* include the following:

```
2012/1/1  
5/25.08:30:00  
2/2  
10/16.1:15
```

4.1.13 day-date

Description

The *day-date* placeholder identifies a day or group of days.

Syntax

day-date::=

```
weekday-expr | relative-weekday-expr |
day n { each month | each quarter | each year } | year/month/day | month/day |
month/day each quarter
```

weekday-expr::=

```
weekday-name | weekday-aggregate | weekday-range [ weekday-name |
weekday-aggregate | weekday-range ]...
```

weekday-name::=

```
monday[s] | tuesday[s] | wednesday[s] | thursday[s] | friday[s] |
saturday[s] | sunday[s]
```

weekday-aggregate::=

```
daily | weekend[s] | weekday[s]
```

weekday-range::=

```
weekday-name-weekday-name
```

relative-weekday-expr::=

```
[ weekday-ordinal weekday-name ]... |
[ { weekday_name }... except weekday-ordinal ]... |
[ { weekday_name }... [ except ] { before | after } weekday-ordinal weekday-
name ]...
```

weekday-ordinal::=

```
first | second | third | fourth | fifth | last
```



Note:

Any day-date string with embedded spaces must be enclosed in double quotation marks.

Semantics

weekday-expr

Identifies one or more weekdays independently of where they occur in a month. If you specify multiple weekday expressions, then they must be individually separated by spaces and collectively enclosed with double quotation marks. To specify Monday, Wednesday, and Friday, for example, use "monday wednesday friday". Mixed expressions are permitted, but they must be enclosed by double quotation marks. To specify Wednesdays and weekends, for example, use "wednesday weekend". Weekday ranges must run from earlier to later in the week. For example, sunday-friday is permitted but not thursday-tuesday.

 **Note:**

Oracle Secure Backup for Windows does not support mixed-case or uppercase weekday names. Specifying `Monday` or `MONDAY` as a weekday name, for example, returns an error.

relative-weekday-expr

Identifies one or more weekdays based on where they occur in a month.

weekday-ordinal weekday-name

Identifies weekdays by the order in which they occur in the month.

weekday-name except weekday-ordinal

Identifies weekdays by name, but excludes those that fall within the specified order.

day-of-week [except] {before | after} weekday-ordinal weekday-name

Identifies specific weekdays that fall before or after another day, or weekdays except those that fall before or after another day.

day n each {month | quarter | year}

Identifies the *n*th ordinal day of each month, quarter, or year. There are 92 days in a quarter; day 92 is considered last even if there are fewer days in the quarter.

year/month/day

Identifies the specified day only once.

month/day

Identifies the specified day every year.

month/day each quarter

Identifies the day of the given relative month (1, 2, or 3) in every calendar quarter.

Examples**Example 4-3 day-date**

Sample values include the following:

```
daily
tuesdays
"monday wednesday friday"
"monday-thursday saturday"
"wednesday weekends"
"last saturday"
"second thursday third sunday"
"thursday friday saturday except first"
"saturday except third"
"saturday sunday after first friday"
"weekdays before last saturday"
"weekends except after last friday"
"monday wednesday except before first sunday"
"day 4 each month"
"day 31 each quarter"
"day 90 each year"
2012/12/25
12/25
"3/1 each quarter"
```

4.1.14 day-specifier

Description

The *day-specifier* placeholder represents a range of time in terms of days.

Syntax

day-specifier::=

year/month/day | *month/day* | *wday* | *wday-wday* | *weekday[s]* | *weekend[s]* | *daily* | *today* | *yesterday*

wday::=

sunday[s] | *monday[s]* | *tuesday[s]* | *wednesday[s]* | *thursday[s]* | *friday[s]*
| *saturday[s]*

Semantics

"[day-date](#) (page 4-9)" describes the possible values for the placeholders *year*, *month*, and *day*.

4.1.15 devicename

Description

The *devicename* placeholder specifies the name of a [tape library](#), [tape drive](#), or disk pool. The [tape device](#) name must be unique among all Oracle Secure Backup device names. It is unrelated to any other name used in your computing environment or the Oracle Secure Backup [administrative domain](#). The disk pool name must be unique within the Oracle Secure Backup administrative domain.

Syntax

devicename::=

devicename

Semantics

devicename

Specifies the name of a tape drive, tape library, or disk pool. Device names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

4.1.16 dupevent

Description

The volume-specific event that determines when the duration specified in a duplication policy begins to elapse. A duplication job is scheduled only if one of these events occurs at the first [active location](#), because duplication takes place only at the first active location.

Syntax

dupevent::=

firstwrite | lastwrite | windowclosed | nonwritable | firstmove

Semantics

firstwrite

The point at which the first write to a [volume](#) occurs.

lastwrite

The point at which the last write to a volume occurs.

windowclosed

The point at which the [write window](#) closes.

nonwritable

The point at which a volume can no longer be written to, either because the write window has closed or because the volume is full.

firstmove

The point at which volume becomes eligible to move from its first active location.

See Also:

- ["event \(page 4-15\)"](#)
- ["duration \(page 4-14\)"](#)
- ["mkdup \(page 3-24\)"](#)

4.1.17 duplicationrule

Description

A duplication rule, in the form *media-family:number*.

Syntax

duplicationrule::=

mediafamily: number

Semantics

mediafamily

Identifies the [media family](#) for this duplication rule.

number

Specifies the number of duplicates to be created for the specified media family.

4.1.18 duration

Description

The *duration* placeholder represents a length of time.

Syntax

duration::=

```
forever | disabled | number{s[econds] | mi[nutes] | h[ours] | d[ays] | w[EEKS] |  
mo[nths] | y[ears]}
```

Semantics

forever

Specifies that the duration is unlimited.

disabled

Specifies no duration. This value is not legal for the `--waittime` option in database storage selectors.

number

Specifies the duration in terms of an integer value of temporal units. To avoid quoting you cannot include a space between *number* and the value that follows it. For example, `3days` is a legal value, but `3 days` is not. The value `3 " days"` is valid.

Example

Example 4-4 duration

Examples of *duration* values include the following:

```
10minutes  
forever  
30 " sec"  
1y
```

4.1.19 element-spec

Description

The *element-spec* placeholder represents the name of a [tape library](#) element.

Syntax

element-spec::=

```
se-spec | ieen | dten
```

Semantics

se-spec

Specifies the number of a storage element in the tape library. Refer to the description of *se-spec* in "[se-spec](#) (page 4-27)".

ieven
Specifies the import/export element *n*.

dten
Specifies [tape drive](#) *n*.

4.1.20 event

Description

The volume-specific event that determines when the duration specified in a rotation rule begins to elapse. Some events are valid only at an [active location](#), and other events are valid only at a [storage location](#).

Syntax

event::=

`firstwrite | lastwrite | windowclosed | nonwritable | arrival | expiration`

Semantics

firstwrite

The point at which the first write to a [volume](#) occurs. This value is valid only at active locations.

lastwrite

The point at which the last write to a volume occurs. This value is valid only at active locations.

windowclosed

The point at which the [write window](#) closes. This value is valid only at active locations.

nonwritable

The point at which a volume can no longer be written to, either because the write window has closed or because the volume is full. This value is valid only at active locations.

arrival

The point at which the volume arrives at a storage location. This value is valid only at storage locations.

expiration

The point at which a volume expires. This value is valid only at storage locations.

See Also:

- "[dupevent](#) (page 4-12)"
- "[duration](#) (page 4-14)"
- "[rotationrule](#) (page 4-26)"

4.1.21 filename

Description

The *filename* placeholder identifies ordinal position of the [backup image](#) within the [volume set](#).

Syntax

filename::=

filename

Semantics

filename

Specifies the file number. The first backup image instance of each volume set is file number 1.

4.1.22 filename-list

Description

The *filename-list* placeholder represents one or more ordinal *filename* values.

Syntax

filename-list::=

filename[,filename]... | filename-filename

Semantics

Refer to "[filename](#) (page 4-16)" for a description of the *filename* placeholder.

4.1.23 iee-range

Description

The *iee-range* placeholder represents a range of import/export elements. The elements need not be continuous.

Syntax

iee-range::=

vacant | none | iee-subrange[,iee-subrange]...

iee-subrange::=

iee-spec-iee-spec | iee-spec[,iee-spec]...

Semantics

Refer to "iee-spec (page 4-17)" for a description of the placeholders and keywords in the *iee-range* syntax. The dash in *iee-spec-iee-spec* expresses an inclusive range of elements.

Example

Example 4-5 iee-range

Examples of *iee-range* values include the following:

```
iee1  
iee1-iee3  
iee1,iee3,iee7-iee9  
vacant  
none
```

4.1.24 iee-spec

Description

The *iee-spec* placeholder represents the number of an import/export storage element in a [tape library](#).

Syntax

iee-spec::=

```
[iee]n | none | vacant
```

Semantics

[iee]n

where *n* is a number ranging from 1 to the maximum number of import/export elements in the tape library.

Elements are referenced by their abbreviation (*iee*) followed by the number of the element, for example, *iee2*. When multiple elements of a particular type exist, element numbering starts at 1. When there is only one element of a type, the number can be omitted: *iee1* and *iee* both refer to the first and only import/export element.

none

Indicates no import/export element.

vacant

Indicates any empty import/export element.

4.1.25 job-type

Description

The type of an Oracle Secure Backup job.

Syntax

job-type::=

dataset | backup | restore | orabackup | orarestore | scan |
mediamovement | duplication | oraparent | catimport | copyinstance | copyfromstage
| stagescan

Semantics

dataset

A [dataset](#) job is a backup of a specified dataset. Oracle Secure Backup assigns a dataset job an identifier consisting of the username of the logged in [Oracle Secure Backup user](#), a slash, and a unique numeric identifier. An example of a dataset job identifier is `admin/15`.

backup

For each dataset job, Oracle Secure Backup creates one subordinate job for each host that it includes. Oracle Secure Backup assigns each [backup job](#) an identifier whose prefix is the parent (dataset) job id, followed by a dot (`.`), then followed by a unique small number. An example of a backup job identifier is `admin/15.1`.

restore

Oracle Secure Backup creates a restore job for each [backup image](#) that must be read to initiate a restore operation. Oracle Secure Backup assigns each job an identifier consisting of the logged in username, a slash, and a unique numeric identifier. An example of a restore job identifier is `admin/16`.

orabackup

Oracle Secure Backup creates an Oracle backup job when the [Recovery Manager \(RMAN\) BACKUP](#) command backs up database files. This job attaches to a parent job whose identifier is created by an Oracle Secure Backup user name, a slash, and a numeric identifier. The Oracle Secure Backup user name is the one that the operating system user is preauthorized to assume (see the `--preauth` option of the [mkuser](#) (page 3-64) command). An example of a parent job identifier is `sbt/15`.

The job identifier of an Oracle backup job is created by using the job identifier of the parent job followed by a dot and a unique numeric identifier to identify each subordinate job. An example of an Oracle backup job identifier is `sbt/15.1`.

orarestore

Oracle Secure Backup creates an Oracle restore job when the [Recovery Manager \(RMAN\) RESTORE](#) command restores database files from a backup image instance. This job attaches to a parent job whose identifier is created by an Oracle Secure Backup user name, a slash, and a numeric identifier. The Oracle Secure Backup user name is the one that the operating system user is preauthorized to assume (see the `--preauth` option of the [mkuser](#) (page 3-64) command). An example of a parent job identifier is `sbt/16`.

The job identifier of an Oracle restore job is created by using the job identifier of the parent job followed by a dot and a unique numeric identifier to identify each subordinate job. An example of an Oracle restore job identifier is `sbt/16.1`.

scan

A scan job runs at a time specified by the backup administrator and scans the volumes [catalog](#) to determine which volumes are eligible for media movement or duplication jobs. The scan occurs on a location-by-location basis. These media

movement and duplication jobs run in specified media movement or duplication windows and when resources are available.

mediamovement

A media movement job specifies that media should be moved from one [location](#) to another, to satisfy its associated [rotation policy](#) or when recalled from a [storage location](#).

duplication

A duplication job specifies that media should be duplicated in accordance with its associated duplication policy.

oraparent

Oracle Secure Backup creates an Oracle backup job when the Recovery Manager (RMAN) `BACKUP` command backs up database files. A parent job is identified by an Oracle Secure Backup user name, a slash, and a numeric identifier. The Oracle Secure Backup user name is the one that the operating system user is preauthorized to assume. An example of a parent job identifier is `sbt/16`.

The `oraparent` is the parent job associated with the `orabackup` job.

catimport

Oracle Secure Backup creates a catalog import job when the `catalog` command is used to import catalog information from all the backup image instances in a backup container. When this job completes, the catalog is updated with the metadata imported from the specified backup container.

copyinstance

Oracle Secure Backup creates a copy instance job when a `cpinstance` command to create a copy of a backup image instance. Each copy instance job is assigned a unique identifier and can be run either immediately or at a later time.

copyfromstage

A `copyfromstage` job copies the backup image instances created by a stage source job to a destination container. A `copyfromstage` job inherits policies from `cpinstance` policies.

stagescan

A `stagescan` job is launched by either a `stagescan` schedule or an on-demand `stagescan` command. A `stagescan` job scans and filters the backup image instances in one or more stage disk pool devices. Instances that match a stage-rule that is attached to the device are grouped and copied by a `copyfromstage` job created by the `stagescan` job. A `stagescan` job can create zero or more `copyfromstage` jobs.

4.1.26 name-format

Description

The `name-format` placeholder specifies the format used for naming backup images.

Valid values for names include upper case alphabets, lower case alphabets, digits, hyphen, underscore, or a period. These can be combined with the name format variables `%H`, `%T`, `%t`, `%R`, `%d`, or `%S`.

If you do not explicitly specify a name format, Oracle Secure Backup uses `%H-%T-%t`. For example, if a backup is created on the host `brhost2` at 10:23:46 on 04/12/2013, then the name used for the backup image is `brhost2-102346-20130412`.

Syntax

name-format::=

%H | %T | %t | %R | %d | %S

Semantics

%H

Specifies the name of the host.

%T

Specifies the date when backup was created in *yyyymmdd* format.

%t

Specifies the time when backup was created in *hhmmss* format

%R

Specifies the name of the Oracle Secure Backup user who created the backup job. This is applicable only for on-demand backups.

%d

Specifies the name of the Oracle Database. This is applicable only for RMAN backups.

%S

Specifies the name of the dataset that contained details about the directories backed up. This is applicable only for file-system backups.

4.1.27 ndmp-backup-type

Description

The *ndmp-backup-type* placeholder specifies the type of [Network Data Management Protocol \(NDMP\)](#) backup for certain [Network Attached Storage \(NAS\)](#) devices.

The placeholder values are specific to NDMP filer vendors so check the applicable backup type with your filer vendor.



Note:

The value specified for *ndmp-backup-type* is case-sensitive. You must use lowercase while specifying the NDMP backup type.

Syntax

ndmp-backup-type::=

dump | image | zfs

Semantics

dump

This mode runs backups less quickly, dumps the `/usr/store` file system in tar format, and permits selective restore of individual user mailboxes.

image

This mode runs backups quickly and dumps the whole `/usr/store` file system. Only complete file-system restore operations are possible.

zfs

This mode runs backups that are specific to the Oracle ZFS Storage Appliance.

4.1.28 numberformat

Description

The `numberformat` placeholder specifies the format in which to display large numbers. If `numberformat` is not specified, then `obtool` uses the value of the `numberformat` (page 5-4) variable. If this variable is unset, then the default is `friendly`.

Syntax

numberformat::=

`friendly` | `precise` | `plain`

Semantics

friendly

Specifies this keyword to display large values in KB, MB, and so on.

precise

Specify this keyword to display precise values with commas.

plain

Specify this keyword to display precise values without commas.

4.1.29 oid

Description

The `oid` placeholder represents the `catalog` identifier of a `volume`, `backup image` section, or `backup piece` record. You can obtain an `oid` in the following ways:

- Run the `lsvol` (page 2-182) command to display the `volume ID` (VOID) for a volume.
- Run the `lsbu` (page 2-122) command to display the `backup ID` for a `backup section`.
- Run the `lspiece` (page 2-160) command with the `--long` option to display the backup piece OID for a backup piece.

Syntax

oid::=

oid

Semantics

oid

Specifies the object identifier. Within the Oracle Secure Backup catalog, Oracle Secure Backup identifies each backup image section with a numeric backup ID. Oracle Secure Backup assigns backup IDs without regard to the time order of backups. For example, backup ID 25 can represent a Monday backup whereas backup ID 6 represents a backup on the following day.

4.1.30 oid-list

Description

The *oid-list* placeholder represents one or more [catalog](#) identifiers. The *oid* placeholder represents a catalog identifier.

Syntax

oid-list::=

oid[,oid]... | oid-oid

Semantics

Refer to "[oid](#) (page 4-21)" for a description of the *oid* placeholder. The dash in *oid-oid* expresses an inclusive range of *oid* values.

Example

Example 4-6 oid-list

The following examples show valid values for *oid-list*:

```
3,42,16  
1-5
```

4.1.31 policyname

Description

Specifies the name of a duplication or [rotation policy](#).

See also:

- "[Volume Duplication Commands](#) (page 1-22)"
- "[Rotation Policy Commands](#) (page 1-20)"

Syntax

policyname::=

string

Semantics

The string represents a name for a duplication or rotation policy.

4.1.32 preauth-spec

Description

The *preauth-spec* placeholder defines an operating system user who is preauthorized to access Oracle Secure Backup.

Syntax

preauth-spec::=

hostname[:os-username[:windows-domain]]+preauth-attr[+preauth-attr]...

Semantics

hostname

This placeholder specifies the host for the operating system user who has preauthorized access to Oracle Secure Backup. Use an asterisk character (*) as a [wildcard](#) to indicate all hosts in the [administrative domain](#).

os-username

This placeholder grants the specified operating system preauthorized access to Oracle Secure Backup. If you specify *os-username* as a Windows account name, then you must explicitly state the *windows-domain* name either as a wildcard or a specific name. Use an asterisk character (*) as a wildcard to indicate all operating system users on the host. By default, all users on the specified host are preauthorized.

windows-domain

This placeholder specifies the Windows domain of *hostname*. This placeholder is only applicable to preauthorized logins from a Windows host. Use an asterisk character (*) as a wildcard to indicate all Windows domains. By default, preauthorized access on the specified host is permitted for all Windows domains.

preauth-attr

Defines the Oracle Secure Backup resources to which the preauthorized operating system user has access. You can specify the following values:

- `rman`
This value preauthorizes Oracle Database SBT backups through [Recovery Manager \(RMAN\)](#). If a matching [preauthorization](#) cannot be found for a given SBT request, then the request fails.
- `cmdline`

This value preauthorizes login through the user-invoked Oracle Secure Backup command-line utilities.

Example

Example 4-7 preauth-spec

```
obhost1+rman
obhost2:jblogg+rman+cmdline
obhost2*:Win-domain+rman
*:jblogg:#+cmdline
```

4.1.33 produce-days

Description

The *produce-days* placeholder specifies days of the week on which a summary report is to be produced.

Syntax

produce-days::=

weekday-name | daily | weekday | weekend

weekday-name::=

monday[s] | tuesday[s] | wednesday[s] | thursday[s] | friday[s] |
saturday[s] | sunday[s]

Semantics

The values are self-explanatory.

4.1.34 protover

Description

The *protover* placeholder represents a [Network Data Management Protocol \(NDMP\)](#) protocol version. Typically, you can allow Oracle Secure Backup to choose the highest protocol version that the server can use to communicate. If it is necessary for testing or some other purpose, then you can change the NDMP protocol version with which Oracle Secure Backup communicates with this server. If an NDMP server cannot communicate using the protocol version you select, then Oracle Secure Backup reports an error rather than using a mutually supported version.

Syntax

protover::=

version_number

Semantics

version_number

Specifies the protocol version number. Valid values are 2, 3, 4, and null (""), which means "as proposed by server". The default is null.

4.1.35 restriction

Description

The *restriction* placeholder specifies the restriction of an operation to a tape, disk pool, or cloud storage device. When multiple tape device restrictions are specified in a list, Oracle Secure Backup selects a tape device from only one of them.

If the backup target is a cloud storage device, then the device must be specified because Oracle Secure Backup never backs up to a cloud storage device by default.

Syntax

restriction::=

devicename | *@hostname* | *devicename@hostname*

Semantics

devicename

Uses the specified tape, disk pool, or cloud storage device.

@hostname

Uses any tape device attached to the host with the name *hostname*.

devicename@hostname

Uses any tape, disk pool, or cloud storage device attached to the host with the name *hostname*. Preference is given to tape when there are multiple device types attached to the host.

4.1.36 role

Description

The *role* placeholder represents a host role in an [administrative domain](#).

Syntax

role::=

admin | *client* | *mediaserver*

Semantics

admin

Specifies the host computer in your administrative domain that contains a copy of Oracle Secure Backup software and the catalogs that store configuration settings and backup history.

client

Specifies a host computer whose locally-accessed data are backed up by Oracle Secure Backup. Most computers defined within the administrative domain are [client](#) hosts.

mediaserver

Specifies a host computer that has one or more secondary storage devices, such as tape libraries, connected to it.

4.1.37 rotationrule

Description

The *rotationrule* placeholder specifies how long a **volume** stays at a particular **location**, as part of a **rotation policy**.

Syntax**rotationrule::=**

```
locationname[:event[:duration]]
```

Semantics**locationname**

The name of an existing location object.

event

The volume-specific event that determines when the duration specified in the rotation rule begins to elapse.

**See Also:**

"[event](#) (page 4-15)" for more information on the *event* placeholder

duration

The length of time after the event that the media remains at the location specified in this rotation rule.

**See Also:**

"[duration](#) (page 4-14)" for details about valid values

4.1.38 schedule-priority

Description

The *schedule-priority* placeholder specifies a schedule priority for a backup, restore, vaulting scan, or **volume** duplication scan job. The priority for a job is a positive numeric value.

The foremost decision criterion that the **scheduler** uses to perform a job (after the earliest time to run this job has arrived) is the schedule priority. The scheduler dispatches higher priority jobs over lower priority ones, providing all resources required to run the job are available. For example, if twenty jobs are in the scheduler and ready

for execution, then Oracle Secure Backup runs the job with the lowest numeric schedule priority.

Syntax

schedule-priority::=

priority_num

Semantics

priority_num

Specifies a positive numeric value. The lower the value, the greater the priority assigned to the job by the scheduler. The default schedule priority is 100. Priority 1 is the highest priority that you can assign to a job.

4.1.39 se-range

Description

The *se-range* placeholder represents a range of [storage elements](#). The elements need not be continuous.

Syntax

se-range::=

all | none | *se-subrange*[,*se-subrange*]. . .

se-subrange::=

se-spec | *se-spec-se-spec*

Semantics

Refer to "[se-spec](#) (page 4-27)" for a description of the *se-spec* placeholder. The dash in *se-spec-se-spec* expresses an inclusive range of *se-spec* values.

Example

Example 4-8 se-range

Examples of *se-range* values include the following:

```
1
1-2
1,3,5,se10-se30
all
none
```

4.1.40 se-spec

Description

The *se-spec* placeholder represents the number of a storage element in a [tape library](#).

Syntax

se-spec::=

[se]*n* | none | vacant

Semantics

[se]*n*

where *n* is a number ranging from 1 to the maximum number of [storage elements](#) in the tape library.

Elements are referenced by their abbreviation (*se*) followed by the number of the element, for example, *se5*. When multiple elements of a particular type exist, element numbering starts at 1. When there is only one element of a type, you can omit the number: *se1* and *se* both refer to the first and only storage element. If you omit the abbreviation, then a storage element is assumed. For example, *se4* and 4 both refer to the fourth storage element.

none

Indicates no storage element.

vacant

Indicates any empty storage element. Specify *vacant* only if the [tape drive](#) is known to be loaded.

4.1.41 size-spec

Description

The *size-spec* placeholder specifies the size of disk pools.

Syntax

size-spec::=

0 | *n* [KB | MB | GB | TB | PB | EB]

Semantics

n

The numeric value that indicates the size of a disk pool. Use one of the following values to specify the unit of the disk pool size: KB, MB, GB, TB, PB, or EB.

0

Specifies that the size of the disk pool is limited only by the size of the underlying file-system that hosts the disk pool.

4.1.42 summary-start-day

Description

The *summary-start-day* placeholder specifies the first day of the week for which summary data is to be produced.

Syntax

summary-start-day::=

weekday-name | yesterday | today

weekday-name::=

monday[s] | tuesday[s] | wednesday[s] | thursday[s] | friday[s] |
saturday[s] | sunday[s]

Semantics

The values are self-explanatory.

4.1.43 time

Description

The *time* placeholder identifies a time in terms of hours, minutes, and (optionally) seconds. Hours are expressed in 24-hour military format.

Syntax

time::=

hhmm | *h[h]:mm* | *h[h]:mm:ss*

Semantics

h

Indicates a one-digit hour number, for example, 3 (which represents 3 a.m.).

hh

Indicates a two-digit hour number, for example, 22 (which represents 10 p.m.).

mm

Indicates a two-digit minute number, for example, 30.

ss

Indicates a two-digit second number, for example, 59.

Example

Example 4-9 time

Sample values for *time* include the following:

```
8:00  
2250  
14:35:30
```

4.1.44 time-range

Description

The *time-range* placeholder represents a time-of-day range.

Syntax

time-range::=

start-time-end-time

Semantics

"[time](#) (page 4-29)" describes the formats for the *start-time* and *end-time*. The dash in *start-time-end-time* expresses an inclusive range of times.

Example

Example 4-10 time-range

The time range is local-time based and takes into account Daylight Savings Time, if it applies to your locale. Sample values for *time-range* include the following:

```
08:00:00-08:30:00
1430-1530
1430-14:35:30
```

4.1.45 vid

Description

The *vid* placeholder represents a unique alphanumeric identifier assigned by Oracle Secure Backup when the [volume](#) was labeled.

Syntax

vid::=

vid

Semantics

vid

Specifies an identity for a volume. The [volume ID](#) usually includes the [media family](#) name of the volume, a dash, and a unique [volume sequence number](#). For example, a volume ID in the `RMAN-DEFAULT` media family could be `RMAN-DEFAULT-000002`. A *vid* can contain up to 31 characters, in any combination of alphabetic and numeric characters, but the last 6 characters must be numeric.

4.1.46 vol-range

Description

The *vol-range* placeholder represents a list of volumes in a [tape library](#). You can specify a [volume ID](#) list or a [barcode](#) list.

Syntax

vol-range::=

```
--volume/-v vid[,vid]... | --barcode/-b tag[,tag]...
```

Semantics

"[vid](#) (page 4-30)" describes the format for the *vid* placeholder.

Example

Example 4-11 vol-range

Sample values for *vol-range* include the following:

```
--volume VOL000001,VOL000002,VOL000005  
--barcode ADE210,ADE202
```

4.1.47 vol-spec

Description

The *vol-spec* placeholder represents the specification of a [volume](#) in a [tape library](#).

Syntax

vol-spec::=

```
--volume/-v vid | --barcode/-b tag
```

Semantics

"[vid](#) (page 4-30)" describes the format for the *vid* placeholder.

4.1.48 vol-status

Description

The *vol-status* placeholder represents the current status of a volume and whether it is available for backup and restore operations.

Syntax

vol-status::=

```
usable | readonly | out-of-service
```

Semantics

usable

Indicates that the volume can be used for any operation.

readonly

Indicates that the volume can be used only for read operations.

out-of-service

Indicates that the volume cannot be used for any operation.

4.1.49 wwn

Description

The `wwn` placeholder represents the World Wide Name (WWN) of a [tape device](#). A WWN is a 64-bit address used to uniquely identify a tape device in a [Fibre Channel](#) network. A WWN is typically assigned to a tape device by the tape device manufacturer, although the WWN can be later changed by a network user.

Restrictions and Usage Notes

Oracle Secure Backup supports tape devices whose operating system-assigned logical names can vary at each operating system restart. Fibre Channel-attached tape drives and libraries connected to [Network Attached Storage \(NAS\)](#) devices fall into this category. You can refer to these tape devices by their WWNs, for example, `nr.WWN[2:000:0090a5:0003f7].a`, rather than their logical names, for example, `nrst0a`. Unlike the logical name, the WWN does not change when you restart.

Any substring of the [attachment](#) raw device name that is the string `$WWN` is replaced with the value of `wwn` each time the device is opened. For example, a usable raw device name for a Network Appliance [filer](#) attached to a [Storage Area Network \(SAN\)](#) is `nr.$WWN.a`. This name specifies a no-rewind, best-compression [tape device](#) having the worldwide name you specify with the `--wwn/-W` option, for example, `--wwn WWN[2:000:0090a5:0003f7]`.

Syntax

wwn::=

`wwn`

Semantics

wwn

Specifies a World Wide Name.

5

obtool Variables

Oracle Secure Backup maintains several internal variables that control various aspects of its operation. These variables are described in this appendix. The variable list is also available through online help with the following command:

```
obtool help var
```

This chapter describes the following variables:

- [browsemode](#) (page 5-1)
- [drive](#) (page 5-1)
- [errors](#) (page 5-2)
- [escape](#) (page 5-2)
- [fs](#) (page 5-2)
- [host](#) (page 5-3)
- [level](#) (page 5-3)
- [library](#) (page 5-3)
- [maxlevel](#) (page 5-3)
- [namewidth](#) (page 5-4)
- [numberformat](#) (page 5-4)
- [snapshot](#) (page 5-4)
- [verbose](#) (page 5-4)
- [viewmode](#) (page 5-5)
- [width](#) (page 5-5)

5.1.1 browsemode

Controls the mode in which the browser is operating.

Values

catalog

Displays exact directory contents for selected backups.

snapshot

Displays live file-system snapshots on hosts accessed through [Network Data Management Protocol \(NDMP\)](#).

5.1.2 drive

Use the `drive` variable to specify a default [tape drive](#) for [tape library](#) operations.

Oracle Secure Backup uses the value of this variable if no `--drive drive-name` option is provided to tape library commands that require a tape drive specification.

Values

drivename

Specifies the name of a tape drive. Note that setting this variable also sets the [library](#) (page 5-3) variable to the name of the tape library that contains the specified tape drive. By default this variable is not set.

5.1.3 errors

Use the `errors` variable to set the level of detail for error messages. If the variable is not set (default), then the level of detail is set by the `--longerrors/-E` command-line option in `obtool`. "[obtool Syntax for Interactive Mode](#) (page 1-3)" describes the command-line option.

Values

long

Includes descriptive text and the `obtool` component name.

short

Includes only descriptive text.

5.1.4 escape

Use the `escape` variable to specify the character to use for quoting special characters. The escape character is used by the `obtool` command-line parser to quote special characters such as single or double quotation marks. Quoting these characters disables their meaning.

Values

char

Specifies an escape character. The default escape character is an ampersand (&). Note that if the escape character is set to an ampersand (&), and if you specify & as part of a file name when running `obtool` commands on the command line, then enclose the file name within single quotes. For example:

```
obtool cd -h phred '/home/markb&patti'
```

Because the ampersand character is within single quotes, it is not interpreted and is considered part of the file name.

5.1.5 fs

Use the `fs` variable to set the default `filesystem-name` for browser operations.

The value of this variable is used if no `--fs filesystem-name` option is provided to browser commands that accept it.

5.1.6 host

Use the `host` variable to specify a default host for host operations.

The value of this variable is used if no `--host hostname` option is provided to browser commands that accept it.

Values

hostname

Specifies a host name. The default value is the name of the host on which `obtool` is running.

5.1.7 level

Use the `level` variable to specify an exact [backup level](#) to which the browser is constrained. You can also specify the level with the `--level` option of the [lsbu](#) (page 2-122) command.

Values

backup-level

Specifies a backup level. Refer to "[backup-level](#) (page 4-4)" for a description of the `backup-level` placeholder. By default this variable is not set.

5.1.8 library

Use the `library` variable to specify a default [tape library](#) for tape library operations.

Oracle Secure Backup uses the value of this variable is used if no `--library library_name` option is provided to library commands that require a tape library specification. If this variable is reset with the [unset](#) (page 3-153) `var` command, then the [drive](#) (page 5-1) variable is also reset.

Values

libraryname

Specifies the name of a tape library. By default this variable is not set.

5.1.9 maxlevel

Use the `maxlevel` variable to set the maximum [backup level](#) to which the browser is constrained. You can also specify the level with the `--maxlevel` option of the [lsbu](#) (page 2-122) command.

Values

backup-level

Specifies a maximum backup level. Refer to "[backup-level](#) (page 4-4)" for a description of the `backup-level` placeholder. By default this variable is not set.

5.1.10 namewidth

Use the `namewidth` variable to set the nominal width in characters for the `ls` (page 2-114) `--long` output. This width controls the column alignment of the `backup ID` data that appears in parentheses following each name, as shown in the following example:

```
ob> ls --long
-rwx----- bkpadmin.g527      74      2012/05/24.12:55 file1      (1)
```

Values

namewidth

Specifies the width of the name field as a decimal value. The default value is 18. The legal range is 1 to 4092.

5.1.11 numberformat

Use the `numberformat` variable to set the display format for certain large numbers. You can also control this setting with the `--numberformat` option of the `ls` (page 2-114) command.

Values

numberformat

Sets the display of large numbers. Refer to "[numberformat](#) (page 4-21)" for a description of the `numberformat` placeholder. By default the `numberformat` variable is unset, which is equivalent to setting it to `friendly`.

5.1.12 snapshot

The value of this variable is used if no `--snapshot snapshot-name` option is provided to browser commands that accept it.

5.1.13 verbose

Use the `verbose` variable to set the level of `obtool` output. If this variable is not set (default), then verbose mode is controlled by the `--verbose/-v` command-line option in `obtool`. "[obtool Syntax for Interactive Mode](#) (page 1-3)" describes the command-line option.

Values

yes

Displays verbose output.

no

Suppresses verbose output.

5.1.14 viewmode

Use the `viewmode` variable to set the display mode for Oracle Secure Backup [catalog](#) directories. Unsetting this variable is equivalent to setting it to `inclusive`.

You can also control the display mode with the `--viewmode` option of the [ls](#) (page 2-114) command.

Values

exact

Displays exact directory contents for selected backups, from the path of the selected backup.

inclusive

Displays all directory contents (default).

specific

Displays the directory contents identified by the data selector.

5.1.15 width

Use the `width` variable to set the line width in characters for adjustable-width output. The number of characters displayed on each line by commands such as [ls](#) (page 2-114) is adjustable. The `width` variable controls, to the degree possible, such line widths. Note that `obtool` exceeds this line width to accommodate long names.

Values

width

Specifies the width of the name field as a decimal value. The default value is 80. The legal range is 80 to 4176.

6

Dataset Language

This chapter describes the language used in dataset files. A [dataset file](#) is a text file that describes the data that Oracle Secure Backup should back up.

This chapter contains the following topics:

- [Overview of the Dataset Language](#) (page 6-1)
- [Dataset File Examples](#) (page 6-2)
- [Backward Compatibility](#) (page 6-4)
- [Dataset Statements](#) (page 6-4)

See Also:

- ["Dataset Commands](#) (page 1-14)"
- The sample dataset files located in the samples subdirectory of the [Oracle Secure Backup home](#)

6.1 Overview of the Dataset Language

The Oracle Secure Backup [dataset](#) language provides a simple, text-based means to define file-system data to back up. The language has the following characteristics:

- Comments can appear anywhere following a pound sign (#).
- Dataset statements use the following syntax:

```
statement-name [ statement-argument ]
```

The *statement-name* placeholder represents a dataset statement. These statements are described in "[Dataset Statements](#) (page 6-4)".

- Some statements can begin a nested block. Statements within the block apply only to the statement that began the block. Nested block statements have the following form:

```
statement-name [ statement-argument ] {  
    statement-name [ statement-argument ]  
    ...  
}
```

- An escape character, which is represented by a backslash (\), can appear anywhere to remove the special meaning of the character following it.
- Blank lines are ignored.

[Example 6-1](#) (page 6-2) is a sample [dataset file](#) that describes a backup of directories on brhost2.

Example 6-1 Sample Dataset

```

#
# A sample dataset file
#
exclude name *.backup           # never back up directories or files
exclude name *~                 # matching *.backup and *~

include host brhost2 {          # back up host brhost2
    include path /usr1/home {    # back up /usr1/home on brhost2,
        exclude path peter      # skip subdirectory peter (relative path)
        exclude path /usr1/home/dinesh # also skip subdir dinesh (absolute path)
    }
    include path /usr2/home      # also back up /usr2/home, including
}                                # all subdirectories

```

6.2 Dataset File Examples

This section presents examples of dataset files.

This section contains the following topics:

- [Backing Up Multiple Paths on Multiple Hosts](#) (page 6-2)
- [Including Dataset Files Within Dataset Files](#) (page 6-2)
- [Defining the Scope of a Backup](#) (page 6-3)

6.2.1 Backing Up Multiple Paths on Multiple Hosts

[Example 6-2](#) (page 6-2) shows a complex [dataset file](#) that describes four host systems to be backed up. It specifies that all files in the `/home`, `/usr`, and `/usr2` directories and all files in subdirectories within these directories are to be backed up.

All files in the `/usr/tmp` directory are excluded from the [dataset](#). Files that have the name `core` and files that have names ending in `.bak`, regardless of where they reside, are also excluded from the dataset.

Example 6-2 Backing Up Multiple Paths on Multiple Hosts

```

include host brhost1
include host brhost2
include host brhost3
include host brhost4

include path /home
include path /usr
include path /usr/usr2

exclude path /usr/tmp
exclude name core
exclude name *.bak

```

6.2.2 Including Dataset Files Within Dataset Files

A [dataset file](#) can logically include the contents of another dataset file. The `include dataset` statement lets you include by reference the contents of another dataset file.

Consider the sample dataset file called `common-exclusions.ds` shown in [Example 6-3](#) (page 6-3).

A dataset file can use these exclusions with the statement shown in [Example 6-4](#) (page 6-3).

To apply these exclusions to one path but not to another, specify the `include dataset` directive within braces as shown in [Example 6-5](#) (page 6-3).

Example 6-3 `common-exclusions.ds`

```
exclude name core
exclude name *~
exclude name *.tmp
exclude name *.temp
```

Example 6-4 Including a Dataset File

```
include dataset common-exclusions.ds
```

Example 6-5 Applying Exclusions to a Path

```
include path /home/root          # do not exclude here
include path /home/frank {      # do exclude here
    include dataset common-exclusions.ds
}
```

6.2.3 Defining the Scope of a Backup

You can use braces with an include rule to define the scope of a backup. In [Example 6-6](#) (page 6-3), Oracle Secure Backup backs up paths `/usr1` and `/usr2` on all servers and backs up `/usr3` and `/usr4` on `brhost3` only. Note that the order in which the rules appear within the braces has no affect on the rules.

You can use additional braces to further refine the scope of rules. [Example 6-7](#) (page 6-3) alters [Example 6-6](#) (page 6-3) to exclude files ending with `.junk` from `usr4` on `brhost3` only.

Example 6-6 Using Braces to Limit Scope

```
# Common trees backed up on all servers:
include path /usr1
include path /usr2

# Servers to back up; on brhost3, we also back up usr3 & usr4, too:
include host brhost1
include host brhost2
include host brhost3 {
    include path /usr3
    include path /usr4
}
```

Example 6-7 Refining the Scope of a Set of Rules

```
# Common trees backed up on all servers:
include path /usr1
include path /usr2

# Servers to back up; on brhost3, back up /usr3 and /usr4, but exclude *.junk
# files in /usr4 only:
include host brhost1
```

```
include host brhost2
include host brhost3 {
    include path /usr3
    include path /usr4 {
        exclude name *.junk
    }
}
```

6.3 Backward Compatibility

If you specify a [wildcard](#) pattern in an `exclude path` or `exclude name` statement, then releases of Oracle Secure Backup after release 10.3 attempt to match the pattern while respecting path separators. If you specify pattern `src/*.pl`, for example, then Oracle Secure Backup would exclude `src/a.pl` but not `src/tmp/b.pl`.

The [exclusion statement](#) wildcard pattern matching in previous releases of Oracle Secure Backup did not respect path separators. If you specified the same `src/*.pl` pattern, for example, then Oracle Secure Backup would exclude both `src/a.pl` and `src/tmp/b.pl`.

If you have upgraded to Oracle Secure Backup release 10.3 or higher from an earlier Oracle Secure Backup release, then you can continue using your existing `exclude path` and `exclude name` statements. Some files and directories that were excluded from backups in the earlier Oracle Secure Backup release are now not excluded. This causes your backup files to be somewhat larger, but all data still backed up.

6.4.1 Dataset Statements

A dataset description can contain the following types of statements:

- [after backup](#) (page 6-5)
- [before backup](#) (page 6-6)
- [cross all mountpoints](#) (page 6-7)
- [cross local mountpoints](#) (page 6-8)
- [cross remote mountpoints](#) (page 6-9)
- [exclude dir](#) (page 6-10)
- [exclude file](#) (page 6-11)
- [exclude name](#) (page 6-11)
- [exclude oracle database files](#) (page 6-13)
- [exclude path](#) (page 6-14)
- [include catalog](#) (page 6-15)
- [include dataset](#) (page 6-16)
- [include host](#) (page 6-16)
- [include path](#) (page 6-17)
- [setenv NDMP](#) (page 6-19)

 **See Also:**

"[Dataset File Examples](#) (page 6-2)" for examples of description files that use these statements.

6.4.1.1 after backup

Purpose

Use the `after backup` statement to direct Oracle Secure Backup to run a computer executable or interpreted program after completing a backup. By using the [before backup](#) (page 6-6) statement, you can also run the same or a different program before the backup begins. These statements are useful, for example, when you want to shut down and restart a database server or inform users that a backup has started or completed.

By default, Oracle Secure Backup stops the [backup job](#) and considers it failed if the specified executable does not exist or fails, that is, returns a nonzero exit code.

Usage Notes

While performing multiple dataset jobs, you may or may not want this statement to apply to all jobs that are a part of the set. To use `after backup` for all jobs, use the statement at the start of the syntax. For instance:

```
after backup "/bin/sh /tmp/a.sh"
include host brhost1 {
include path /tmp/backup
}
include host brhost2 {
include path /tmp/backup
}
```

On the other hand, to use the `after backup` statement for a single job in a set of jobs, include the statement within the syntax of that particular dataset job. For instance:

```
include host brhost1 {
include path /tmp/backup
after backup "/bin/sh /tmp/a.sh"
}
include host brhost2 {
include path /tmp/backup
}
```

Syntax

after backup::=

```
after backup [ optional ] pathname
```

The *pathname* placeholder represents the name of the program to be run on a [client](#) host. For backups using a [Network Data Management Protocol \(NDMP\) data service](#), Oracle Secure Backup runs the program on the [administrative server](#).

The `optional` keyword specifies that Oracle Secure Backup should ignore the status returned from the invoked program and also the inability to invoke this program.

Example

Example 6-8 after backup Statement

This example directs Oracle Secure Backup to pass the argument `/usr2` is being saved to program `/etc/local/nfy` on host `brhost2` after backing up directory `/usr2`.

```
include host fserver {
    include path /usr2
    after backup "/etc/local/nfy '/usr2 backup complete'"
}
```

Oracle Secure Backup automatically appends the following arguments to any that you specify:

- The token `after`
- The name of the [client](#)
- The name of the directory or file being backed up
- The exit status of the backup operation (a numeric value documented in the file `OSB_HOME/samples/obexit.h`.)

Thus, in this example Oracle Secure Backup runs the `nfy` program on `brhost2` as if you entered:

```
/usr/local/nfy '/usr2 backup complete' after brhost2 /usr2 exit-code
```

6.4.1.2 before backup

Purpose

Use the `before backup` statement to direct Oracle Secure Backup to run a computer executable or interpreted program before beginning a backup. This statement is parallel to the [after backup](#) (page 6-5) statement.

By default, Oracle Secure Backup does not begin the [backup job](#) and considers it failed if the specified executable does not exist or fails, that is, returns a nonzero exit code.

Usage Notes

While performing multiple dataset jobs at once, you may or may not want this statement to apply to all jobs that are a part of the set. To use the `before backup` for all jobs, use the statement at the start of the syntax. For instance:

```
before backup "/bin/sh /tmp/a.sh"
include host brhost1 {
include path /tmp/backup
}
include host brhost2 {
include path /tmp/backup
}
```

On the other hand, to use `before backup` for a single job in a set of jobs, include the statement within the syntax of that particular dataset job. For instance:

```
include host brhost1 {
include path /tmp/backup
```

```
before backup "/bin/sh /tmp/a.sh"
}
include host brhost2 {
include path /tmp/backup
}
```

Syntax

The *pathname* placeholder represents the name of the program to be run on a [client host](#). For backups using a [Network Data Management Protocol \(NDMP\) data service](#), Oracle Secure Backup runs the program on the [administrative server](#).

before backup::=

```
before backup [ optional ] pathname
```

The *optional* keyword specifies that Oracle Secure Backup should ignore the status returned from the invoked program and also the inability to invoke this program.

Example

Example 6-9 before backup Statement

This example directs Oracle Secure Backup to pass the argument `/usr2 is being saved` to program `/etc/local/nfy` on host `brhost2` before backing up directory `/usr2`.

```
include host brhost2 {
    include path /usr2
    before backup "/etc/local/nfy '/usr2 is being saved'"
}
```

Oracle Secure Backup automatically appends the following arguments to any that you specify:

- The token `before`
- The name of the client
- The name of the directory or file being backed up

Thus, in this example Oracle Secure Backup runs the `nfy` program on `brhost2` as if you entered:

```
/usr/local/nfy '/usr2 is being saved' before brhost2 /usr2
```

6.4.1.3 cross all mountpoints

Purpose

Use the `cross all mountpoints` statement to cross local and remote mount points. A local mount point mounts a local file system; a remote mount point is a local mount of a file system accessed over the network. By default, a [file-system backup](#) does not cross mount points.

Suppose `/home/usr1/loc_data` mounts a local file system, while `/home/usr1/rem_data` is an [Network File System \(NFS\)](#) mount point for a file system on a network host. You can use `cross all mountpoints` to specify that a backup of `/home/usr1` includes all files in this directory, whether local or mounted.

Syntax

cross all mountpoints::=

```
cross all mountpoints
```

Examples

Example 6-10 Global Host Inclusion

This example crosses all local and remote mount points on hosts `brhost1` and `brhost2`.

```
cross all mountpoints
include host brhost1 {
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-11 Global Path Inclusion

This example crosses all local and remote mount points in the paths for host `brhost1` but not `brhost2`.

```
include host brhost1 {
    cross all mountpoints
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-12 Local Path Inclusion

This example crosses all local and remote mount points in the `/home/usr1` path, but not in the `/home/usr2` path, on `brhost1`.

```
include host brhost1 {
    include path /home/usr1 {
        cross all mountpoints
    }
    include path /home/usr2
}
```

6.4.1.4 cross local mountpoints

Purpose

Use the `cross local mountpoints` statement to cross local (but not remote) mount points.

Suppose `/home/usr1/loc_data` mounts a local file system while `/home/usr1/rem_data` is a [Network File System \(NFS\)](#) mount point for a file system on a network host. You can use `cross local mountpoints` to specify that a backup of `/home/usr1` includes files in `/home/usr1/loc_data` but not `/home/usr1/rem_data`.

Syntax

cross local mountpoints::=

```
cross local mountpoints
```

Examples

Example 6-13 Global Host Inclusion

This example crosses only local mount points in the file systems for hosts `brhost1` and `brhost2`.

```
cross local mountpoints
include host brhost1 {
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-14 Global Path Inclusion

This example crosses local mount points in the `/home/usr1` path on host `brhost1`, but does not cross mount points in the `/home/usr2` path on `brhost2`.

```
include host brhost1 {
    cross local mountpoints
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-15 Local Path Inclusion

This example crosses local mount points found in the `/home/usr1` path, but no mount points in the `/home/usr2` path, on `brhost1`.

```
include host brhost1 {
    include path /home/usr1 {
        cross local mountpoints
    }
    include path /home/usr2
}
```

6.4.1.5 cross remote mountpoints

Purpose

Use the `cross remote mountpoints` statement to cross remote (but not local) mount points.

Suppose `/home/usr1/loc_data` is a mount point for a local file system, while `/home/usr1/rem_data` is a [Network File System \(NFS\)](#) mount point for a file system on a network host. You can use `cross remote mountpoints` to specify that a backup of `/home/usr1` includes files in `/home/usr1/rem_data` but not `/home/usr1/loc_data`.

Syntax

cross remote mountpoints::=

```
cross remote mountpoints
```

Examples

Example 6-16 Global Host Inclusion

This example crosses only remote mount points in the file systems on hosts `brhost1` and `brhost2`.

```
cross remote mountpoints
include host brhost1 {
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-17 Global Path Inclusion

This example crosses only remote mount points in the `/home/usr1` path on `brhost1`.

```
include host brhost1 {
    cross remote mountpoints brhost3
    include path /home/usr1
}
include host brhost2 {
    include path /home/usr2
}
```

Example 6-18 Local Path Inclusion

This example crosses only remote mount points in the `/home/usr1` path and only local mount points in the `/home/usr2` path.

```
include host brhost1 {
    include path /home/usr1 {
        cross remote mountpoints
    }
    include path /home/usr2 {
        cross local mountpoints
    }
}
```

6.4.1.6 exclude dir

Purpose

Use the `exclude dir` statement to identify a directory or set of directories to exclude from a backup. It differs from `exclude name` in that it does not exclude files matching the specified pattern.

Syntax

exclude dir::=

```
exclude dir pattern
```

Semantics

pattern

Specifies the directory or set of directories to be excluded. The *pattern* placeholder must not include any path separators. It supports [UNIX-style wildcard syntax](#) expression-based pattern matching.

6.4.1.7 exclude file

Purpose

Use the `exclude file` statement to identify file-system objects to exclude from backup by file name, without regard for the directory location of the file. It differs from `exclude name` in that it does not exclude directories matching the specified pattern.

Syntax

exclude file::=

```
exclude file pattern
```

Semantics

pattern

Specifies the file or set of files to be excluded. The *pattern* placeholder must not include any path separators. It supports [UNIX-style wildcard syntax](#) expression-based pattern matching.

6.4.1.8 exclude name

Purpose

Use the `exclude name` statement to identify file-system objects to exclude from backup either by the right-most matching component name in the path, which is called the leafname, or by a matching relative path or pattern.



See Also:

["Backward Compatibility \(page 6-4\)"](#)

Syntax

exclude name::=

```
exclude name { leafname | relative_pathname }
```

Semantics

leafname

Oracle Secure Backup compares the component name of each file-system object with the specified *leafname*. If they match, then Oracle Secure Backup does not back up the file-system object. If it is a directory, then Oracle Secure Backup does not back up the directory contents.

Oracle Secure Backup interprets *leafname* as a Oracle Secure Backup-style [wildcard](#) expression if it contains any of the unescaped special characters *, ?, [, or]. If *leafname* contains these characters, then Oracle Secure Backup performs a wildcard comparison rather than a string comparison to determine whether the names match.

relative_pathname

Oracle Secure Backup compares the component name of each file-system object with the specified *relative_pathname* relative to the current included path. If they match, then Oracle Secure Backup does not back up the file-system object. If *relative_pathname* references a directory, then Oracle Secure Backup does not back up the directory contents.

Oracle Secure Backup interprets *relative_pathname* as a Oracle Secure Backup-style wildcard expression if it contains any of the unescaped special characters *, ?, [, or]. If *relative_pathname* contains these characters, then Oracle Secure Backup performs a wildcard comparison rather than a string comparison to determine whether the names match.

Example

Example 6-19 `exclude name` Statement

Assume a directory tree containing the following files and directories:

```
/src
/src/abc
/src/abc/a.pl
/src/tmp
/src/tmp/g.pl
/src/tmp/src/d.plaf
/src/tmp/src/a.pldir
/src/tmp/src/a.pldir/a.pl
/src/tmp/src/a.pldir/s.tmp
/src/tmp/src/a.pl
/src/a.pl
/src/b.pl
```

You create a dataset with the following contents:

```
exclude name d
exclude name *.tmp
```

The dataset statements exclude files or directories named `d` and files whose names end in `.tmp`. For the assumed directory tree, the following items would be excluded from backup operations:

```
/src/tmp/src/d.plaf
/src/tmp/src/a.pldir/s.tmp
```

6.4.1.9 exclude oracle database files

Purpose

Use the `exclude oracle database files` statement to exclude all Oracle database-related files that would ordinarily be backed up by [Recovery Manager \(RMAN\)](#) or files whose backup is not recommended. Oracle Secure Backup excludes the files regardless of whether the files being excluded are part of an existing RMAN backup strategy.

Oracle Secure Backup excludes the following types of files:

- Data files (production files and image copies of those files)
- Control files
- Redo logs, both online and archived
- Flashback logs
- Change tracking file
- Backup pieces
- Tempfiles

Note:

You use the Oracle Enterprise Manager job [scheduler](#) to schedule a database backup through RMAN and the Oracle Secure Backup job scheduler to schedule a [file-system backup](#). Thus, to back up an Oracle database host with Oracle Secure Backup, you must set up two schedules in Enterprise Manager and Oracle Secure Backup. Use the `exclude oracle files` statement in the Oracle Secure Backup schedule so that the Oracle database-related files are not backed up twice.

Syntax

exclude oracle database files::=

```
exclude oracle database files
```

Example

Example 6-20 exclude oracle database files Statement

This dataset file excludes Oracle database-related files from the backup of host `brhost2`.

```
exclude name *.backup
exclude name *~
include host brhost2 {
    exclude oracle database files
    exclude path /usr1/home
}
```

6.4.1.10 exclude path

Purpose

Use the `exclude path` statement to identify the path name or [wildcard](#) pattern of file-system objects to exclude from the backup.



See Also:

["Backward Compatibility \(page 6-4\)"](#)

Syntax

`exclude path::=`

```
exclude path  
    (absolute-path | relative-path)
```

Semantics

absolute-path

Specifies a path or pattern matching subdirectories or files in subdirectories relative to the root of the file system. Absolute paths on Windows platforms begin with *drive-letter:*, and on UNIX with */*.

relative-path

Specifies a path or pattern matching subdirectories or files in subdirectories relative to the current `include path`.

Examples

Example 6-21 `exclude path` Statement

Assume the following set of directories and files to be backed up on host `osblin1`:

```
/src  
/src/abc  
/src/abc/a.tmp  
/src/tmp  
/src/tmp/g.pl  
/src/tmp/src/d.tmp1  
/src/tmp/src/a.tmporary  
/src/tmp/src/a.pldir/a.tmp  
/src/tmp/src/d.tmp-out  
/src/tmp/src/a.  
/src/a.pl  
/src/b.pl  
/misc  
/misc/yesterday.tmp  
/misc/tmssql.out
```

The following dataset specifies a backup of the `/` directory on `osblin1`, but skips files in `/src/tmp` and files with the extension `.tmp` at any level of the `/src` directory.

```
include host osblin1 {
  include path / {
    exclude path src/tmp
    exclude name *.tmp
  }
}
```

6.4.1.11 include catalog

Purpose

Use the `include catalog` statement to direct Oracle Secure Backup to back up all data on the [administrative server](#) required to restore the Oracle Secure Backup [catalog](#). This directive is expanded internally by the [dataset](#) parser to a list of all required files and databases.

This directive can be included in other datasets. But it cannot be used within an [include host](#) (page 6-16) bloc, because by definition it only applies to the administrative server host.

You can add extra files and paths on the administrative server host to the files backed up by `include catalog` by listing [include path](#) (page 6-17), [exclude path](#) (page 6-14) and [exclude name](#) (page 6-11) directives within block delimiters beneath the `include catalog` directive. No other directives are permitted within the `include catalog` block.

A catalog backup is always created as a [full backup](#) and never as an [incremental backup](#). Restoring from incremental backups is difficult without the contents of the catalog, so creating catalog backups as full backups is more reliable.

In a catalog recovery situation, the [wallet](#) containing encryption keys might not be available. Therefore, the expanded catalog directive and its children are handled in a separate job by the [scheduler](#), which runs with storage encryption policies disabled.

You can still use transient passphrase encryption to protect this backup, because transient passphrase encryption does not depend upon the wallet.

If you use `include path` directives to add extra files with sensitive contents to the catalog backup, then consider using transient passphrase encryption to protect the backup containing these files.

 **Note:**

A catalog backup written to a cloud storage device is not encrypted. You can use transient passphrase encryption to back up the catalog to a cloud storage device.

Syntax

include catalog::=

```
include catalog
  [ { directive... } ]
```

Semantics

include catalog

Include all data required for a future catalog recovery.

directive

Specify [include path](#) (page 6-17) directives to add to the data backed up for catalog backups. Use [exclude path](#) (page 6-14) and [exclude name](#) (page 6-11) directives to subtract from the data backed up for catalog backups.

Example

Example 6-22 include catalog Directive with Extra Files

This example includes every dataset file in the `admin/default_rules` directory.

```
include catalog {
    include path /home/adminuser
}
```

6.4.1.12 include dataset

Purpose

Use the `include dataset` statement to direct Oracle Secure Backup to read another [dataset file](#) and logically substitute its contents for the `include dataset` statement. This statement is analogous to include statements found in most programming languages.

Syntax

include dataset::=

```
include dataset dataset_file_name
```

The `dataset_file_name` placeholder represents the name of a dataset file or directory. If you supply the name of a [dataset directory](#), then Oracle Secure Backup includes each member of the directory.

Example

Example 6-23 include dataset Statement

This example includes all dataset files in the `admin/default_rules` directory.

```
include dataset admin/default_rules
```

6.4.1.13 include host

Purpose

Use the `include host` statement to identify the name of a [client](#) host to back up. It is recommended that you add the `include host` statement prior to the [include path](#) (page 6-17) and [include dataset](#) (page 6-16) statements, in the [dataset file](#).

A usable dataset file must have at least one host statement either within the dataset file or within an included dataset file.

The `include host` statements takes either of the following forms.

Syntax 1

include host::=

```
include host hostname
```

Syntax 2

include host::=

```
include host hostname {statements_that_apply_to_hostname}
```

The *hostname* placeholder represents the name of a client you defined earlier with the Oracle Secure Backup [Web tool](#) interface or the `mkhost` or `renhost` commands.

Example

Example 6-24 include path Statement

This example includes host `brhost2`:

```
include host brhost2
```

6.4.1.14 include path

Purpose

Use the `include path` statement to identify the name of a file-system object to back up.

Backup paths cannot exceed the maximum path length of the file system being backed up, and in any case they cannot exceed 260 characters on Windows systems or 1024 characters on other operating systems.

Path names on both Windows and Linux/UNIX can include the standard wildcard characters `*`, `?`, `[`, and `]`. If you have path names that include any of these wildcard characters, then you must precede each such character with a backslash (`\`) character to prevent special interpretation of these characters.

To reduce the risk of unauthorized access to obfuscated wallets, Oracle Secure Backup, by default, does not back up obfuscated wallets. However, you can back up the obfuscated wallet by explicitly listing its file name with the complete path in the `include path` statement of your dataset. [Example 6-30](#) (page 6-19) describes how to include an obfuscated wallet in your dataset. The obfuscated wallet is also backed up if it is included in an Oracle Secure Backup encrypted backup.

During an Oracle Secure Backup encrypted backup, the obfuscated wallet is backed up if the dataset includes the directory that contains the `cwallet.sso` file. For example, an encrypted backup of the dataset that contains the following `include path` statement backs up the contents of the wallet directory along with the obfuscated wallet that is contained in this directory:

```
include path /usr/local/apps/wallet
```

Syntax

include path::=

```
include path absolute-pathname
```

The *absolute-pathname* placeholder represents the path name of the file-system object to back up, starting at the file-system root. Surround path names containing spaces within single or double quotes.

Examples



Note:

Wildcard characters cannot be used to include the obfuscated wallet in your backup. For example, you cannot use the following statement to add the obfuscated wallet to a dataset:

```
include path /usr/local/apps/wallet/cwallet.*
```

Example 6-25 include path Statement on Windows

This example shows an `include path` statement on a Windows system. The path contains spaces, so it is surrounded by double quotes.

```
include path "C:\Documents and Settings"
```

Example 6-26 include path Statement on Linux/UNIX

For Linux or UNIX systems, the `include path` statements do not include [tape drive](#) designators or quotation marks. This example shows an `include path` statement on a Linux or UNIX system.

```
include path /space      { # include the local root directory
    exclude name core    # but no core files (for UNIX)
    exclude name *~      # and no emacs backup files
}
include path /etc
```

Example 6-27 include host Statements

You can nest an `include path` statement within an `include host` statement. Consider the [dataset](#) statements shown in this example.

Oracle Secure Backup interprets each `include path` statement in the [dataset file](#) to apply to each `include host` statement. Thus, Oracle Secure Backup backs up the `/home` and `/project` directories on each host, `brhost2` and `brhost3`.

```
include host brhost2
include host brhost3
include path /home
include path /project
```

Example 6-28 Dataset File with include host and include path Statements

This example backs up `/home` on host `brhost2` and `/project` on host `brhost3`. The statements in this example are equivalent to the statements in [Example 6-29](#) (page 6-19).

```
include host brhost2 {
    include path /home
    include path /project
}
include host brhost3 {
    include path /home
    include path /project
}
```

Example 6-29 Dataset File with include host and include path Statements

The statements in this example are equivalent to the statements in [Example 6-28](#) (page 6-19).

```
include host brhost2 {
    include path /home
}
include host brhost3 {
    include path /project
}
```

Only include multiple hosts or paths in a dataset file if you always back them up. The Oracle Secure Backup [scheduler](#) and [on-demand backup](#) functions use dataset file names, not path names, to define each [backup job](#).

Example 6-30 Dataset File for backing up Obfuscated Wallets in Unencrypted Backups

This example shows a dataset that is used to include an obfuscated wallet as part of an unencrypted backup. The obfuscated wallet `cwallet.sso` is stored in the `/usr/local/apps/wallet` directory. The following dataset includes the obfuscated wallet along with the contents of the `/usr/local/apps/wallet` directory.

```
include host brhost2 {
    include path /usr/local/apps/wallet
    include path /usr/local/apps/wallet/cwallet.sso
}
```

Although `cwallet.sso` is part of the `/usr/local/apps/wallet` folder, it will be included in an unencrypted backup only if it is explicitly listed using an include path statement.

6.4.1.15 setenv NDMP

Purpose

Use the `setenv NDMP` statement to set [Network Data Management Protocol \(NDMP\)](#) environment variable name-value pairs while creating or modifying a dataset. You can set one environment variable per `setenv` statement. These environment variables are passed down to the NDMP filer when this dataset is being backed up.

Syntax

setenv NDMP ::=

```
setenv NDMP:variable-name variable-value
```

While using the `setenv` statement, ensure that each NDMP environment variable has `NDMP:` as its prefix.

Examples

Example 6-31 Adding NDMP Values to a Dataset

This example uses the `setenv NDMP` statement to add NDMP variable values for a dataset that will backup files on the host `NDMP_HOST1`.

```
include host NDMP_HOST1
{
include path PATH1
setenv NDMP:DMP_NAME test_name1
setenv NDMP:UPDATE y
setenv NDMP:ZFS_FORCE y
}
```

7

Defaults and Policies

Oracle Secure Backup [defaults and policies](#) are configuration data that control how Oracle Secure Backup operates within an [administrative domain](#). These policies are grouped into several policy classes. Each policy class contains policies that describe a particular area of operations.

The policy classes are as follows:

- [Backup Compression Policies](#) (page 7-1)
- [Backup Encryption Policies](#) (page 7-3)
- [Copy Backup Image Instance Policies](#) (page 7-7)
- [Cloud Storage Device Policies](#) (page 7-8)
- [Daemon Policies](#) (page 7-9)
- [Device Policies](#) (page 7-13)
- [Duplication Policies](#) (page 7-17)
- [Index Policies](#) (page 7-19)
- [Log Policies](#) (page 7-22)
- [Media Policies](#) (page 7-24)
- [Naming Policies](#) (page 7-27)
- [NDMP Policies](#) (page 7-28)
- [Operations Policies](#) (page 7-31)
- [Scheduler Policies](#) (page 7-39)
- [Security Policies](#) (page 7-42)
- [Staging Policies](#) (page 7-46)
- [Vaulting Policies](#) (page 7-47)

See Also:

"[Policy Commands](#) (page 1-18)" to learn about the `obtool` policy commands

7.1 Backup Compression Policies

These policies, if specified, control how Oracle Secure Backups performs backup compression.

The compression policies are as follows:

- [option](#) (page 7-2)

- [buffersize](#) (page 7-2)
- [excludeformats](#) (page 7-3)

Usage Notes

- There is no one best compression level. The best level to use depends on your specific environment and compression requirements, as well as network traffic characteristics (workload), backup speed, and the content of the data set being compressed.
- Oracle Secure Backup compression options are not applicable to database backups performed using RMAN. For database backups, similar compression options can be specified as part of RMAN commands.
- Oracle Secure Backup compression options are not applicable to NDMP hosts (`--access ndmp`).
- If Oracle Secure Backup finds hardware capable of doing hardware compression, then it disables any software compression option that may be set, with appropriate warning messages as part of the job.

7.1.1 option

Use this policy to specify how to compress all backup data in a domain. By default no compression value is set when the domain is created. The value specified is used to compress all file system backups on all Oracle Secure Backup clients where compression is not enforced, either at the backup job level or at the client policy level.

Values

low

Compresses data as best as possible without compromising too much on CPU usage and speed. Choose this option if you want the data compressed, but you do not want backup speed or CPU load to be overly affected.

medium

Provides a balance between compression ratio and speed.

basic

This option is generally better in terms of compression ratio than the `medium` option. It is slower than the `low` and `medium` options, but faster than the `high` option.

high

Compresses data as much as possible, using extensive CPU. This option is best suited for backups over slower networks where the limiting factor is network speed.

7.1.2 buffersize

Use this policy to set the size of buffer that Oracle Secure Backup uses to allocate a buffer for performing compression.

7.1.3 excludeformats

Use this policy to add to the default list of compressed file formats that are always excluded from Oracle Secure Backup software compression. Use the `addp` and `rmp` commands, respectively, to add and remove values.

By default, the following file formats are always excluded from Oracle Secure Backup software compression: `.3GP`, `.`

`7Z`, `.AVI`, `.BZ`, `.BZ2`, `.BZA`, `.CAB`, `.DEB`, `.FLAC`, `.GIF`, `.GZ`, `.GZ2`, `.GZIP`, `.JBIG2`, `.JPEG`, `.JPG`, `.LZ`, `.LZMA`, `.LZO`, `.M2TS`, `.MKV`, `.MOV`, `.MP3`, `.MP4`, `.MPG`, `.MPKG`, `.PACK`, `.PDF`, `.PKG`, `.PNG`, `.RAR`, `.RPM`, `.TIF`, `.VOB`, `.Z`, `.ZZ`, `.ZIP`, and `.ZIPX`

Values

list_of_formats

A list of compressed file formats (for example, `.zip2` `.bz3` `.gz3`)

The following is an example of using the `addp` command to specify compressed file formats which will not be considered for software compression. The `lsp` command is then used to display the formats to be excluded:

```
ob> addp backupcomp/exclude .tar .scf .fff
ob> lsp backupcomp/exclude
excludeformats .TAR
               .SCF
               .FFF
```

7.2 Backup Encryption Policies

These policies control how Oracle Secure Backup performs [backup encryption](#). For example, you can specify whether backups must be encrypted for the entire [administrative domain](#) or for specific clients in the domain, which encryption algorithm to use for encryption, and how keys are managed.

The `global algorithm`, `global keytype`, and `global rekeyfrequency` policies are used to provide default values to newly created clients. The `client algorithm`, `client keytype`, and `client rekeyfrequency` policies define the actual values used for a given client.

The encryption policies are as follows:

- [algorithm](#) (page 7-3)
- [enablehardwareencryption](#) (page 7-4)
- [encryption](#) (page 7-5)
- [keytype](#) (page 7-5)
- [rekeyfrequency](#) (page 7-6)
- [requireencryptablemedia](#) (page 7-6)

7.2.1 algorithm

Use the `algorithm` policy to specify the algorithm used in encrypting backups written to tape.

At the [administrative domain](#) level, the `algorithm` policy specifies the default algorithm for all backups. At the client level, it specifies the default algorithm for backups from this client.

Values



Note:

The algorithms available are the same as those available in [Recovery Manager \(RMAN\)](#).

AES128

Uses AES 128-bit encryption. This is the default.

AES192

Uses AES 192-bit encryption.

AES256

Uses AES 256-bit encryption.

7.2.2 enablehardwareencryption

Use the `enablehardwareencryption` policy to control whether Oracle Secure Backup uses hardware-based encryption.

The LTO4 interface to hardware encryption is implemented through the SCSI specification for hardware encryption. Encryption is performed by the LTO4 drive in hardware instead of in software by Oracle Secure Backup.

Hardware-based encryption brings no changes to the existing Oracle Secure Backup encryption model. All encryption decisions, policies, key management, and settings for hardware-based encryption are identical with those for software-based encryption.



Note:

It is not possible to back up using hardware-based encryption and then restore using software-based encryption. Nor is it possible to back up using software-based encryption and then restore using hardware-base encryption.

Values

yes

Enables Oracle Secure Backup to use hardware-based encryption. This value is the default.

no

Performs software-based encryption instead of hardware-based encryption.

7.2.3 encryption

Use the `encryption` policy to specify whether data written to tape backups must be encrypted by default.

This policy can be set as a global policy for the [administrative domain](#). It can also be overridden at the [client](#) level, using the `--encryption` option of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

 **Note:**

If a database backup is encrypted at the [Recovery Manager \(RMAN\)](#) level, then Oracle Secure Backup always writes the backup to tape in the encrypted form provided by RMAN, regardless of the setting for the `encryption` policy. If `encryption` is set to `required`, then Oracle Secure Backup does not encrypt the data a second time.

Values

required

Encrypts all backups, regardless of policy settings on specific clients or jobs. If this policy is enabled at the administrative domain level, then all backup data written to tape is encrypted, regardless of other policies for specific clients or settings for specific jobs. If this policy is defined at the client level, then all backup data written to tape from this client is encrypted, regardless of settings for specific jobs.

allowed

Does not encrypt backups to tape unless the policy set on a client or the settings for a job specify encryption. This is the default.

7.2.4 keytype

Use the `keytype` policy to specify the method for generating the encryption key.

Values

transparent

Generates keys randomly using the Oracle Random Number Generator as a seed for the key. The keys are stored in a host-specific key store. This is the default.

passphrase

Generates keys based on a backup administrator-supplied passphrase.

 **Note:**

- The backup administrator must set the passphrase for a given host using the `chhost` command. Until the passphrase is set, backups are encrypted in transparent mode.
- If the passphrase is lost or forgotten, then backups created with it cannot be restored.

7.2.5 rekeyfrequency

Use the `rekeyfrequency` policy to manage how often keys are generated. Older keys are retained in a wallet-protected key store.

The `rekeyfrequency` policy can be defined at the global level for an entire [administrative domain](#). The global policy can be overridden at the [client](#) level.

Values

duration

Specifies the frequency of generating keys for transparent mode encryption. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder.

A key is automatically generated at midnight on the day when the specified duration expires. This key is then added to the [wallet](#) and is used on subsequent backup operations. Older keys are retained in the wallet for restoring older backups.

 **Note:**

If the `keytype` (page 7-5) policy is set to `passphrase`, then the administrator is responsible for managing key regeneration.

The default value is `30days`, which means keys are generated after thirty days. Minimum duration is 1 day.

perbackup

Generates keys for each backup. Older keys are retained in the wallet for restoring older backups.

disabled

Does not generate keys automatically at regular intervals.

systemdefault

Specifies that this host should use the current administrative domain policy. Valid only as a client-based policy.

7.2.6 requireencryptablemedia

Use the `requireencryptablemedia` policy to control whether Oracle Secure Backup requires a tape capable of hardware encryption.

This policy is ignored if the tape drive is incapable of hardware encryption or cannot identify encryption-capable tapes.

Values

yes

Puts the job into a pending state until a hardware-encryptable tape is made available.

no

Attempts to mount a tape capable of hardware encryption. If mounting such a tape is not possible, then Oracle Secure Backup falls back to software encryption. This value is the default.

7.3 Copy Backup Image Instance Policies

These policies control the behavior of copy instance jobs which copy backup image instances from one storage location to another.

The backup image instance policies are as follows:

- [defaultjobpriority](#) (page 7-7)
- [encryption](#) (page 7-7)
- [copyoptions](#) (page 7-8)

7.3.1 defaultjobpriority

Use the `defaultjobpriority` policy to specify the default priority that is assigned to copy instance jobs. Oracle Secure Backup uses the default priority if not no priority is specified while creating a copy instance job.

Values

n

Specifies the default priority. The default value is 150.

7.3.2 encryption

Use the `encryption` policy to specify whether data written by a copy instance job must be encrypted. This policy can be set at a global level for the administrative domain. It can be overridden at the client level, using the `--encryption` option of the `cpinstance` command.

Values

required

Encrypts all the backup image instances, regardless of policy settings on specific clients or jobs. If this policy is enabled at the administrative domain level, then all backup image instances written to a storage device are encrypted, regardless of other policies for specific clients or settings for specific copy instance jobs. If this policy is defined at the client level, then all backup image instances written to a storage device from this client is encrypted, regardless of settings for specific jobs.

allowed

Does not encrypt backup image instance while writing them to a storage device unless the policy set on a client or the settings for a copy instance job specify encryption. This is the default.

7.3.3 copyoptions

Use the `copyoptions` policy to specify additional options for a backup image instance copy job dispatched by the scheduler used for the `obdup` program. Whenever the scheduler initiates a copy job, it supplies the specified command-line options to `obdup`. For example, you can turn on diagnostic output mode in `obtar` by setting this value to `-d`.

Values

-d

Enables the debug mode for the `obdup` program.

7.4 Cloud Storage Device Policies

These policies allow you to more easily manage cloud storage devices.

The cloud storage device policies are as follows:

- [proxyserver](#) (page 7-8)
- [proxyuser](#) (page 7-8)
- [proxypassword](#) (page 7-9)
- [segmentsize](#) (page 7-9)
- [streamsperjob](#) (page 7-9)
- [transfertimeout](#) (page 7-9)
- [usepersistentcon](#) (page 7-9)

7.4.1 proxyserver

If a proxy server is specified, then Oracle Secure Backup uses it to connect to Oracle Cloud Infrastructure.

Values

There is no default value.

7.4.2 proxyuser

This policy defines the credentials if your proxy server requires a user name.

Values

There is no default value.

7.4.3 proxypassword

This policy provides a password if your proxy server requires authentication for connecting to Oracle Cloud Infrastructure.

Values

There is no default value.

7.4.4 segmentsize

A backup is split into multiple segments for uploading to Oracle Cloud Infrastructure. This policy defines the size of a segment.

Values

The default value is 10485760.

7.4.5 streamsperjob

This policy defines the number of parallel connections that Oracle Secure Backup makes for each job when uploading backups to Oracle Cloud Infrastructure.

Values

The default value is 4.

7.4.6 transfertimeout

This policy defines the amount of time that Oracle Secure Backup waits before aborting an operation.

Values

The default value is 5 minutes.

7.4.7 usepersistentcon

When this policy is set, Oracle Secure Backup attempts to use an existing connection. If the policy is off, then Oracle Secure Backup always creates a new connection for each request.

Values

The default value is `yes`.

7.5 Daemon Policies

These policies control aspects of the behavior of [daemons](#) and services. For example, you can specify whether logins should be audited and control how the index daemon updates the [catalog](#).

The daemon policies are as follows:

- [auditlogins](#) (page 7-10)
- [obhttpdwindowslogon](#) (page 7-10)
- [obhttpdwindowpassword](#) (page 7-10)
- [obixdmaxupdaters](#) (page 7-10)
- [obixdrechecklevel](#) (page 7-11)
- [obixdupdaternicevalue](#) (page 7-11)
- [webautostart](#) (page 7-11)
- [webpass](#) (page 7-12)
- [windowscontrolcertificateservice](#) (page 7-13)

7.5.1 auditlogins

Use the `auditlogins` policy to audit attempts to log in to Oracle Secure Backup.

Values

yes

Enables the policy. All attempts to log in to Oracle Secure Backup are logged by the administrative `observed` to its log file.

no

Disables the policy (default).

7.5.2 obhttpdwindowslogon

Use the `obhttpdwindowslogon` policy to set a username to access the Oracle Secure Backup Web Server on a Windows administrative domain.

Values

username

Specifies the Windows username or domain username. By default, no username is set.

7.5.3 obhttpdwindowpassword

Use the `obhttpdwindowpassword` policy to set the password for the username created using the [obhttpdwindowslogon](#) (page 7-10) policy.

Values

password

Specifies the password for the Windows administrative username. By default, no password is set.

7.5.4 obixdmaxupdaters

Use the `obixdmaxupdaters` policy to specify the maximum number of [catalog](#) update processes that can operate concurrently.

The Oracle Secure Backup index daemon (`obixd`) is a daemon that manages the Oracle Secure Backup catalogs for each [client](#). Oracle Secure Backup starts the index daemon at the conclusion of each backup and at other times throughout the day.

Values

n

Specifies the number of concurrent `obixd` [daemons](#) to allow. The default is 2.

7.5.5 obixdrechecklevel

Use the `obixdrechecklevel` policy to control the level of action by the Oracle Secure Backup index daemon to ensure that a host backup catalog is valid before making it the official [catalog](#).

Values

structure

Specifies that the index daemon should verify that the structure of the catalog is sound after any updates to a backup catalog (default). This verification is a safeguard mechanism and is used to by the index daemon to double-check its actions after a catalog update.

content

Specifies that the index daemon should verify that the structure and content of the catalog is sound after any updates to a backup catalog. This is the most time-consuming and comprehensive method.

none

Specifies that the index daemon should take no extra action to affirm the soundness of the catalog after updates to the backup catalog. This is the fastest but also the least safe method.

7.5.6 obixdupdaternicevalue

Use the `obixdupdaternicevalue` policy to set the priority at which the index daemon runs. The higher the value, the more of the CPU the index daemon yields to other competing processes. This policy is not applicable to Windows hosts.

Values

n

Specifies the index daemon priority. The default is 0, which means that the index daemon runs at a priority assigned by the system, which is normal process priority. You can use a positive value (1 to 20) to decrease the priority, thereby making more CPU time available to other processes. To give the daemon a higher priority, enter a negative number.

7.5.7 webautostart

Use the `webautostart` policy to specify whether the [Apache Web server](#) automatically starts when you restart `observed`.

Values

yes

Enables the policy.



Note:

The installation process sets `webautostart` to `yes`, which is not the default value.

no

Disables the policy (default).

7.5.8 webpass

Use the `webpass` policy to specify a password to be passed to the Web server.

If the Web server's [Secure Sockets Layer \(SSL\) certificate](#) requires a password (PEM pass phrase), then entering it in this policy enables `observed` to pass it to the Oracle Secure Backup Web server when it is started. The password is used when decrypting certificate data stored locally on the [administrative server](#) and never leaves the computer.

The installation script configures a password for the `webpass` policy. You can change this password, although in normal circumstances you should not be required to do so.

Values

password

Specifies the password.

Required Actions If the Web Server Password Is Changed

If you change the Oracle Secure Backup Web tool server password, then you must regenerate the web server key and certificate. Use the following procedure:

1. At the command line, issue the `obwebcert upgrade` command, and follow the instructions given:

```
# obwebcert upgrade
```

```
Please enter admin password:
```

```
Web Certificate has been successfully updated.
```

```
The Oracle Secure Backup Service Daemon (observed) will need to be  
restarted before the web server will be functional. Please execute the  
following
```

```
command to restart observed:
```

```
obctl restart
```

```
# obctl restart
```

```
Oracle Secure Backup Service Daemon has been stopped.
```

```
Oracle Secure Backup Service Daemon has been started.
```

```
#
```

2. Confirm that the `obhttpd` daemons are running. You can do so by logging in to the Web tool, or on Linux and UNIX systems you can also issue a `ps -ef | grep ob` command.

7.5.9 windowscontrolcertificateservice

Use the `windowscontrolcertificateservice` to specify whether Oracle Secure Backup should attempt to put the Windows `certificate` service in the appropriate mode before backing up or recovering a certificate service database.

Values

yes

Specifies that Oracle Secure Backup should start the certificate service before a backup, stop it, and then restart the certificate service for a restore.

no

Disables the policy (default).

7.6 Device Policies

These policies control how a `tape device` is automatically detected during `device discovery` and when tape device write warnings are generated.

The device policies are as follows:

- [checkserialnumbers](#) (page 7-13)
- [deletediskorphans](#) (page 7-14)
- [disableasyncio](#) (page 7-15)
- [discovereddevicestate](#) (page 7-15)
- [errorrate](#) (page 7-15)
- [maxdriveidletime](#) (page 7-15)
- [maxacsejectwaittime](#) (page 7-16)
- [poolfreespacegoal](#) (page 7-17)
- [returntoservicecheck](#) (page 7-17)

7.6.1 checkserialnumbers

Use the `checkserialnumbers` policy to control `tape device` serial number checking.

While not a requirement of the SCSI-2 standard, practically all modern tape drives and libraries support the Unit Serial Number Inquiry Page, by which a device can be programmatically interrogated for its serial number.

If the `checkserialnumbers` policy is enabled, then whenever Oracle Secure Backup opens a tape device, it checks the serial number of that device. If the tape device does not support serial number reporting, then Oracle Secure Backup simply opens the tape device. If the tape device does support serial number checking, then Oracle Secure Backup compares the reported serial number to the serial number stored in the device object. Three results are possible:

- There is no serial number in the device object.
If Oracle Secure Backup has never opened this tape drive since the device was created or the serial number policy was enabled, then it cannot have stored a serial number in the device object. In this case, the serial number is stored in the device object, and the open succeeds.
- There is a serial number in the device object, and it matches the serial number just read from the device.
In this case, Oracle Secure Backup opens the tape device.
- There is a serial number in the device object, and it does not match the serial number just read from the device.
In this case, Oracle Secure Backup returns an error message and does not open the tape device.

**Note:**

Oracle Secure Backup also performs serial number checking as part of the `--geometry/-g` option to the `obtool lsdev` command. This option causes an Inquiry command to be sent to the specified device, and `lsdev` displays its vendor, product ID, firmware version, and serial number.

Values**Yes**

Specifies that serial numbers are checked whenever a tape device is opened. This is the default value.

No

Specifies that tape device serial numbers are ignored.

7.6.2 deletediskorphans

Use the `deletediskorphans` policy to control the automatic daily (midnight) clean-up of disk pool orphans from the disk pool. A disk pool orphan is a backup image that exists in the disk pool but has not been put into the catalog database. This can occur if there is a failure during the backup operation.

You must catalog any disk pool that you import in your domain. If you do not catalog the imported disk pool before the automatic orphan clean-up, then all your backup files that do not have corresponding catalog entries will be seen as [disk pool orphans](#) and will be deleted.

Values**yes**

Specifies that the daily orphan clean-up is enabled. Set to this value after cataloging your disk pool.

no

Specifies that the daily disk orphan clean-up is disabled. This is the default setting.

7.6.3 disableasyncio

Use the `disableasyncio` policy to control the use of asynchronous I/O throughout the administrative domain. Asynchronous I/O enables you to improve the write throughput for tape devices that support multiple command queues.

Values

yes

Specifies that asynchronous I/O is disabled.

no

Specifies that asynchronous I/O is enabled. This is the default setting.

7.6.4 discovereddevicestate

Use the `discovereddevicestate` policy to determine whether a [tape device](#) discovered by the `discoverdev` (page 2-85) command is immediately available for use by Oracle Secure Backup.

Values

in service

Specifies that discovered tape devices are available to Oracle Secure Backup immediately.

not in service

Specifies that discovered tape devices are not available to Oracle Secure Backup until explicitly placed in service (default).

7.6.5 errorrate

Use the `errorrate` policy to set the [error rate](#). The error rate is the ratio of recovered write errors that occur during a [backup job](#) per the total number of blocks written, multiplied by 100. If the error rate for any backup is higher than this setting, then Oracle Secure Backup displays a warning message in the [backup transcript](#).

Values

n

Specifies the error rate to be used with the [tape device](#). The default is 8.

none

Disables error rate checking. You can disable error rate checking to avoid warning messages when working with a [tape drive](#) that does not support the [Small Computer System Interface \(SCSI\)](#) commands necessary to check the error rate.

7.6.6 maxdriveidletime

Use the `maxdriveidletime` policy to set how long a tape can remain idle in a [tape drive](#) after the conclusion of a backup or restore operation. When this set time is up, Oracle Secure Backup automatically unloads the tape from the tape drive.

You cannot specify this parameter on a drive-by-drive basis. You must have the [modify administrative domain's configuration](#) (page 8-4) right to modify this policy.

Values

duration

Specifies the length of time that a tape can remain idle before Oracle Secure Backup unloads it. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default is `5minutes`, which means that Oracle Secure Backup unloads a tape when it has been idle for five minutes.



Note:

The `duration` placeholder must be specified by some combination of `seconds`, `minutes` and `hours` only.

The minimum value that can be specified is `0seconds`. The maximum value is `24hours`. A duration of `0` results in an immediate tape unload at the conclusion of any backup or restore operation.

forever

Specifies that a tape remains in the tape drive at the conclusion of a backup or restore operation. The tape is not unloaded automatically.

7.6.7 maxacsejectwaittime

This policy applies only to StorageTek Automated Cartridge System Library Software (ACSL) systems. Use the `maxacsejectwaittime` policy to set how long an outstanding `exportvol` request waits for the ACS cartridge access port to be cleared.

Values

duration

Specifies the length of time that Oracle Secure Backup waits for an ACS cartridge access port to be cleared before canceling an `exportvol` request.

Manual [operator](#) intervention is required to remove the tapes from the cartridge access port after an ACS `exportvol` operation has finished. Access to the ACSLS server is denied until the tapes are removed or a period greater than `maxacsjectwaittime` has passed. Oracle recommends that you schedule exports only when a human operator is locally available and that you batch export operations such that multiple volumes are specified for each `exportvol` operation.

Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default is `5minutes`.



Note:

The `duration` placeholder must be specified by some combination of `seconds`, `minutes` and `hours` only.

The minimum value that can be specified is `0seconds`. The maximum value is `forever`.

forever

Specifies that Oracle Secure Backup never cancels an `exportvol` request while waiting for an ACS cartridge access port to clear.

7.6.8 `poolfreespacegoal`

Use the `poolfreespacegoal` policy to control the amount of free space that must be maintained in the pool at any point-in-time. The scheduler maintains this space by deleting expired backup image instances.

Values***n***

Specifies the amount of free space that must be available in the disk pool. The value is expressed as a percentage of the total disk pool capacity.

7.6.9 `returntoservicecheck`

Use the `returntoservicecheck` policy to check the accessibility status of a disk pool or tape device, that was previously taken offline, before automatically returning it to service.

Values**yes**

Specifies that Oracle Secure Backup checks the accessibility status of the device before it is returned to service.

no

Specifies that Oracle Secure Backup automatically returns a device to service once its out-of-service timer expires. This is the default setting.

7.7 Duplication Policies

These policies control how Oracle Secure Backup performs [volume](#) duplication.

The volume duplication policies are as follows:

- [duplicateovernetwork](#) (page 7-17)
- [duplicationjobpriority](#) (page 7-18)
- [duplicationoptions](#) (page 7-18)

7.7.1 `duplicateovernetwork`

Use the `duplicateovernetwork` policy to control whether Oracle Secure Backup is allowed to duplicate a [volume](#) to a different [media server](#) than the one containing the [original volume](#) being duplicated. Oracle Secure Backup does not duplicate between tape devices attached to different media servers by default, because it requires heavy use of network bandwidth.

Values**yes**

Allow duplication between tape devices attached to different media servers.

no

Disallow duplication between tape devices attached to different media servers. This is the default value.

7.7.2 duplicationjobpriority

Use the `duplicationjobpriority` policy to specify the priority of **volume** duplication jobs relative to other jobs.

Values***n***

Specifies the priority of the job. Default: 200.

**Note:**

By default, backup jobs are scheduled with a priority of 100. As a result, backup jobs take precedence over volume duplication jobs by default.

7.7.3 duplicationoptions

Use the `duplicationoptions` policy to specify additional options that are used during duplication. The option values must be preceded by a hyphen (-).

Values**d**

Enables debug mode. When specified, additional information is printed in the duplication job transcript. This option does not take any argument.

K *mask*

Specifies device driver debug options. *mask* is the bitwise inclusive or one of the values listed in [Table B-3](#) (page B-21).

l

Does not display volume label details in duplication job transcripts during a copy operation.

N

Does not use the tape helper during the duplication operation.

n

Uses NDMP to perform the volume duplication. This is the default setting.

s

Uses the SCSI interface to perform volume duplication, instead of the NDMP protocol. This option cannot be used with `-n`.

7.8 Index Policies

These policies control how Oracle Secure Backup generates and manages the [catalog](#). For example, you can specify the amount of elapsed time between catalog cleanups.

The index policies are as follows:

- [asciiindexrepository](#) (page 7-19)
- [autoindex](#) (page 7-19)
- [earliestindexcleanuptime](#) (page 7-19)
- [generatendmpindexdata](#) (page 7-20)
- [indexcleanupfrequency](#) (page 7-20)
- [latestindexcleanuptime](#) (page 7-20)
- [maxindexbuffer](#) (page 7-20)
- [positiondatainterval](#) (page 7-21)
- [saveasciiindexfiles](#) (page 7-21)

7.8.1 asciiindexrepository

Use the `asciiindexrepository` policy to specify the directory where ASCII index files are saved before being imported into the Oracle Secure Backup [catalog](#) by the index daemon.

Values

pathname

Specifies the path name for the index files. The default path name is the `admin/history/host/hostname` subdirectory of the [Oracle Secure Backup home](#).

7.8.2 autoindex

Use the `autoindex` policy to specify Oracle Secure Backup whether backup [catalog](#) data should be produced for each backup it performs.

Values

yes

Specifies that catalog data should be produced for each backup (default).

no

Specifies that catalog data should not be produced for each backup.

7.8.3 earliestindexcleanuptime

Use the `earliestindexcleanuptime` policy to specify the earliest time of day at which [catalog](#) information should be cleaned up. Cleanup activities should take place during periods of lowest usage of the [administrative server](#).

Values

time

Specifies the time in hour and minutes. Refer to "[time](#) (page 4-29)" for a description of the `time` placeholder. The default value is `23:00`.

7.8.4 generatendmpindexdata

Use the `generatendmpindexdata` policy to specify whether Oracle Secure Backup should produce backup [catalog](#) information when backing up a [client](#) accessed through [Network Data Management Protocol \(NDMP\)](#).

Values

yes

Specifies that catalog data should be produced for backups of NDMP clients (default).

no

Specifies that catalog data should not be produced for backups of NDMP clients.

7.8.5 indexcleanupfrequency

Use the `indexcleanupfrequency` policy to specify the amount of elapsed time between [catalog](#) cleanups.

Typically, you should direct Oracle Secure Backup to clean up catalogs on a regular basis. This technique eliminates stale data from the catalog and reclaims disk space. Catalog cleanup is a CPU-intensive and disk I/O-intensive activity, but Oracle Secure Backup performs all data backup and restore operations without interruption when catalog cleanup is in progress.

Values

duration

Specifies the frequency of catalog cleanup operations. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default is `21days`, which means that Oracle Secure Backup cleans the catalog every three weeks.

7.8.6 latestindexcleanuptime

Use the `latestindexcleanuptime` policy to specify the latest time of day at which index catalogs can be cleaned up.

Values

time

Specifies the latest index cleanup time. Refer to "[time](#) (page 4-29)" for a description of the `time` placeholder. The default value is `07:00`.

7.8.7 maxindexbuffer

Use the `maxindexbuffer` policy to specify a maximum file size for the local index buffer file.

Backup performance suffers if index data is written directly to an [administrative server](#) that is busy with other tasks. To avoid this problem, Oracle Secure Backup buffers index data in a local file on the [client](#) during the backup, which reduces the number of interactions that are required with an administrative server. This policy enables you to control the maximum size to which this buffer file can grow.

Values

bufferize

Specifies the buffer size in blocks of size 1 KB. The default value is 6144, which is 6 MB. Setting the buffer size to 0 causes Oracle Secure Backup to perform no local buffering.

7.8.8 positiondatainterval

Use the `positiondatainterval` policy to specify the amount of data in KB that must be written to tape before a position mark is written to the tape.

Oracle Secure Backup uses this information during subsequent restore jobs to rapidly position a tape to the requested files.

Values

n

Specifies the position data interval in terms of KB transferred. The default value is 1024 (1 MB), which means that information is obtained after Oracle Secure Backup writes each 1 MB (1024*1024) of data to tape.

7.8.9 saveasciindexfiles

Use the `saveasciindexfiles` policy to determine whether to save or delete temporary ASCII files used by the index daemon.

When Oracle Secure Backup performs a backup, it typically generates index information that describes each file-system object it saves. Specifically, it creates a temporary ASCII file on the [administrative server](#) in the `admin/history/index/client` subdirectory of the [Oracle Secure Backup home](#). When the backup completes, the index daemon imports the index information into the index [catalog](#) file for the specified [client](#).

Values

yes

Directs Oracle Secure Backup to retain each temporary ASCII index file. This option might be useful if you have written tools to analyze the ASCII index files and generate site-specific reports.

no

Directs Oracle Secure Backup to delete each temporary ASCII index file when the backup completes (default).

7.9 Log Policies

These policies control historical logging in the [administrative domain](#). For example, you can specify which events should be recorded in the activity log on the [administrative server](#): all, backups only, restore operations only, and so forth.

The log policies are as follows:

- [adminlogevents](#) (page 7-22)
- [adminlogfile](#) (page 7-22)
- [clientlogevents](#) (page 7-23)
- [jobretaintime](#) (page 7-23)
- [logretaintime](#) (page 7-23)
- [transcriptlocation](#) (page 7-23)
- [transcriptretaintime](#) (page 7-24)
- [unixclientlogfile](#) (page 7-24)
- [windowsclientlogfile](#) (page 7-24)

7.9.1 adminlogevents

Use the `adminlogevents` policy to specify the events to be logged in the activity log on the [administrative server](#). Separate multiple event types with a comma. By default this policy is not set, which means that no activity log is generated.

Values

backup

Logs all backup events.

backup.commandline

Logs command-line backups that specify files to be backed up on the command line.

backup.scheduler

Logs [scheduled backup](#) operations.

restore

Logs restore operations.

all

Logs everything specified by the preceding options.

7.9.2 adminlogfile

Use the `adminlogfile` policy to specify the path name for the activity log on the [administrative server](#).

Values

pathname

Specifies the path name of a log file, for example, `/var/log/admin_srvr.log`. By default this policy is not set, which means that no log file is generated.

7.9.3 clientlogevents

Use the `clientlogevents` policy to specify the events to be logged in the activity log on the `client` host.

Values

See the values for the `adminlogevents` (page 7-22) policy. By default this policy is not set.

7.9.4 jobretaintime

Use the `jobretaintime` policy to set the length of time to retain `job list` history.

Once a job completes the duration value specified in the `jobretaintime` policy, the job history in the obscheduled process is refreshed and information for that job is no longer available.

Values

duration

Retains the job history for the specified period. The default is `30days`. Refer to "`duration` (page 4-14)" for a description of the `duration` placeholder.

7.9.5 logretaintime

Use the `logretaintime` policy to set the length of time to retain Oracle Secure Backup log files.

Several components of Oracle Secure Backup maintain log files containing diagnostic messages. This option lets you limit the size of these files, which can grow quite large. Oracle Secure Backup periodically deletes all entries older than the specified duration.

Values

duration

Retains the diagnostic logs for the specified period. The default is `7days`. Refer to "`duration` (page 4-14)" for a description of the `duration` placeholder.

7.9.6 transcriptlocation

Use the `transcriptlocation` policy to determine the location of the job transcripts.

Values

admin

Lists job transcripts stored on the administrative server.

mediaserver

Lists the job transcripts stored on each media server host. This is the default value.

7.9.7 transcriptretaintime

Use the `transcriptretaintime` policy to specify the length of time to retain Oracle Secure Backup job transcripts.

When the Oracle Secure Backup [scheduler](#) runs a job, it saves the job output in a transcript file. You can specify how long transcript files are to be retained.

Values***duration***

Retains the job transcripts for the specified period. The default is `7days`. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder.

7.9.8 unixclientlogfile

Use the `unixclientlogfile` policy to specify the path name for log files on UNIX [client](#) hosts. Oracle Secure Backup logs each of the events selected for [clientlogevents](#) (page 7-23) to this file on every UNIX client.

Values***pathname***

Specifies the path name for the log files on UNIX clients. By default this policy is not set, which means that no log file is generated.

7.9.9 windowsclientlogfile

Use the `windowsclientlogfile` to specify the path name for log files on Windows [client](#) hosts. Oracle Secure Backup logs each of the events selected for [clientlogevents](#) (page 7-23) to this file on each Windows client.

Values***pathname***

Specifies the path name for the log files on Windows clients. By default this policy is not set, which means that no log file is generated.

7.10 Media Policies

These policies control domain-wide media management. For example, you can specify a [retention period](#) for tapes that are members of the null [media family](#).

The media policies are as follows:

- [barcodesrequired](#) (page 7-25)
- [blockingfactor](#) (page 7-25)
- [freedstucktapethreshold](#) (page 7-25)
- [maxblockingfactor](#) (page 7-26)

- [overwriteblanktape](#) (page 7-26)
- [overwriteforeigntape](#) (page 7-26)
- [overwriteunreadabletape](#) (page 7-27)
- [volumeretaintime](#) (page 7-27)
- [writewindowtime](#) (page 7-27)

7.10.1 barcodesrequired

Use the `barcodesrequired` policy to determine whether every tape is required to have a readable `barcode`.

By default, Oracle Secure Backup does not discriminate between tapes with readable barcodes and those without. This policy ensures that Oracle Secure Backup can always solicit a tape needed for restore by using both the barcode and the `volume ID`. Use this feature only if every `tape drive` is contained in a `tape library` with a working barcode reader.

Values

default

States that the current device contains readable barcodes.

yes

Requires tapes to have readable barcodes.

no

Does not require tapes to have readable barcodes (default).

7.10.2 blockingfactor

Use the `blockingfactor` policy to define the size of every tape block written during a backup or restore operation. You can modify this value so long as it does not exceed the limit set by the `maxblockingfactor` (page 7-26) policy.

See Also:

Oracle Secure Backup Administrator's Guide for more information on blocking factors

Values

unsigned integer

Specifies the block factor in blocks of size 512 bytes. The default value is 128, which means that Oracle Secure Backup writes 64 KB blocks to tape.

7.10.3 freedstucktapethreshold

Use the `freedstucktapethreshold` policy to specify the maximum number of attempts that Oracle Secure Backup makes to free a tape that it considers stuck (partially inserted) in a tape drive or storage element.

Values

n

Specifies the number of attempts that Oracle Secure Backup makes to free a stuck tape. The default is 2.

7.10.4 maxblockingfactor

Use the `maxblockingfactor` policy to define the maximum size of a tape block read or written during a backup or restore operation. Blocks over this size are not readable.



See Also:

Oracle Secure Backup Administrator's Guide for more information on maximum blocking factors

Values

unsigned integer

Specifies the maximum block factor in blocks of size 512 bytes. The default value is 128, which represents a maximum block size of 64 KB. The maximum setting is 4096, which represents a maximum tape block size of 2 MB. This maximum is subject to further constraints by `tape device` and operating system limitations outside of the scope of Oracle Secure Backup.

7.10.5 overwriteblanktape

Use the `overwriteblanktape` policy to specify whether Oracle Secure Backup should **overwrite** a blank tape.

Values

yes

Overwrites blank tapes (default).

no

Does not overwrite blank tapes.

7.10.6 overwriteforeigntape

Use the `overwriteforeigntape` policy to specify whether Oracle Secure Backup should **overwrite** an automounted tape recorded in an unrecognizable format.

Values

yes

Overwrites tapes in an unrecognized format.

no

Does not overwrite tapes in an unrecognized format (default).

7.10.7 overwriteunreadabletape

Use the `overwriteunreadabletape` policy to specify whether Oracle Secure Backup should [overwrite](#) a tape whose first block cannot be read.

Values

yes

Overwrites unreadable tapes.

no

Does not overwrite unreadable tapes (default).

7.10.8 volumeretaintime

Use the `volumeretaintime` policy to specify a [retention period](#) for tapes that are members of the `null` [media family](#).

Values

duration

Retains the volumes for the specified period. The default is `disabled`, which means that the volumes do not automatically expire. You can [overwrite](#) or unlabel the [volume](#) at any time. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder.

7.10.9 writewindowtime

Use the `writewindowtime` policy to specify a write-allowed time for tapes that are members of the `null` [media family](#).

Values

duration

Retains the volumes for the specified period. The default is `disabled`, which means that the [write window](#) never closes. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder.

7.11 Naming Policies

This class contains a single policy, which specifies a WINS server for the [administrative domain](#).

The naming policy is as follows:

- [winsserver](#) (page 7-27)

7.11.1 winsserver

Use the `winsserver` policy to specify an IP address of a Windows Internet Name Service (WINS) server. The WINS server is used throughout the [administrative domain](#).

Oracle Secure Backup provides the ability for UNIX systems to resolve Windows [client](#) host names through a WINS server. Setting this policy enables Oracle Secure Backup to support clients that are assigned IP addresses dynamically by WINS.

Values

wins_ip

Specifies a WINS server with the IP address *wins_ip*. By default this policy is not set.

7.12 NDMP Policies

These policies specify [Network Data Management Protocol \(NDMP\) data management application \(DMA\)](#) defaults. For example, you can specify a password used to authenticate Oracle Secure Backup to each NDMP server.

The NDMP policies are as follows:

- [authenticationtype](#) (page 7-28)
- [backupev](#) (page 7-28)
- [backuptype](#) (page 7-29)
- [dmahosts](#) (page 7-29)
- [password](#) (page 7-29)
- [port](#) (page 7-30)
- [protocolversion](#) (page 7-30)
- [restoreev](#) (page 7-30)
- [username](#) (page 7-31)

7.12.1 authenticationtype

Use the `authenticationtype` policy to specify the means by which the Oracle Secure Backup [Network Data Management Protocol \(NDMP\) client](#) authenticates itself to an NDMP server.

You can change the authentication type for individual hosts by using the `--ndmpauth` option of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

Values

authtype

Specifies the authentication type. Refer to "[authtype](#) (page 4-3)" for a description of the `authtype` placeholder. The default is `negotiated`, which means that Oracle Secure Backup determines (with the NDMP server) the best authentication mode to use. Typically, you should use the default setting.

7.12.2 backupev

Use the `backupev` policy to specify backup environment variables. Oracle Secure Backup passes each variable to the [client](#) host's [Network Data Management Protocol \(NDMP\) data service](#) every time it backs up NDMP-accessed data.

 **Note:**

NDMP environment variables are specific to each data service. For this reason, specify them only if you are knowledgeable about the data service implementation.

You can also select client host-specific environment variables, which are sent to the NDMP data service each time data is backed up from or recovered to the client host, by using the `--backupev` and `--restoreev` options of the `mkhost` (page 3-26) and `chhost` (page 2-43) commands.

Values***name=value***

Specifies a backup environment variable name and value, for example, `VERBOSE=y`. By default the policy is not set.

7.12.3 backuptype

Use the `backuptype` policy to specify a default backup type. Backup types are specific to [Network Data Management Protocol \(NDMP\)](#) data services; a valid backup type for one [data service](#) can be invalid, or undesirable, for another. By default Oracle Secure Backup chooses a backup type appropriate to each data service.

You can change the backup type for individual hosts by using the `--ndmpbackuptype` option of the `mkhost` (page 3-26) and `chhost` (page 2-43) commands.

Values**`ndmp-backup-type`**

Specifies a default backup type. Refer to "[ndmp-backup-type](#) (page 4-20)" for a description of the `ndmp-backup-type` placeholder.

7.12.4 dmahosts

Use the `dmahosts` policy to list Oracle Secure Backup hosts eligible to run the NDMP Data Management Agent ([DMA](#)) while performing backups on a third-party NDMP server.

You can add a comma separated list of hosts running the Oracle Secure Backup software with either the admin sever role or the media server role.

7.12.5 password

Use the `password` policy to specify a password used to authenticate Oracle Secure Backup to each [Network Data Management Protocol \(NDMP\)](#) server.

You can change the NDMP password for individual hosts by using the `--ndmppass` option of the `mkhost` (page 3-26) and `chhost` (page 2-43) commands.

Values

password

Specifies a password for NDMP authentication. By default this policy is not set, that is, the default password is null.

7.12.6 port

Use the `port` policy to specify a TCP port number for use with [Network Data Management Protocol \(NDMP\)](#).

You can change the TCP port for individual hosts by using the `--ndmpport` option of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

Values

port_num

Specifies a TCP port number. The default value for `port_num` is 10000.

7.12.7 protocolversion

Use the `protocolversion` policy to specify a [Network Data Management Protocol \(NDMP\)](#) version.

Typically, you should let Oracle Secure Backup negotiate a protocol version with each NDMP server (default). If it is necessary for testing or some other purpose, then you can change the NDMP protocol version with which Oracle Secure Backup communicates with this server. If an NDMP server cannot communicate using the protocol version you select, then Oracle Secure Backup reports an error rather than using a mutually supported version.

You can change the NDMP protocol version for individual hosts by using the `--ndmpver` option of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

Values

protocol_num

Specifies a protocol number. Refer to "[protover](#) (page 4-24)" for a description of the `protover` placeholder. The default is 0, which means "as proposed by server."

7.12.8 restoreev

Use the `restoreev` policy to specify restore environment variables. Oracle Secure Backup passes each variable to the `client` host's [Network Data Management Protocol \(NDMP\) data service](#) every time it recovers NDMP-accessed data.

You can also select client host-specific environment variables, which are sent to the NDMP data service each time data is backed up from or recovered to the client host, by using the `--backupev` and `--restoreev` options of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

 **Note:**

NDMP environment variables are specific to each data service. For this reason, specify them only if you are knowledgeable with the data service implementation.

Values***name=value***

Specifies a backup environment variable name and value, for example, `VERBOSE=y`. By default the policy is not set.

7.12.9 username

Use the `username` policy to specify the name used to authenticate Oracle Secure Backup to each [Network Data Management Protocol \(NDMP\)](#) server.

You can change the NDMP username for individual hosts by using the `--ndmpuser` option of the [mkhost](#) (page 3-26) and [chhost](#) (page 2-43) commands.

Values***username***

Specifies a username for authentication on NDMP servers. The default is `root`.

7.13 Operations Policies

These policies control various backup and restore operations. For example, you can set the amount of time that a [Recovery Manager \(RMAN\) backup job](#) waits in the Oracle Secure Backup [scheduler](#) queue for the required resources to become available.

The operations policies are as follows:

- [autohistory](#) (page 7-32)
- [autolabel](#) (page 7-32)
- [backupimagerechecklevel](#) (page 7-32)
- [backupoptions](#) (page 7-33)
- [databuffersize](#) (page 7-33)
- [disablerds](#) (page 7-34)
- [fullbackupcheckpointfrequency](#) (page 7-34)
- [incrbackupcheckpointfrequency](#) (page 7-34)
- [overwritecheckfrequency](#) (page 7-35)
- [mailport](#) (page 7-35)
- [mailserver](#) (page 7-35)
- [mailfrom](#) (page 7-35)
- [maxcheckpointrestarts](#) (page 7-36)

- [maxentriesrestoreoperation](#) (page 7-36)
- [progressupdatefrequency](#) (page 7-36)
- [restoreoptions](#) (page 7-37)
- [rmanpriority](#) (page 7-37)
- [restartablebackups](#) (page 7-36)
- [rmanresourcewaittime](#) (page 7-38)
- [rmanrestorestartdelay](#) (page 7-38)
- [tcpbufsize](#) (page 7-38)
- [useloadbalance](#) (page 7-38)
- [windowsskipcdfs](#) (page 7-39)
- [windowsskiplockedfiles](#) (page 7-39)

7.13.1 autohistory

Use the `autohistory` policy to specify whether Oracle Secure Backup updates backup history data every time a [client](#) host is backed up. This history data is used to form file selection criteria for an [incremental backup](#).

Values

yes

Updates backup history data when a client host is backed up (default). This history data is used to form file selection criteria for incremental backups.

no

Does not update backup history data when a client host is backed up.

7.13.2 autolabel

Use the `autolabel` policy to specify whether Oracle Secure Backup creates a [volume label](#) and a [backup image label](#) for a [backup image](#) whenever it backs up data.

Values

yes

Enables label generation (default).

no

Disables label generation. You should not disable label generation unless directed by Oracle Support Services.

7.13.3 backupimagerechecklevel

Use the `backupimagerechecklevel` policy to specify whether Oracle Secure Backup performs block-level verification after each [backup section](#) is completed.

Oracle Secure Backup can optionally reread each block that it writes to tape during a [backup job](#). It provides a second verification that the backup data is readable. The first check is performed by the read-after-write logic of the [tape drive](#) immediately after the data is written.

Values

block

Performs block-level verification after each backup section is completed. Oracle Secure Backup backs up the tape to the beginning of the backup section, reads the contents, and performs one of these actions:

- Leaves the tape positioned after the backup section if it was the last section of the backup
- Continues with [volume](#) swap handling if it has more data to write

 **Note:**

Choosing `block` substantially increases the amount of time it takes to back up data.

none

Performs no verification (default).

7.13.4 backupoptions

Use the `backupoptions` policy to specify additional options to apply to backups dispatched by the [scheduler](#). Whenever the scheduler initiates a backup, it supplies the specified command-line options to `obtar`. For example, you can turn on diagnostic output mode in `obtar` by setting this value to `-j`.

Values

obtar-options

Specifies user-supplied `obtar` options. See "[obtar Options](#) (page B-14)" for details on `obtar` options. By default no options are set.

 **Note:**

Whatever you enter is passed directly to `obtar`, so be sure to specify valid options. Otherwise, your backup or restore jobs fails to run.

7.13.5 databuffersize

Use the `databuffersize` policy to control the size of the shared memory buffer used for data transfer in a local file-system backup or restore operation. It is expressed in tape blocks, and the default value is 6. The default size of this shared memory, therefore, is 6 times the current tape block size.

You can use this policy to tune backup performance. It is relevant only to file-system backup and restore operations where the client and the media server are collocated.

**See Also:**

"[blockingfactor](#) (page 7-25)" for more information on tape block size

7.13.6 `disablerds`

Use the `disablerds` policy to specify whether Reliable Datagram Socket (RDS) is used for communication between the client and media server. Where possible, Remote Direct Memory Access (RDMA) is used along with RDS. To use RDS, the client and media server must be connected over Infiniband.

This setting, which is applicable to the entire administrative domain, can be overridden at the host level by using the `--disablerds` option of the `chhost` or `mkhost` commands.

**See Also:**

"[chhost](#) (page 2-43)" and `mkhost`"[mkhost](#) (page 3-26)" for more information about `--disablerds`

Values

yes

Does not use RDS over Infiniband to transfer data between the client and media server. Instead TCP/IP is used for communication.

no

Uses RDS over Infiniband to transfer data between the client and media server. This is the default setting.

7.13.7 `fullbackupcheckpointfrequency`

Use the `fullbackupcheckpointfrequency` policy to specify checkpoint frequency, that is, how often Oracle Secure Backup takes a checkpoint during a [full backup](#) for restartable backups.

Values

nMB

Takes a checkpoint after every *n* MB transferred to a [volume](#).

nGB

Takes a checkpoint after every *n* GB transferred to a volume. By default, Oracle Secure Backup takes a checkpoint for every 8 GB transferred to a volume.

7.13.8 `incrbackupcheckpointfrequency`

Use the `incrbackupcheckpointfrequency` policy to specify checkpoint frequency, that is, how often Oracle Secure Backup takes a checkpoint during an [incremental backup](#) for restartable backups.

Values***n*MB**

Takes a checkpoint after every *n* MB transferred to a [volume](#).

***n*GB**

Takes a checkpoint after every *n* GB transferred to a volume. By default, Oracle Secure Backup takes a checkpoint for every 2 GB transferred to a volume.

Choose the period at which Oracle Secure Backup takes a checkpoint during an incremental backup for any backup that is restartable. The value is represented in volume of bytes moved. (In the default case, a checkpoint is taken for each 8 GB transferred to a volume.)

7.13.9 overwritecheckfrequency

Use the `overwritecheckfrequency` policy to control the frequency at which the tape position is monitored for being overwritten.

Values***n***

Indicates the number of blocks that must be written to a tape before the tape position is checked. You can set this value to a minimum of 1024 blocks and a maximum of 65535 blocks. The default value is 1024 blocks.

To disable the checking of tape position to detect overwrite, set the value to 0.

7.13.10 mailport

Use the `mailport` policy to specify the [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#) port number to which Oracle Secure Backup sends e-mail requests from Windows hosts.

Values***port_num***

Specifies a TCP/IP port number. The default value is 25.

7.13.11 mailserv

Use the `mailserver` policy to specify the name of the host to which Oracle Secure Backup sends e-mail requests from Windows hosts.

Values***hostname***

Specifies a host name. The default value is `localhost`.

7.13.12 mailfrom

Use the `mailfrom` policy to specify a *from* address for e-mails generated by Oracle Secure Backup. The default value is (none), in which case the *from* address is

`root@fqdn` OR `SYSTEM@fqdn`, where `fqdn` is the fully qualified domain name of the Oracle Secure Backup [administrative server](#).

Specifying a different address can help in configurations with multiple backup domains, because it minimizes the requirement to configure the mail server to allow e-mail from each specific system.

7.13.13 maxcheckpointrestarts

Use the `maxcheckpointrestarts` policy to specify the maximum number of times Oracle Secure Backup attempts to restart an operation from the same checkpoint. If this limit is reached, then Oracle Secure Backup discards the checkpoint and restarts the backup from the beginning.

Values

n

Specifies the maximum number of restarts. The default value is 5.

7.13.14 maxentriesrestoreoperation

Use the `maxentriesrestoreoperation` policy to set the maximum number of concurrent restore jobs that can be run at a given time. If the maximum number of restore jobs is already running, any additional requests will generate a request error message.

Values

n

Specifies the maximum number of concurrently running restore jobs. The default value is 1,00,000.

7.13.15 progressupdatefrequency

Use the `progressupdatefrequency` policy to control the frequency at which the Oracle Secure Backup data service communicates its progress during a backup or restore operation. The information communicated includes details such as the number of files and the amount of data transferred. You can view this information by using the `--progress` option of the `lsjob` command.

Values

n

Specifies the frequency, in minutes, at which the Oracle Secure Backup data service communicates its progress. The default is 1 minute.

7.13.16 restartablebackups

Use the `restartablebackups` policy to specify whether the restartable backups feature is enabled. This feature enables Oracle Secure Backup to restart certain types of failed backups from a mid-point rather than from the beginning.

Values

yes

Enables restartable backups (default).

 **Note:**

If you use the restartable backups feature, then ensure that the `/tmp` directory on the [administrative server](#) is on a partition that maintains at least 1 GB of free space.

no

Disables restartable backups.

7.13.17 restoreoptions

Use the `restoreoptions` policy to specify additional options to apply to restore operations dispatched by the [scheduler](#). Whenever the scheduler initiates a restore operation, it supplies the specified command-line options to [obtar](#). For example, you can turn on diagnostic output mode in `obtar` by setting this value to `-J`.

Values

obtar-options

Specifies user-supplied `obtar` options. See "[obtar Options](#) (page B-14)" for details on `obtar` options. By default no restore options are set.

 **Note:**

Whatever you enter is passed directly to `obtar`, so be sure to specify valid options. Otherwise, your backup or restore jobs fail to run.

7.13.18 rmanpriority

This topic describes the `rmanpriority` policy and its usage.

Use the `rmanpriority` policy to set the default priority value for scheduling `rman` backup jobs and `rman` restore jobs.

A job priority specified at the database storage selector level or the media management parameter level will override the priority value set using this policy for that particular job.

Values

priority

Sets the default priority value for `rman` backup jobs and restore jobs. This value can range between 1, which specifies the highest priority job, and 214783647, which specifies the lowest priority job. The default priority value is 100.

**See Also:**

[About Setting the Job Priority for RMAN Operations](#) (page C-2)

7.13.19 rmanresourcewaittime

Use the `rmanresourcewaittime` policy to select the duration to wait for a resource.

When a [Recovery Manager \(RMAN\)](#) job has been started and requires certain resources, the resources might not be available immediately. The `rmanresourcewaittime` policy controls the amount of time that the job waits in the Oracle Secure Backup [scheduler](#) queue for the required resources to become available. If the resources are unavailable after the wait time, then the job fails with an error message. If the resources become available within the specified time, then the job completes successfully.

Values

duration

Specifies the time to wait for a resource. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. Note that all values are valid except `disabled`. The default is `forever`.

7.13.20 rmanrestrestartdelay

Use the `rmanrestrestartdelay` policy to select the amount of time to wait before starting a restore operation after a restore request has been received. You can use this delay to queue all requests and optimize the retrieval of data from tape.

Values

delay_time

Specifies the time to delay. Valid values are a number followed by `seconds`, `minutes`, or `hours`. The default is `10seconds`.

7.13.21 tcpbufsize

Use the `tcpbufsize` policy to specify the size of [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#) buffers used in performing backups over the network, for hosts for which no buffer size has been specified directly using `mkhost` or `chhost`. The default value for `tcpbufsize` is the system default.

This policy is used in tuning backup performance.

7.13.22 useloadbalance

Use the `useloadbalance` policy to determine whether Oracle Secure Backup should use network load balancing while transferring data between clients and media servers.

Network load balancing distributes the load of multiple backup and restore jobs across all the network connections available between the client and media server.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for more information about network load balancing

Values**yes**

Uses network load balancing while transferring data.

no

Does not use network load balancing while transferring data (default).

7.13.23 windowsskipcdfs

Use the `windowsskipcdfs` policy to determine whether Oracle Secure Backup should back up Windows CD-ROM file systems (CDFS).

Values**yes**

Does not back up CDFS file systems (default).

no

Backs up the contents of CDFS file systems.

7.13.24 windowsskiplockedfiles

Use the `windowsskiplockedfiles` policy to determine whether Oracle Secure Backup logs an error message when it encounters a locked Windows file. Files are locked when in use by another process.

Values**yes**

Skips locked files and does not write a message to the transcript or archive's index file.

no

Logs an error message to the transcript and to the archive's index file (default).

7.14 Scheduler Policies

These policies control the behavior of the [scheduler](#). For example, you can specify a frequency at which the scheduler attempts to dispatch backup jobs.

The scheduler policies are as follows:

- [applybackupsfrequency](#) (page 7-40)
- [cachealljobs](#) (page 7-40)
- [defaultstarttime](#) (page 7-40)

- [maxdataretries](#) (page 7-41)
- [pollfrequency](#) (page 7-41)
- [recyclejobthreshold](#) (page 7-41)
- [retainbackupmetrics](#) (page 7-41)

7.14.1 applybackupsfrequency

Use the `applybackupsfrequency` policy to specify a frequency at which the Oracle Secure Backup `scheduler` attempts to dispatch jobs.

Values

duration

Specifies how often the scheduler dispatches jobs. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. Note that the `forever` and `disabled` values are not legal. The default value is `5minutes`, that is, Oracle Secure Backup attempts to dispatch jobs every five minutes.

7.14.2 cachealljobs

Use the `cachealljobs` policy to specify whether all details of the Oracle Secure Backup scheduler jobs should be stored. By default, Oracle Secure Backup caches information for all jobs in the `obscheduled` process. The job cache enables Oracle Secure Backup to list job information rapidly and efficiently. Each cached job consumes less than 10 KB of memory.

To disable job caching, after setting the policy value to `no`, you must also terminate and relaunch the `obscheduled` process for the new policy setting to reflect.

You can use the [jobretaintime](#) (page 7-23) policy to set the duration for which job related information will be retained.



See Also:

"[ctldaemon](#) (page 2-83)" for more information on suspending and resuming `obscheduled`

Values

yes

Stores the details of a scheduler job. This is the default option.

no

Does not store the details of a scheduler job.

7.14.3 defaultstarttime

Use the `defaultstarttime` policy to specify the default start time for each [trigger](#).

Values

time

Specifies the default trigger start time. Refer to "[time](#) (page 4-29)" for a description of the `time` placeholder. The default value is `00:00` (midnight).

7.14.4 maxdataretries

Use the `maxdataretries` policy to specify the maximum number of times to retry a failed [client](#) backup.

While attempting to back up a client, certain errors can occur that cause the backup to fail. (See the *Oracle Secure Backup Administrator's Guide* for a description of triggers.) Retryable failures include those caused by the client being unavailable because it is out of service or down, unable to communicate through the network, or has insufficient disk space for temporary backup files.

Values

n

Specifies the maximum number of times to retry. The default value is `6`.

7.14.5 pollfrequency

Use the `pollfrequency` policy to specify the frequency at which Oracle Secure Backup scans the contents of the [scheduler catalog](#) for manual changes.

Values

duration

Specifies the scheduler catalog polling frequency. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. Note that the `forever` value is not legal. The default value is `30minutes`.

7.14.6 recyclejobthreshold

Use the `recyclejobthreshold` policy to specify the number of scheduler jobs that must be completed before resetting the jobs back to the beginning. Once a scheduler job reaches the `recyclejobthreshold` value, the next scheduler job will start a fresh series of scheduler jobs.

Values

n

Specifies the job sequence number as the threshold for scheduler jobs. The minimum value can be set to `1000`, whereas the maximum value can be set to `500000`. The default `recyclejobthreshold` is `90000`.

7.14.7 retainbackupmetrics

Use the `retainbackupmetrics` policy to specify whether Oracle Secure Backup saves a summary of metrics produced by each [backup operation](#) in the [client](#) host's observed log.

Values**yes**

Saves a metric summary.

no

Does not save a metric summary (default).

7.15 Security Policies

These policies control aspects of domain security. For example, you can enable [Secure Sockets Layer \(SSL\)](#) encryption for backup data in transit or set the key size for each host [identity certificate](#).

The security policies are as follows:

- [autocertissue](#) (page 7-42)
- [certkeysize](#) (page 7-43)
- [certlifetime](#) (page 7-43)
- [certwarning](#) (page 7-43)
- [encryptdataintransit](#) (page 7-44)
- [loginduration](#) (page 7-44)
- [minuserpasswordlen](#) (page 7-44)
- [passwordgracetime](#) (page 7-44)
- [passwordlifetime](#) (page 7-45)
- [passwordreusetime](#) (page 7-45)
- [securecomms](#) (page 7-45)
- [trustedhosts](#) (page 7-45)
- [untrustedhostjobs](#) (page 7-46)
- [webinactivitytimeout](#) (page 7-46)
- [websessiontimeout](#) (page 7-46)

7.15.1 autocertissue

Use the `autocertissue` policy to indicate whether observed on the [administrative server](#) transmits signed certificates ([certificate](#) response messages) over the network as part of the [mkhost](#) (page 3-26) command processing.

Values**yes**

Transmits signed certificates over the network during host creation (default).

no

Does not transmit signed certificates over the network during host creation.

7.15.2 certkeysize

Use the `certkeysize` policy to indicate the key size to be used when creating the [public key/private key](#) pair used in every [identity certificate](#) in the [administrative domain](#). Certification Authorities typically choose key sizes of 1024 or 2048.

Values

size

Specifies the size of the key in bytes. Valid values are 512, 768, 1024 (default), 2048, 3072, or 4096. Key sizes of 512 or 768 are not regarded as secure; 1024 or 2048 are regarded as secure; and 3072 or 4096 are regarded as very secure.

7.15.3 certlifetime

Use the `certlifetime` policy to define the lifetime for certificates created during domain re-certification.



See Also:

[obcm](#) (page A-5) for more information on the `recertifydomain` option

Values

duration

You can set the lifetime of a certificate between a minimum of 1 year and a maximum of 20 years. The default duration is 10 years.

7.15.4 certwarning

Use the `certwarning` policy to set the duration through which backup results display a warning about the upcoming expiry of the existing host certificate.

This policy also defines the advisory period, during which less obvious warnings appear in log files, transcripts, emails, and reminder messages. The advisory period is always three times the length of the warning period. For example, if you use the `certwarning` policy to set the warning period to 7 days, then the advisory period is automatically set to 21 days.

The certificate warning period must be less than the certificate lifetime set in the [certlifetime](#) (page 7-43) policy.

Values

duration

You can set the host certificate warning period to a minimum of 3 days and a maximum of 18 months. The default value is 14 days.

For more information on setting the duration, see the [duration](#) (page 4-14) placeholder.

disabled

You can choose to disable the `certwarning` policy. By doing so, you disable all advisory and warning notifications relating to the expiry of your host certificate.

7.15.5 `encryptdataintransit`

Use the `encryptdataintransit` policy to enable [Secure Sockets Layer \(SSL\)](#) encryption for file-system and unencrypted [Recovery Manager \(RMAN\)](#) backup data before it passes over the network. This policy does not enable or disable encryption for data at rest, that is, data stored on disk or tape.

If RMAN backup data is encrypted by RMAN, then this policy does not encrypt it again.

Values**yes**

Enables encryption for bulk data transferred over the network.

no

Disables encryption for bulk data transferred over the network (default).

7.15.6 `loginduration`

Use the `loginduration` policy to specify the amount of time a login token remains valid in `obtool` after it is created.

Oracle Secure Backup creates a login token each time you log in through the `obtool`. If a valid token exists when you invoke either tool, then you do not have to log in again.

Values**duration**

Specifies the duration of the login token. Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default value is `15minutes`.

7.15.7 `minuserpasswordlen`

Use the `minuserpasswordlen` security policy to specify the minimum required Oracle Secure Backup user password length. Valid values are the integers from 8 (the default value) to 16.

This security policy only affects passwords for users created with the `mkuser` or `chuser` commands. Other passwords in the Oracle Secure Backup domain, such as NDMP host passwords, are not affected because they are not under the control of Oracle Secure Backup.

You can change the `minuserpasswordlen` security policy value when you install Oracle Secure Backup on UNIX and Linux by modifying the `minimum user password length` parameter in the `obparameters` file.

7.15.8 `passwordgracetime`

Use the `passwordgracetime` policy to specify the grace time for an Oracle Secure Backup user password. The grace time of a password is the time, in number of days,

during which the user can continue using the current password even after it has expired.

This value must be greater than or equal to 1 day. The default grace time of a password is set to 3 days. If the grace time is set to 'disabled, no grace time is provided and the user must change the password during the next login after the password expiration.

7.15.9 passwordlifetime

Use the `passwordlifetime` policy to specify the lifetime, in number of days, of an Oracle Secure Backup user password. This value must be greater than or equal to 1 day. The default lifetime of a password is set to 180 days. If the password lifetime is set to 'disabled', then the password never expires.

7.15.10 passwordreusetime

Use the `passwordreusetime` policy to specify the time, in number of days, after which an Oracle Secure Backup user password can be reused. This value must be greater than or equal to 1 day. The default reuse time of a password is set to 1 year. If the password reuse time is set to 'disabled', the password can never be reused.

7.15.11 securecomms

Use the `securecomms` policy to specify whether daemon components use [Secure Sockets Layer \(SSL\)](#) for authentication and message integrity.

Values

yes

Enables SSL encryption for authentication and message integrity (default).

no

Disables SSL encryption for authentication and message integrity.

7.15.12 trustedhosts

Use the `trustedhosts` policy to control whether Oracle Secure Backup restricts certain operations to trusted hosts only. These operations include:

- Use of `obtar` commands
- Direct access to physical devices and libraries
- Access to encryption keys

Values

yes

Specifies that restricted operations can be run only from an administrative or media server. If a restricted operation is attempted from a host that has only the [client](#) role, then the attempt fails with an `illegal request from non-trusted host` error.

no

The restricted operations can be run from any host in the [administrative domain](#).

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for more information on trusted hosts

7.15.13 untrustedhostjobs

Use the `untrustedhostjobs` policy to control whether Oracle Secure Backup accepts jobs from an untrusted client host (hosts that are not the administrative server or media server).

Values

yes

Specifies that jobs from untrusted client hosts must be accepted. This is the default setting.

no

Specifies that jobs from untrusted hosts must not be accepted. Specifies that no user, including the administrative user, can submit backup, duplication, copy instance, or vaulting jobs from the client host. Restore jobs from this client can be submitted by a user who has the appropriate privileges. If the `trustedhost` policy is disabled, then jobs are accepted from the host regardless of the setting of the `untrustedhostjobs` policy.

7.15.14 webinactivitytimeout

Use the `webinactivitytimeout` policy to specify the length of time an Oracle Secure Backup Web tool session can be inactive before you must re-authenticate it. The default value is 15 minutes.

7.15.15 websessiontimeout

Use the `websessiontimeout` policy to specify the length of time an Oracle Secure Backup Web tool session persists before timing out.

You can set this policy value between 60 seconds and 24 hours. The default value is 24 hours.

7.16 Staging Policies

These policies control stage scan properties.

The staging policies are as follows:

- [defaultscanjobpriority](#) (page 7-46)
- [obstagescandebuglevel](#) (page 7-47)

7.16.1 defaultscanjobpriority

Use the `defaultscanjobpriority` policy to specify the default priority of a stagescan job.

Values

n

A value from 1 to 2147483647, where a lower value is a higher priority. The default value is 150.

7.16.2 obstagescandebuglevel

Use the `obstagescandebuglevel` policy to set the debug level for the job transcript created by a stagescan job.

Values

fatal

Shows only catastrophic failures.

error

Logs fatal messages and errors.

info

Logs error messages and additional information. This is the default value.

debug1

Displays informational messages, the backup image name, and the names of instances that are skipped because the instance flags indicate that the instance should not be copied (the flags are set to stage-in-progress, stage-complete, or deleted).

debug2

Displays `debug1` messages and also full stage rule information for each disk pool that is scanned. Additionally, during scanning this level displays instance-stage rule matching information.

7.17 Vaulting Policies

These policies control how Oracle Secure Backup performs vaulting.

The vaulting policies are as follows:

- [autorunmmjobs](#) (page 7-47)
- [autovolumerelease](#) (page 7-48)
- [invretrydelay](#) (page 7-48)
- [maxinvretrytime](#) (page 7-48)
- [minwritablevolumes](#) (page 7-49)
- [offsitecustomerid](#) (page 7-49)
- [reportretaintime](#) (page 7-49)

7.17.1 autorunmmjobs

Use the `autorunmmjobs` policy to control whether manual intervention is needed to start a media movement job after it has been scheduled.

Values

no

If this policy is set to `no`, then media movement jobs are not started automatically by the scheduler. The Oracle Secure Backup operator must run the job through the `obtool runjob` command. This is the default value.

yes

If this policy is set to `yes`, then media movement jobs are started automatically by the scheduler.



Note:

Even if `autorunmmjobs` is set to `yes`, manual intervention might still be required to *complete* a media movement job for a variety of reasons.

7.17.2 autovolumerelease

Use the `autovolumerelease` policy to automatically release recalled volumes when restore jobs requiring those volumes have completed. Only volumes automatically recalled by Oracle Secure Backup are released.

Values

yes

Enables the policy. When all restore jobs dependent upon a `volume` are completed, the volume is released to be returned to its previous `location`.

no

Disables the policy (default).

7.17.3 invretrydelay

Use the `invretrydelay` policy to specify how long Oracle Secure Backup waits before retrying an export operation or inventory operation to verify if a volume has been physically removed from a library.

duration

Refer to "`duration` (page 4-14)" for a description of the `duration` placeholder. The default value is `2minutes`.

7.17.4 maxinvretrytime

Use the `maxinvretrytime` policy to specify how long Oracle Secure Backup continues retrying an export or inventory operation. When this duration is completed, the job is put in an *input required* state, an alert e-mail is sent to the e-mail recipients in the location object, and the following prompt is displayed in the transcript:

```
go      - proceed with the volume movement
quit    - give up and abort this media movement job
```

duration

Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default value is `15minutes`.

7.17.5 minwritablevolumes

Use the `minwritablevolumes` policy to specify the minimum number of writable volumes that must be available in each [tape library](#) always. If the number of writable volumes in a tape library drops to less than this value, then Oracle Secure Backup initiates early rotation of volumes in that tape library.

You can override this policy for an individual [location](#).

Values***n***

Specifies the minimum number of writeable volumes for each tape library.

7.17.6 offsitecustomerid

Use the `offsitecustomerid` policy to define the default customer ID string used in reports generated by Oracle Secure Backup. You can override this policy for an individual [location](#).

7.17.7 reportretaintime

Use the `reportretaintime` policy to define how long vaulting reports (pick/distribution) are retained.

Values**duration**

Refer to "[duration](#) (page 4-14)" for a description of the `duration` placeholder. The default value is `7days`.

8

Classes and Rights

Table 8-1 (page 8-1) defines the predefined `obtool` classes. The **rights** are described in "Class Rights (page 8-2)".

Table 8-1 Classes and Rights

Class Rights	admin	operator	oracle	user	reader	monitor
access file system backups (page 8-2)	all	all	owner	owner	none	all
access Oracle database backups (page 8-3)	all	all	owner	owner	none	all
browse backup catalogs with this access (page 8-3)	privileged	notdenied	permitted	permitted	named	none
display administrative domain's configuration (page 8-4)	yes	yes	yes	yes	no	yes
list any backups owned by user (page 8-4)	yes	yes	yes	yes	no	yes
list any backup, regardless of its owner (page 8-4)	yes	yes	no	no	no	yes
list any jobs owned by user (page 8-5)	yes	yes	yes	yes	no	yes
list any job, regardless of its owner (page 8-5)	yes	yes	no	no	no	yes
manage devices and change device state (page 8-5)	yes	yes	yes	no	no	no
modify administrative domain's configuration (page 8-4)	yes	no	no	no	no	no
modify any backup, regardless of its owner (page 8-5)	yes	yes	no	no	no	no
modify any backups owned by user (page 8-5)	yes	yes	yes	yes	no	no
modify any job, regardless of its owner (page 8-5)	yes	yes	no	no	no	no
modify any jobs owned by user (page 8-5)	yes	yes	yes	yes	no	no
modify catalog (page 8-6)	yes	no	no	no	no	no
modify own name and password (page 8-6)	yes	yes	yes	yes	yes	no
perform file system backups as privileged user (page 8-6)	yes	yes	no	no	no	no
perform file system backups as self (page 8-6)	yes	yes	yes	no	no	no

Table 8-1 (Cont.) Classes and Rights

Class Rights	admin	operator	oracle	user	reader	monitor
perform file system restores as privileged user (page 8-6)	yes	yes	no	no	no	no
perform file system restores as self (page 8-7)	yes	yes	yes	yes	no	no
perform Oracle database backups and restores (page 8-6)	yes	no	yes	no	no	no
query and display information about devices (page 8-7)	yes	yes	yes	yes	no	yes
receive email describing internal errors (page 8-7)	yes	yes	yes	no	no	no
receive email regarding expired passphrase keys (page 8-7)	yes	no	no	no	no	no
receive email requesting operator assistance (page 8-7)	yes	yes	yes	no	no	no

**See Also:**

["Class Commands](#) (page 1-13)"

8.1 Class Rights

This section describes the [rights](#) in Oracle Secure Backup classes.

8.1.1 access file system backups

This right specifies the type of access to file-system backups. The values are as follows:

- `owner` indicates that the Oracle Secure Backup user can access only file-system backups created by the user.
- `class` indicates that the Oracle Secure Backup user can access file-system backups created by any Oracle Secure Backup user in the same [class](#).
- `all` indicates that the Oracle Secure Backup user can access all file-system backups.
- `none` indicates that the Oracle Secure Backup user has no access to file-system backups.

You can set this right with the `--fsrights` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.2 access Oracle database backups

This right specifies the type of access to Oracle database backups made through the [SBT interface](#). The values are as follows:

- `owner` indicates that the Oracle Secure Backup user can access only SBT backups created by the user.
- `class` indicates that the Oracle Secure Backup user can access SBT backups created by any Oracle Secure Backup user in the same [class](#).
- `all` indicates that the Oracle Secure Backup user can access all SBT backups.
- `none` indicates that the Oracle Secure Backup user has no access to SBT backups.

You can set this right with the `--orarights` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.3 browse backup catalogs with this access

This right applies to browsing access to the Oracle Secure Backup [catalog](#). The [rights](#) are listed in order of decreasing privilege. Your choices are:

- `privileged` means that Oracle Secure Backup users can browse all directories and catalogs.
- `notdenied` means that Oracle Secure Backup users can browse any catalog entries for which they are not explicitly denied access. This option differs from `permitted` in that it allows access to directories having no stat record stored in the catalog.
- `permitted` means that Oracle Secure Backup users are bound by normal UNIX rights checking. Specifically, Oracle Secure Backup users can only browse directories if at least one of these conditions is applicable:
 - The UNIX user defined in the Oracle Secure Backup identity is listed as the owner of the directory, and the owner has read rights.
 - The UNIX group defined in the Oracle Secure entity is listed as the group of the directory, and the group has read rights.
 - Neither of the preceding conditions is met, but the UNIX user defined in the Oracle Secure Backup identity has read rights for the directory.
- `named` means that Oracle Secure Backup users are bound by normal UNIX rights checking, except that others do not have read rights. Specifically, Oracle Secure Backup users can only browse directories if at least one of these conditions is applicable:
 - The UNIX user defined in the Oracle Secure Backup identity is listed as the owner of the directory, and the owner has read rights.
 - The UNIX group defined in the Oracle Secure Backup identity is listed as the group of the directory, and the group has read rights.
- `none` means that Oracle Secure Backup users have no rights to browse any directory or catalog.

You can set this right with the `--browse` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.4 display administrative domain's configuration

This right allows [class](#) members to list objects, for example, hosts, devices, and users, in the [administrative domain](#).

You can set this right with the `--listconfig` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.5 modify administrative domain's configuration

This right allows [class](#) members to edit, that is, create, modify, rename, and remove, all configuration data in an Oracle Secure Backup [administrative domain](#). The data includes the following:

- Classes
- Users
- Hosts
- Devices
- Defaults and policies
- Schedules
- Datasets
- Media families
- Summaries
- Backup windows
- Rotation policies
- Duplication policies
- Duplication windows

You can set this right with the `--modconfig` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.6 list any backup, regardless of its owner

This right enables class members to view information about backup images, backup image instances, and backup sections that they create.

You can set this right with the `--listanybackups` option of the [mkclass](#) or [chclass](#) commands.

8.1.7 list any backups owned by user

This right enables class members to view information about backup images and backup image instances that they create.

You can set this right with the `--listownbackups` option of the [mkclass](#) or [chclass](#) commands.

8.1.8 list any job, regardless of its owner

This right enables [class](#) member to view the status of any scheduled, ongoing, and completed jobs and transcripts for any job.

You can set this right with the `--listanyjob` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.9 list any jobs owned by user

This right enables [class](#) members to view the status of scheduled, ongoing, and completed jobs that they create and transcripts for jobs that they create.

You can set this right with the `--listanyjob` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.10 manage devices and change device state

This right enables [class](#) members to control the state of devices.

You can set this right with the `--managedevs` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.11 modify any backup, regardless of its owner

This right enables admin and operator class members to modify all backups.

You can set this right with the `--modanybackups` option of the [mkclass](#) or [chclass](#) commands.

8.1.12 modify any backups owned by user

This right enables admin and operator class members to modify backups that they create.

You can set this right with the `--modownbackups` option of the [mkclass](#) or [chclass](#) commands.

8.1.13 modify any job, regardless of its owner

This right enables [class](#) members to make changes to all jobs.

You can set this right with the `--modanyjob` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.14 modify any jobs owned by user

This right enables [class](#) members to modify only jobs that they configured.

You can set this right with the `--modownjob` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.15 modify catalog

This right enables [class](#) members to modify the Oracle Secure Backup volumes catalog.

8.1.16 modify own name and password

This right enables [class](#) members to modify the password and given name attributes for their own user objects.

You can set this right with the `--modself` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.17 perform file system backups as privileged user

This right enables [class](#) members to back up files and directories while acting as a privileged user. A privileged user is `root` on UNIX or a member of the Administrators group on Windows.

You can set this right with the `--backuppriv` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.18 perform file system backups as self

This right allows the [class](#) member to back up only those files and directories to which the member has access by using either UNIX user and group names or a Windows domain account.

You can set this right with the `--backupself` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.19 perform Oracle database backups and restores

This right enables [class](#) members to back up and restore Oracle databases. Users with this right are Oracle Secure Backup users that are mapped to operating system accounts of Oracle database installations.

You can set this right with the `--orauser` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.20 perform file system restores as privileged user

This right enables [class](#) members to restore the contents of backup images and backup image instances as a privileged user. A privileged user is `root` on UNIX and a member of the Administrators group on Windows.

You can set this right with the `--restpriv` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.21 perform file system restores as self

This right enables [class](#) members to restore the contents of backup images and backup image instances under the restrictions of the access rights imposed by the user's UNIX name/group or Windows domain/account.

You can set this right with the `--restself` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.22 query and display information about devices

This right enables [class](#) members to query the state of all storage devices configured within the [administrative domain](#).

You can set this right with the `--querydevs` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.23 receive email describing internal errors

This right enables [class](#) members to receive email messages describing errors that occurred in any Oracle Secure Backup activity.

You can set this right with the `--mailerrors` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.24 receive email regarding expired passphrase keys

This right enables [class](#) members to receive email messages describing expired passphrase keys.

You can set this right with the `--mailrekey` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

8.1.25 receive email requesting operator assistance

This right enables [class](#) members to receive email when Oracle Secure Backup needs manual intervention. Occasionally, during backups and restores, [operator](#) assistance might be required, as when a different volume is required to continue a backup. In such cases, Oracle Secure Backup sends e-mail to all users who belong to classes with this attribute.

You can set this right with the `--mailinput` option of the [mkclass](#) (page 3-2) or [chclass](#) (page 2-28) commands.

A

Miscellaneous Programs

This appendix describes the following miscellaneous Oracle Secure Backup programs:

- [makedev](#) (page A-1)
- [obcleanup](#) (page A-3)
- [obcm](#) (page A-5)
- [uninstallob](#) (page A-9)

A.1.1 makedev

Purpose

Use the `makedev` tool to configure a [tape device](#) for use with Oracle Secure Backup. This tool provides an alternative to creating a [device special file](#) with `installlob`.

Prerequisites

You must run this utility as `root` on a Linux or UNIX system.

Usage Notes

Note the following aspects of `makedev` usage:

- The `makedev` tool creates device special files for a UNIX [media server](#). For each [tape drive](#) that you define, `makedev` creates one special file. For each [tape library](#) you define, `makedev` creates a single device file.
- The `makedev` tool prompts you for any required information that you do not supply on the command line. You can respond to any prompt with a question mark (?) to display more information.

Syntax

```
install/makedev [ -u unit ] [ -d ] [ -b bus ] [ -t target ] [ -l lun ] [ -f ]  
[ -n ] [ -x ] [ -y ] [ -z ] [ -h | ? | -? ] [ -dr | -mh ]
```

Semantics

-u *unit*

Creates the device special file for the tape device specified by [Oracle Secure Backup logical unit number](#), which can range in value from 0 through 31.

The Oracle Secure Backup logical unit number of a tape device is a number assigned by you and used by `makedev` to create unique filenames for the tape devices connected to the media server. Although it is not a requirement, unit numbers usually start at 0.

-d

Uses the default value for each unspecified option instead of prompting for it. Note that you must always specify a unit number (-u) even if you use this option.

-b bus

Specifies the [SCSI](#) bus number, address, or instance (depending on operating system type), to which the tape device is attached.

[Table A-1](#) (page A-2) lists the default SCSI bus designation for each supported operating system type.

Operating System	Default SCSI Bus Type
Solaris	esp0 (driver name/instance)

-t target

Specifies the SCSI target ID of the tape device, which can range from 0 through 15. The default depends on the logical unit number that you specified with the -u option.

-l lun

Specifies the [SCSI LUN](#) of the tape device. Most operating systems support only LUN 0 and 1. The default LUN is 0.

Be careful not to confuse the SCSI LUN with the Oracle Secure Backup logical unit number. The LUN is part of the hardware address of the tape device; the Oracle Secure Backup logical unit number is part of the device special file name.

-f

Replaces any existing files or drivers without prompting for confirmation. By default, makedev prompts you to confirm replacement of any existing device special files.

-n

Displays the commands that is processed by makedev to generate device special files, but does not actually create the files.

-x

Displays all commands as they are processed by makedev.

-y

Traces entry and exit from each subscript as it is processed by makedev.

-z (AIX only)

Generates a trace file, `makedev.trc`, in the current directory. This file contains the output of the methods used to define and configure the tape device.

[-h | -?]

Displays a summary of makedev usage. You might be required to type `- \?` instead of `-?` to avoid shell [wildcard](#) expansion.

-dr

Creates special files for a tape drive. This the default.

-mh

Creates special files for a SCSI tape library.

Example

Example A-1 Creating a Device Special File for a Tape Drive

This example uses `makedev` to create a device special file. The example creates a special file for a tape drive, unit 0, at the default SCSI bus and target.

```
# install/makedev -u 0 -d
```

A.1.2 obcleanup

Purpose

Use the `obcleanup` tool to generate an editable file listing the volumes in the Oracle Secure Backup catalog and to remove unneeded records.

If previously used volumes are unlabeled or overwritten, then the index daemon automatically removes expired backups from the catalog at the interval set by the [indexcleanupfrequency](#) (page 7-20) index policy (the default is 21 days). In this case, no manual intervention is necessary.

If volumes expire but are not unlabeled or overwritten, then their catalog entries persist unless you remove them with `obcleanup`. You can also use `obcleanup` to remove references to volumes that are no longer needed but are not set to expire. Because the catalogs can consume considerable disk space, you might want to run `obcleanup` periodically to keep the admin subdirectory of the Oracle Secure Backup home to a manageable size.

Prerequisites

The `obcleanup` utility operates only on the administrative server.

Usage Notes

When you run the `obcleanup` program on the command line, it lists the contents of the catalogs in a file, which is opened in an editor. The default text editor is set by the `EDITOR` environment variable. On Linux and UNIX, the default is `/bin/vi` if the `EDITOR` environment variable is not set. On Windows the default is Notepad.

Each line in the file contains a reference to a [volume](#) that you could purge from the catalogs. For example:

#Item	Identification	Created	Where	Notes
1	VOL000001	2004/06/07.15:51	IS	IX volume is full

Volumes that have expiration policies associated with them are noted in this file. If you have discarded or overwritten tapes, then use a text editor to delete the lines corresponding to these tapes from the file, save the modified file, and exit the editor.

After you delete records from the generated file and save it, `obixd` runs in the background and automatically removes the deleted records from the catalogs. You can configure the `obixd` cycle time in the index policy. The default cycle time is 21 days.

Syntax

```
etc/obcleanup [ -a ] [ -d ] [ -s { d | v | t } ] [ -v ]...
etc/obcleanup [ -V ]
```

Semantics

-a

Shows individual archive records in addition to volume records.

-d

Shows previously deleted records.

-s

Sorts the list by date (d), volume ID (v), or volume tag (t).

-v

Operates in verbose mode. The more -v options you specify, the more verbose the output.

-V

Displays the obcleanup version and exits.

Example

Example A-2 Sample Output from obcleanup

This example shows the editable file generated by the obcleanup utility for host brhost2.

```
% etc/obcleanup

# This file lists all volumes described in Oracle Secure Backup's
# "volumes" and "index" databases on brhost2.
#
# Edit this file to delete entries from Oracle Secure Backup's databases.
# Delete each line whose corresponding database entry you want
# to remove. Do not change the contents of the undeleted lines!
#
# Once you've finished, save your changes and exit the editor.
# obcleanup will ask you to confirm these changes before applying
# them to the databases.
#
#Item Identification                Created      Where Notes
#-----
 1 tag 00000105                      IS
 2 tag 00000110                      IS
 3 tag 00000111                      IS
 4 tag 00000121                      IS
 5 tag 00000155                      IS
 6 tag 00000156                      IS
 7 tag 00000157                      IS
 8 tag 00000158                      IS
 9 tag AEA649S                       IS
10 tag AEA650S                       IS
11 tag AEA655S                       IS
12 tag AFX935                        IS
13 tag AFX936                        IS
14 tag AFX936                        IS
15 full-000001                      2008/01/17.18:12 IX
16 full-000002                      2008/01/17.18:12 IX
```

17	full-000003	2008/01/17.18:12	IX
18	full-000004	2008/06/05.01:02	IX
19	full-000005	2008/07/04.01:02	IX
20	full-000006	2008/08/06.01:04	IX
21	full-000007	2008/09/06.01:00	IX
22	full-000008	2008/09/06.01:00	IX
23	full-000009	2008/11/04.15:05	IX
24	full-000010	2008/11/04.15:05	IX

A.1.3 obcm

Purpose

Use the `obcm` tool to renew, export, or import an [identity certificate](#), to manage the encryption key wallet, to update domain certificates, and to create a wallet used for cloud storage devices. Importing or exporting an identity certificate is required if you do not accept the default Oracle Secure Backup security behavior, which is for the [Certification Authority \(CA\)](#) to issue a signed [certificate](#) to each host over the network.

When using a cloud storage device, use the `obcm` tool to create and manage the cloud wallet.

The `observed` daemon on the [administrative server](#) acts as the CA. The CA has two responsibilities for certificates: it accepts certificate signing requests from hosts within the system as part of the `mkhost` process and sends signed certificates back to the requesting host.

In [manual certificate provisioning mode](#), you run `obcm export --certificate` on the administrative server to export a signed certificate for the newly configured host. You must manually transfer this signed certificate to the newly configured host.

After manually transferring the certificate to the host, run `obcm import` on the newly configured host to import the signed certificate into the host's [wallet](#). In this case, `obcm` directly accesses the wallet of the host. After it has made changes to the local wallet, `obcm` notifies the local `observed` so that the local `observed` can re-create the [obfuscated wallet](#).

Prerequisites

All `obcm` commands should be run as `root` in Linux or UNIX or as an administrative user in Windows.

You must have write permissions in the wallet directory, which by default is `/usr/etc/ob/wallet` on Linux and UNIX and `C:\Program Files\Oracle\Backup\db\wallet` on Windows.

Syntax

```
obcm chpass --keywallet/-k name
  [ --newpass/-n new_password ] [ --oldpass/-o old_password ]
obcm decertify [ --nq | --resign ]
obcm display [--cloudwallet/-c | --idwallet/-i | --keywallet/-k | --crl/-l]
  [--password/-p password] [--verbose/-v]
obcm export { --certificate/-c | --request/-r } --file/-f cert_file
  --host/-h hostname
obcm import --file/-f signed_certificate_file
obcm mkow --keywallet/-k key_wallet [ --password/-p psword ]
obcm recertifydomain [ --nocomm/-h ] [ --expires/-e months ] [ --noquery/--nq ]
```

```
obcm ca [ enable | disable ] certification authority
obcm verifycomm
obcm wallet [--create/-c] [--cloudwallet/-L | --wpath/-w wallet_path] [--add/-a
certificate_path]
```

Semantics

chpass --keywallet/-k name [--newpass/-n new_password [--oldpass/-o old_password]

Changes the password for the Oracle Secure Backup encryption key wallet. The `--keywallet` argument is required. If `--newpass` or `--oldpass` is not specified, then you are prompted for the corresponding password.

decertify [--nq | --resign]

Deletes local host certification data. If you specify `--nq`, then the command does not display a confirmation message. If you do not specify this option, then the command displays a confirmation message. "[Command Execution in Interactive Mode \(page 1-3\)](#)" describes the message.

Specify the `--resign` option to remove the client host from the Oracle Secure Backup administrative domain. This option is necessary when moving a host from one backup domain to another.

For proper decertification of a host, Oracle recommends that you first close all `obtool` sessions and Oracle Secure Backup processes running on that host.

If you run `obcm decertify` as a user other than `root` in Linux or UNIX or an administrative user in Windows, then Oracle Secure Backup does not display an error but the host is not decertified. An attempt to decertify the [administrative server](#) fails with an error. The `obcm decertify` command can be run more than once on other hosts, but only the first operation actually decertifies the host.

You can use the `rmhost --nocomm/-N hostname` command to remove a decertified host from the Oracle Secure Backup domain.

To recertify a decertified host, Oracle recommends that you use the `updatehost` command with the `recertify` option, rather than using the `rmhost` and `mkhost` commands in `obtool`. Because the `rmhost` and the `mkhost` commands remove the host and then add it back in to the domain, they attribute some Oracle Secure Backup objects as `deleted`. The `rmhost` command also deletes the catalog restore data for that host.

display {[cloudwallet/-c | -idwallet/-I] | [keywallet/-k | --crl/-l]} [password/-p password] [verbose/-v]

Displays the contents of the identity, encryption key, or cloud wallet. The `--crl` option displays the certificate revocation list. If no wallet type is specified, then data from the identity wallet is displayed. You can use the `--password` option to display the contents of the password-protected encryption key wallet. This can be useful during a recovery from a lost [catalog](#), when the obfuscated version of the encryption key wallet has been lost.

export [--certificate/-c | --request/-r] [--file/-f cert_file] [--host/-h hostname]

The `--certificate` option exports a signed certificate chain for the specified host to the specified text file. The `--request` option exports a certificate request for the specified host to the specified text file. Both the `--file` and `--hostname` arguments are required.

import [--file/-f signed_certificate_chain]

Imports a `signed_certificate_chain` from the specified text file. The `--file` argument is required.

mkow [--keywallet/-k key_wallet] [--password/-p password]

Re-creates the obfuscated encryption key wallet with the existing password, in instances like Oracle Secure Backup disaster recovery. If `--password` is not specified, then you are prompted for the password.

recertifydomain [--nocomm/-h] [--expires/-e months] [--noquery/--nq]

Triggers the renewal of the signing certificate of your domain. This command must be run on the administrative host.

Use the `--nocomm` option to request the renewal of certification authority, with no interaction with other Oracle Secure Backup components. Note that in the case where the Oracle Secure Backup service daemon cannot start, using the `--nocomm` parameter is mandatory.

Use the `--expires` option to set the lifetime duration, in months, for the renewed certificates in your domain. This value overrides the lifetime set using the [certlifetime](#) (page 7-43) policy.

Using the `--expires` parameter is mandatory in the following scenarios:

- The certificates have already expired.
- `obcm` version 12.2.0.1 is executing within an Oracle Secure Backup 12.2.0.1 or prior domain.

Before using the `obcm recertifydomain` command, you must meet the following requirements:

- Ensure that `observed` is running on your domain
- Temporarily suspend the backup scheduler
- Ensure that the current host is the administrative server
- Ensure that there are no active or pending jobs

ca [enable | disable] *certification authority*

Manages host certification on support versions of Oracle Secure Backup. This command temporarily enables or disables recertification of signing certificates. To permanently disable renewal of certificates, see how to renew certificates in manual certificate provisioning mode in the *Oracle Secure Backup Installation and Configuration Guide*.

verifycomm

Verifies the validity of host certificates by determining whether `obcm` can successfully communicate with `observed`. Run this command to diagnose connection errors in your domain.

wallet [--create/-c] [--cloudwallet/-L | --wpath/-w wallet_path] [--add/-a certificate_path]

Creates a user wallet and imports certificates into the wallet. The following are the `wallet` options:

- `--cloudwallet`
indicates that the certificate management function will be applied to the cloud wallet
- `--wpath` specifies a path for the wallet to be created
- `--add` adds a trust point to the wallet
using the specified certificate

Examples

Example A-3 Exporting a Signed Certificate Chain

This example exports a signed certificate chain for host `new_client` to the file `new_client_cert.f`. The utility runs on the administrative server.

```
obcm export -c -f /tmp/new_client_cert.f -h new_client
```

Example A-4 Importing a Signed Certificate Chain

This example imports a signed certificate chain from the file `client_cert.f`. The utility is run on the host being added to the administrative domain.

```
obcm import -f /tmp/new_client_cert.f
```

Example A-5 Creating a Cloud Wallet Containing Trust Points Using Certificate Files

This example creates a cloud wallet containing trust points using certificate files.

1. Create a cloud wallet, entering a password when prompted:

```
#obcm wallet --create --cloudwallet
Wallet Password:
```

2. Add the downloaded certificate to the cloud wallet just created. Use the same password you used when you created the cloud wallet:

```
#obcm wallet --cloudwallet --add /tmp/cacertificate1.crt
Wallet password:
```

3. Add the intermediate CA certificate. Use the same password you used when you created the cloud wallet:

```
#obcm wallet --cloudwallet --add /tmp/cacertificate2.crt
Wallet Password:
```

4. You can use the `obcm` command `display --cloudwallet -v` to validate that the certificates were added correctly to the cloud wallet. The output should show two trust points in the wallet, as follows:

```
There are 0 certificate requests in the wallet
There are 0 certificates in the wallet
There are 2 trust points in the wallet
```

Trust point:

```
DN: CN=Symantec Class 3 Secure Server CA - G4,OU=Symantec Trust
Network,O=Symantec Corporation,C=US
Issuer: CN=VeriSign Class 3 Public Primary Certification Authority -
G5,OU=(c) 2006 VeriSign\, Inc. - For
authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
Type: NZDST_CLEAR_PTP
Public key size: 2048
Key usage: CA CERT SIGNING
Serial number: 0x513FB9743870B73440418D30930699FF
Version: NZTTVERSION_X509v3
Signature algorithm: NZDCATSHA256RSA
Valid from: 2013/10/31.00:00:00 (UTC)
Valid to: 2023/10/30.23:59:59 (UTC)
```

Trust point:

```
DN: CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c)
```

```
2006 VeriSign\, Inc. - For
    authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
    Issuer: CN=VeriSign Class 3 Public Primary Certification Authority -
G5,OU=(c) 2006 VeriSign\, Inc. - For
    authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
Type: NZDST_CLEAR_PTP
Public key size: 2048
Key usage: CA CERT SIGNING
Serial number: 0x18DAD19E267DE8BB4A2158CDCC6B3B4A
Version: NZTTVERSION_X509v3
Signature algorithm: NZDCATSHA1RSA
Valid from: 2006/11/08.00:00:00 (UTC)
Valid to: 2036/07/16.23:59:59 (UTC)
```

A.1.4 uninstallob

Purpose

Use the `uninstallob` tool to uninstall Oracle Secure Backup from your system. The `uninstallob` script gives the user the choice to save the administrative directory if uninstalling an administrative server or to save the system's identity if uninstalling a media server or client.

Prerequisites

You must run this utility as `root` on a Linux or UNIX system.

Syntax

```
install/uninstallob
```

Example

Example A-6 Uninstalling Oracle Secure Backup

This example uses `uninstallob` to uninstall Oracle Secure Backup from an administrative server.

```
# install/uninstallob
Do you want to save the admin directory (y or n) [y]? :y
Do you want to continue (y or n) [n]? : y
Oracle Secure Backup was successfully uninstalled
```

B

obtar

The primary user interfaces for [file-system backup](#) and restore operations are the Oracle Secure Backup [Web tool](#) and `obtool`. The underlying engine that Oracle Secure Backup uses to back up and restore data is `obtar`. You can use the `obtar` command-line interface directly, although this practice is recommended only for advanced users.

This appendix contains these sections:

- [obtar Overview](#) (page B-1)
- [Optimizing Your Use of obtar](#) (page B-2)
- [obtar -c](#) (page B-6)
- [obtar -x](#) (page B-8)
- [obtar -t](#) (page B-11)
- [obtar -zz](#) (page B-14)
- [obtar Options](#) (page B-14)

B.1 obtar Overview

`obtar` is a descendent of the original Berkeley UNIX `tar(1)` command. The `obtar` command-line interface conforms to the POSIX 1003.2 standards for UNIX command lines as follows:

- Options are single letters preceded with a dash, as in `-c`.
- If an option requires an argument, then it follows the option and can be separated from the option with a space, as in `-c argument`.
- Multiple options can be combined after a single dash if no multiple options require an argument. If only one option requires an argument, then this option must appear last in the group. For example, if `-c` takes an argument, then you might specify `-vPZc argument`.

[Table B-1](#) (page B-1) explains the basic `obtar` modes. The description of each mode includes the most common options. "[obtar Options](#) (page B-14)" describes additional options.

Table B-1 obtar Modes

Option	Description
obtar -c (page B-6)	Creates a one-time backup image of the directories and files specified on the command line.
obtar -x (page B-8)	Restores directories and files.
obtar -t (page B-11)	Lists the contents for a backup image.

Table B-1 (Cont.) `obtar` Modes

Option	Description
<code>obtar -zz</code> (page B-14)	Displays a list of the backup images contained on the volume.

If you back up directories and files so that the necessary Oracle Secure Backup [catalog](#) data is generated, such as when using the `-G`, or `-N` options, then you can use `obtool` or the Oracle Secure Backup [Web tool](#) to browse the catalog and restore the files. If you do not generate the catalog files, however, then you can still perform a raw restore operation.

B.2 Optimizing Your Use of `obtar`

This section describes ways you can optimize your use of `obtar`, and provides information about some more advanced backup features of `obtar`.

This section includes the following topics:

- [Using tar with Backup Images Created by `obtar`](#) (page B-2)
- [Backing Up and Restoring Raw File Systems](#) (page B-3)
- [Changing Criteria for Incremental Backups](#) (page B-4)
- [Backing Up Across Mount Points](#) (page B-5)

B.2.1 Using tar with Backup Images Created by `obtar`

By default, `obtar` generates backup images that are fully compatible with `tar`. This section offers tips for using `tar` with backup images created with `obtar`.

When you create a [backup image](#) with `obtar -g`, `obtar` creates several files in the backup image that provide information about the backup image. `obtar` knows that these files are special and never extracts them from the backup image as actual files. To `tar`, the files appear to be ordinary files; when you use `tar` to extract a backup image, `tar` creates several files that have the prefix `###`. When you restore a backup image with `obtar -x`, `obtar` does not create these files.

You can use any of the following `obtar` options and still maintain compatibility with `tar`:

`-b, -B, -c, -f, -h, -l, -m, -t, -v, -x`

When you are using `tar` to extract a backup image that spans multiple volumes, note that each section of a backup image that spans multiple volumes is a valid `tar` file. `obtar` can correctly extract the contents of the backup image, but `tar` encounters an early end-of-file condition after it extracts the first section of the backup image. At this point, you have extracted only the first part of the data for the file that continues across the [volume](#) break. To restore the file completely, you must do the following:

1. Move the first file fragment to a location that is not overwritten as you continue the extraction.
2. Load the next volume and continue the extraction. The second file fragment is extracted.

3. Use the UNIX `cat` command to append the second file fragment to the first file fragment to obtain the complete file. For example:

```
cat first_frag second_frag > complete_file
```

4. Delete the file fragments.

B.2.2 Backing Up and Restoring Raw File Systems

When `obtar` encounters a special file while backing up a tree, it usually writes only the special file name and attributes to the [backup image](#). If a special file is mentioned at the top level of the backup tree, however, either explicitly or with a [wildcard](#), then `obtar` backs up the file name, attributes, and contents. In this section, special files includes both block special files and character special files.

 **Note:**

Oracle Secure Backup does not support the backup or restore of the contents of character special files.

For example, the following command creates a backup image consisting of all the special file names in the `/dev` directory, but neither opens nor reads any special file:

```
obtar -cvf tape0 /dev
```

On the other hand, the following command causes `obtar` to open `/dev/sd0a`, `/dev/sd13a`, `/dev/sd13b`, and so on and write the entire contents of the underlying raw file systems to the backup image:

```
obtar -cvf tape0 /dev/sd0a /dev/sd13*
```

Because this form of access bypasses the native Linux or UNIX file system, you can use it to back up raw file systems that contain data other than Linux or UNIX data, for example, a disk partition containing a database.

Because `obtar` has no idea which blocks are used or unused on the raw file system, the entire file system is always saved. This is different from a backup using the vendor-supplied Linux or UNIX file system, which saves only blocks in use.

When restoring data to a raw file system, the size of the file system to which you are restoring must be at least the size of the file system that was backed up. When restoring a raw file system, all data currently on the file system is lost. It is totally overwritten by the data from the backup image.

To restore a raw file system, the raw file system must have been formatted using `mkfs`, `mkvol`, or a similar tool, and the special file referring to the raw file system must exist. Otherwise, the data is restored as a normal file.

 **Note:**

Never back up or restore a mounted file system. If a file system is mounted, then activity by other processes might change the file system during the backup or restore, causing it to be internally inconsistent.

B.2.2.1 Backing Up Raw Partitions

You can use `obtool` to back up raw partitions. The raw file system must not be mounted during the backup. You can back up the block device file by including the path of the device file in a dataset.

To back up raw partitions:

1. Create a dataset for the raw partition.

For example, you can create a dataset named `rawpart.ds` as follows:

```
include host brhost2
{
  include path /dev/sda3
}
```

2. Back up the partition.

The following `obtool` command makes a backup using the dataset created in the previous step:

```
ob> backup -D rawpart.ds --restriction lib1 --go
```

B.2.2.2 Restoring Raw Partitions

You can use `obtool` to restore raw partitions. The raw file system must not be mounted during the restore operation.

To restore raw partitions:

1. Use `obtool` to set the host to which you want to restore:

For example, run the `cd` command as follows to set the host to `brhost2`:

```
ob> cd --host brhost2
```

2. Restore the partition.

The following `obtool` command restores partition `/dev/sda3`:

```
ob> restore --select latest /dev/sda3 --go
```

B.2.3 Changing Criteria for Incremental Backups

When `obtar` decides if a file is to be included in an [incremental backup](#), it usually uses the `mtime` for the file, which is the time at which the contents of the file were last modified. If a file was added to a directory by using `mv` or `cp -p`, then it might not get backed up because its modified time is not changed from those of the original copy of the file. You can get around this problem by telling `obtar` to use `ctime`, which is the status change time, rather than `mtime` as the criterion for inclusion in an incremental

backup. The status change time of a file is the time at which a file's inode was last modified.

Using `ctime` results in the selection of all files that would have been selected using `mtime` plus those that have been moved or copied into the directory. Specify this option by specifying `-Xuse_ctime` on the command line. For a [scheduled backup](#), you can include `-Xuse_ctime` in the `backupoptions` policy.

There is a drawback to using `-Xuse_ctime`. When using the `mtime` criterion, `obtar` resets the `atime` of each file after it has been backed up. `atime` is the last accessed time. The act of backing up a file does not change the `atime` of the file. If you are using `ctime` as the selection criterion, then `obtar` cannot reset the time last accessed because it would reset the file's change time, thus turning every incremental backup into a [full backup](#). In other words, specifying `-Xuse_ctime` also turns on `-Xupdtu`.

The important points are as follows:

- If `-Xuse_ctime` is not specified, then incremental test is `mtime`, `atimes` are left unchanged, and moved files might be missed.
- If `-Xuse_ctime` is specified, then incremental test is `ctime`, `atimes` reflect time of backup, and moved files are caught.

B.2.4 Backing Up Across Mount Points

A local mount point mounts a local file system. A remote mount point is a local mount for a file system accessed over the network. By default, `obtar` does not cross local or remote mount points unless the mount point is explicitly specified.

You can control mount point behavior with the following `obtar` options:

- `-Xchkmnttab`

By default, `obtar` performs a `stat(2)` operation to determine whether a file represents a mount point. If a remotely mounted file system is down or not responding, then the `stat(2)` operation can cause the `obtar` process to hang.

The `-Xchkmnttab` option causes `obtar` to consult local mount table `/etc/mnttab` before performing these `stat(2)` operations and to skip directories determined to be remote mount points. Local mount points are not skipped.

You can specify `-Xchkmnttab` either on the command line or in the `backupoptions` policy. The `-Xchkmnttab` option is overridden by `-Xcrossmp`.

- `-Xcrossmp`

The `-Xcrossmp` option directs `obtar` to cross all mount points even if the `-Xchkmnttab` option is specified. You can specify the `-Xcrossmp` option on the command line or in the `backupoptions` policy.

See Also:

["backupoptions \(page 7-33\)"](#)

B.3.1 obtar -c

Purpose

Use `obtar -c` to create a single [backup image](#). You might use `obtar -c` to perform an [on-demand backup](#) or to back up data to a [volume](#) that you could transport to another site.

For NDMP backups, `obtar` uses the default NDMP backup type set for the data service. You can override this setting by specifying a backup type at the host level or by using the NDMP policy. `obtar` verifies that the user-specified backup type is valid for the data service that is used for the backup operation. However, the comparison used by `obtar` is case-sensitive and recognizes only lowercase values. Thus, if you specify the backup type using upper case, `obtar` does not recognize it as a valid backup type and uses the default NDMP backup type for the backup operation.

If the user ID (UID) or group ID (GID) of a file that is being backed up is greater than 2097151, Oracle Secure Backup substitutes the value 60002 for the UID or GID in the tar header file and returns a warning. This is because the maximum value for UID and GID, as defined by the POSIX standard (extended tar format), is 2097151. Therefore, when this backup is restored, the UID or GID for the restored file is 60002.

Syntax

`obtar -c::=`

```
obtar -c [ -f device ]  
[ -H host ] [ -G ]  
[ -v [ -v ] ] [ -z ]  
{ [ -C directory ] pathname... }...
```

Semantics

You can specify several options with `obtar -c`. This section describes those options that you are most likely to use. Refer to "[obtar Options](#) (page B-14)" to learn about additional `obtar -c` options.

-f device

Specifies the name of a [tape device](#). If you do not specify `-f`, then `obtar` writes to the tape device specified by the `TAPE` environment variable, if it is defined.

-H host

Specifies the host on which the data to be backed up is located. If you do not specify `-H`, then `obtar` looks for the data on the local host.

-G

Writes an index of the contents of the backup image to the [catalog](#) and generates a [volume label](#). The catalog data includes the names of all the files and directories written to the backup image. `obtool` uses this information to find the backup image containing the data to be restored.

When you create backup images with `obtar -c`, `obtar` does not ordinarily generate catalog files or volume identification. But you can use `-G` to generate them.

-v

Displays the path names of the files and directories being backed up. If you specify `-v` (or `-vv`), then `obtar` displays the path names of files and directories being backed up and their permissions, owner, size, and date of last modification.

-z

Create a labeled backup image.

-C directory

Causes `obtar` to change to the specified directory before backing up the subsequent files or directories. You use this option to control the path name information that is saved in the backup image.

pathname

Specifies one or more files or directories to back up. `obtar` issues a warning message if the contents of a file that you have specified change while a backup is taking place. The backup image you create includes data and path name information. When you restore the data, `obtar` uses `pathname` as the location for the restored data. The `obtar -x` command, which you use to restore data, provides options that let you specify a different `host` or `directory` location for the restored data.

If `pathname` refers to data available through a mount of a local or remote file system, then `obtar -c` does not cross the mount point unless you specify `-Xcrossmp` (page B-25).

You can also use the `-c` option to modify the `pathname` information that `obtar` records when you create the backup image.

Examples**Example B-1 Backing Up to a Volume**

To create a backup image on a volume, specify a tape device name with the `-f` option. This example backs up the directory `/doc` to the volume loaded on the tape device `tape0`.

```
obtar -c -f tape0 /doc
```

Example B-2 Backing Up Multiple Files

You can specify multiple directories or files to back up at a time. This example backs up the file `/jane/abc` and the file `/bob/xyz`.

```
obtar -c -f my_tape /jane/abc /bob/xyz
```

Example B-3 Changing Directory Information

You can use the `-c` option to control the path name information that is saved in the backup image. You use `-c` to specify the directory in which subsequent path names are located. `obtar` does not save that directory as part of the path name information in the backup image.

This example backs up the directory `/home/jane/current`. It uses the `-v` option to display the path names of the data being backed up.

```
obtar -cv -f tape1 -C /home/jane current
```

```
current/  
current/file1  
current/file2
```

As shown in the information displayed by the `-v` option, the path name information that `obtar` records in the backup image is the content of the relative path name `current`. When you subsequently restore the directory, unless you specify otherwise, `obtar` restores it to the directory named `current`, relative to your current directory.

Example B-4 Changing Directory Information

This example backs up the files `/test/proj3/trial7/test1` and `/test/proj3/trial7/test2`.

```
obtar -cv -f /dev/nrwst1 -C /test/proj3 trial7/test1 trial7/test2

trial7/test1
trial7/test2
```

The path name information that `obtar` records in the backup image includes the relative path names `trial7/test1` and `trial7/test2`. When you subsequently restore the files, unless you specify otherwise, `obtar` restores them to the directory `trial7` in your current working directory, first creating `trial7` if it does not exist.

B.3.2 obtar -x

Purpose

Use `obtar -x` to extract files from a [backup image](#). You can extract the entire contents of a backup image or only part of the backup image.

To restore data to your own directories, you do not need special [rights](#). To restore data into directories as `root`, you must be either be logged in as `root` or specify the `-R` option with the `obtar` command.

Syntax

```
obtar -x::=

obtar -x [ -kpORvzZ ]
[ -f device ]...
[ -F { cur|file-number } ]
[ -H destination-host ]
[ -s, prefix, [replacement, ] ] [ pathname ]...
```

Semantics

You can specify several options with `obtar -x`; this section describes those options that you are most likely to use. Refer to "[obtar Options](#) (page B-14)" to learn about additional `obtar -x` options.

pathname

Specifies the path names of files or directories to be extracted from the backup image. If you specify a directory, then `obtar` recursively extracts the contents of the directory. If you do not specify a path name, then `obtar` extracts the entire contents of the backup image.

-f device

Specifies the name of the [tape device](#) where the data is located. If you do not specify `-f`, then `obtar` reads from the tape device specified by the `TAPE` environment variable, if it is defined.

-F {cur|file-number}

Specifies the number of the backup image on the [volume set](#). If you do not specify `-F`, then `obtar` extracts the backup image at the current position of the [volume](#). If you specify `cur`, then `obtar` extracts the backup image at the volume's current position. This is the default. If you specify *file-number*, then `obtar` extracts the backup image at the specified file position.

-H destination-host

Specifies the host to which the data is restored. If you do not specify `-H`, then `obtar` restores the data to the local host.

-s,prefix,[replacement,]

Specifies where `obtar` should place the extracted files and directories. Use this option to extract files from a backup image and place them in a [location](#) that differs from the place from which you backed them up.

When you use `-s`, `obtar` substitutes the *replacement* string for *prefix* in the path name being restored. *prefix* must include the first part of the original path name. For example, if you backed up the directory `/home/jane/test`, and if you wanted the data restored to `/home/tmp/test`, then you would specify the string as follows:

```
-s,/home/jane,/home/tmp
```

If you omit the *replacement* string, then `obtar` assumes a null string, which causes `obtar` to remove the *prefix* from every *pathname* where it is found. The delimiter character, shown as a comma (,) in the syntax statement, can be any character that does not occur in either the *prefix* or the *replacement* string.

When you use `-s`, `obtar` displays the names of the files or directories as they are restored.

-k

Prevents `obtar` from overwriting any existing file that has the same name as a file in the backup image. In other words, `obtar` only restores files that do not exist.

-O

Causes `obtar` to stop after restoring the requested files. If `-O` is not specified, then `obtar` searches the entire backup image for subsequent copies of the requested files.

-R

Causes `obtar` to run with `root` access. To use `-R` you must be a member of a [class](#) with the `perform restores as privileged user` right. You are not required to use `-R` if you are logged in as `root`.

-v

Displays the path names of the files and directories being restored. If you specify `-v -v` (or `-vv`), then `obtar` displays the path names of files and directories being restored and their permissions, owner, size, and date of last modification.

-Z

Displays the [volume label](#) of the backup image if it has one.

-Z

Prevents `obtar` from decompressing any data that was compressed previously with `-z`. If you do not specify `-Z`, then `obtar` decompresses any data that was compressed previously with `-z`.

Examples

Example B-5 Extracting Files from a Backup Image

This example extracts the contents of backup image 4, which is on the volume loaded on tape device `tape1`.

```
obtar -x -f tape1 -F 4
```

Example B-6 Displaying the Contents of a Backup Image

This example uses the `-v` option to display the contents of the backup image as it is being extracted.

```
obtar -x -v -f tape1 -F 4
```

```
doc/  
doc/chap1  
doc/chap2  
test/  
test/file1  
test/file2
```

Example B-7 Displaying the Volume Label

This example uses the `-z` option to display the volume label of the volume being extracted.

```
obtar -x -z -f tape1 -F 4
```

Example B-8 Extracting Data to a Different Location

Use the `-s` option to place the extracted data in a location different from its original location. This option is particularly useful if you have backed up data and specified absolute path names. If you do not use `-s`, then `obtar` restores the data into the original directory, overwriting any existing data with that same name. This example extracts the `/doc` directory and places it in a directory called `/tmp/doc`.

```
obtar -x -f tape1 -s,/doc,/tmp/doc, /doc
```

Example B-9 Preventing obtar from Overwriting Files

This example prevents `obtar` from overwriting any files in the `/doc` directory that have the same names as files in the backup image:

```
obtar -x -f tape1 -k /doc
```

Example B-10 Restoring a Raw File-System Partition

This example restores the contents of a raw file-system partition. The partition is assumed to have been previously formatted and to be currently unmounted.

```
obtar -x -f tape0 /dev/rdsk/dks0d10s1
```

B.3.3 obtar -t

Purpose

Use `obtar -t` to list the names of files and directories contained in a [backup image](#). You can list the entire contents of a backup image or just part of the backup image. You can catalog a backup image by specifying `-Gt`. `obtar -t` does not list or import NDMP backups.

Syntax

`obtar -t::=`

```
obtar -t [ -f device ]  
[ -F { cur | file-number } ]  
[ -Gvz ]  
[ pathname ]...
```

Semantics

You can specify several options with `obtar -t`; this section describes those options that you are most likely to use. Refer to "[obtar Options](#) (page B-14)" to learn about additional `obtar -t` options.

-f device

Specifies the name of a [tape device](#). If you do not specify `-f`, then `obtar` reads from the tape device specified by the `TAPE` environment variable, if it is defined.

-F {cur | file-number}

Specifies the number of the backup image on the [volume set](#). If the file is on a [volume](#) different from the one currently loaded, then `obtar` prompts you to make any required volume changes. If you do not specify `-F`, then `obtar` reads the backup image at the current position of the volume.

If you specify `cur`, then `obtar` reads the backup image at the volume's current position. This is the default.

If you specify `file-number`, then `obtar` reads the backup image at the specified file position.

-v

Displays additional information about the contents of the backup image. The output is similar to that of the UNIX `ls -l` command. The additional information includes file and directory permissions, owner, size, and date of last modification.

-z

Displays the [volume label](#) of the backup image.

pathname

Specifies one or more path names of files or directories you want listed. If you specify a directory, then `obtar` recursively lists the contents of the directory. If you do not specify any path name arguments, then `obtar` lists the entire contents of the backup image at the volume's current [location](#) or at the location you specify with the `-F` option.

Examples

Example B-11 Displaying the Contents of a Backup Image

This example displays the contents of the backup image located at the current position of the volume loaded on tape device `tape1`.

```
# obtar -t -f tape1

project/
project/file1
project/file2
project/file3
```

Example B-12 Displaying the Contents of a Backup Image on a Volume Set

To display the contents of a particular backup image on a volume set, use the `-F` option. This example displays the contents of backup image 4.

```
# obtar -t -f tape1 -F 4

doc/
doc/chap1
doc/chap2
test/
test/file1
test/file2
```

Example B-13 Displaying Additional Information About a Backup Image

To display additional information about a backup image, use the `-v` option. This example uses the `-v` option to display additional information about backup image 4.

```
# obtar -t -v -f tape1 -F 4

drwxrwxr-x jane/rd      0 Feb 24 16:53 2000 doc/
-rw-r--r-- jane/rd     225 Feb 24 15:17 2000 doc/chap1
-rwxrwxr-x jane/rd     779 Feb 24 15:17 2000 doc/chap2
drwxrwxr-x jane/rd      0 Feb 24 16:55 2000 test/
-rwxrwxr-x jane/rd     779 Feb 24 16:54 2000 test/file1
-rw-r--r-- jane/rd     225 Feb 24 16:54 2000 test/file2
```

Example B-14 Displaying Information About a File in an Image

To display information about a particular file or directory that is contained in the backup image, include the file or directory name as the last argument on the command line. This example displays information about the directory `test`, which is contained in backup image 4.

```
# obtar -t -f tape1 -F 4 test

test/
test/file1
test/file2
```

Example B-15 Displaying Information About Multiple Directories

You can specify multiple path names from the backup image. This example displays information about the directories `test` and `doc`. `obtar` lists the directories in the order they appear in the backup image.

```
# obtar -t -f tape1 -F 4 test doc

doc/
doc/chap1
doc/chap2
test/
test/file1
test/file2
```

Example B-16 Cataloging a File-System Backup Image

Use the `-G` option to catalog the contents of a backup image. This example catalogs backup image 1 on the volume loaded into `tape drive` `tape1` (only partial output is shown). In this example, the image contains a `file-system backup`. You can catalog only one backup image at a time.

```
# obtar -f tape1 -tG -F 1

Volume label:
  Volume tag:          DEV100
  Volume ID:          VOL000001
  Volume sequence:    1
  Volume set owner:   root
  Volume set created: Tue Nov 22 15:57:36 2012

Archive label:
  File number:        1
  File section:       1
  Owner:              root
  Client host:        osbsvr2
  Backup level:       0
  S/w compression:   no
  Archive created:    Tue Nov 22 15:57:36 2012

/home/someuser/
/home/someuser/.ICEauthority
/home/someuser/.Xauthority
/home/someuser/.aliases
/home/someuser/.bash_history
/home/someuser/.bash_logout
/home/someuser/.bash_profile
/home/someuser/.bashrc
.
.
.
```

Example B-17 Cataloging an RMAN Backup Image

This example also catalogs backup image 1 on the volume loaded into `tape drive` `tape1`. In this example, the image contains an RMA backup of archived redo log files.

```
# obtar -f tape1 -tG -F 1

Volume label:
  Volume tag:          ADE202
  Volume ID:          RMAN-DEFAULT-000002
  Volume sequence:    1
  Volume set owner:   root
  Volume set created: Mon Feb 13 10:36:13 2006
  Media family:       RMAN-DEFAULT
  Volume set expires: never; content manages reuse
```

```

Archive label:
  File number:      1
  File section:    1
  Owner:           root
  Client host:     osbsvr1
  Backup level:    0
  S/w compression: no
  Archive created: Mon Feb 13 10:36:13 2006
  Backup piece name: 05hba0cd_1_1
  Backup db name:   ob
  Backup db id:    1585728012
  Backup copy number: non-multiplexed backup
  Backup content:  archivelog

```

B.3.4 obtar -zz

Purpose

Use `obtar -zz` to display all Oracle Secure Backup labels on a [volume](#).

Syntax

```

obtar -zz::=
obtar -zz [ -f device ]

```

Semantics

You can specify several options with `obtar -zz`; this section describes the option that you are most likely to use. Refer to "[obtar Options](#) (page B-14)" to learn about additional `obtar -zz` options.

-f device

Specifies the name of a [backup image file](#) or [tape device](#). If you omit the `-f` option, then `obtar` reads from the tape device specified by the `TAPE` environment variable, if it is defined.

Example

Example B-18 Displaying the Labels of All Backup Images on a Volume

As shown in [Example B-18](#) (page B-14), you can use `-zz` to display the labels of all backup images on a volume.

```
obtar -zzf tape0
```

Seq #	Volume ID	Volume Tag	Backup Image File Sect	Client Host	Backup Level	Backup Image Create Date & Time
1	VOL000003		1 1	campy	0	05/01/00 14:08:23
1	VOL000003		2 1	phred	0	05/01/00 15:37:00
1	VOL000003		3 1	mehitibel	0	05/01/00 15:38:08

B.3.5 obtar Options

The rows in [Table B-2](#) (page B-15) lists `obtar` options alphabetically. The columns indicate the `obtar` modes in which the options can be specified.

Table B-2 obtar Options

Option	-c	-t	-x	-zz
-A (page B-18)	x			
-b (page B-19)	x	x	x	
-B (page B-19)		x	x	
-C (page B-19)	x			
-e (page B-19)	x ¹	x	x	
-E (page B-19)	x ²			
-f (page B-20)	x	x	x	x
-F (page B-20)	x	x	x	
-G (page B-20)	x	x		
-h (page B-21)	x			
-H (page B-21)	x		x	
-J (page B-21)	x	x	x	x
-k (page B-21)			x	
-K (page B-21)	x		x	
-l (page B-21)	x		x	
-L (page B-22)	x			

Table B-2 (Cont.) obtar Options

Option	-c	-t	-x	-zz
-m (page B-22)			x	
-M (page B-22)	x			
-O (page B-23)			x	
-P (page B-23)	x			
-q (page B-23)		x	x	
-R (page B-23)	x	x	x	x
-s (page B-23)			x	
-u (page B-24)			x	
-U (page B-24)	x			
-v (page B-24)	x	x	x	
-V (page B-24)				
-w (page B-24)	x		x	
-Xallowdiffs pdev (page B-24)			x	
-Xcatalog (page B-25)				
-Xchkmnttab (page B-25)	x		x	

Table B-2 (Cont.) obtar Options

Option	-c	-t	-x	-zz
-Xcleara (page B-25)	x			
-Xcrossmp (page B-25)	x		x	
-Xdepth (page B-25)	x	x	x	
-Xfamily (page B-25)	x			
-Xhighlatency (page B-25)	x			
-Xhome (page B-25)	x		x	
-Xincrstore (page B-25)			x	
-Xinstance (page B-25)				
-Xkv (page B-26)	x			
-Xmarkerfiles (page B-26)	x			
-Xnice (page B-26)	x	x	x	x
-Xno_mod_chk (page B-26)	x			
-Xnochaselinks (page B-26)	x			

Table B-2 (Cont.) obtar Options

Option	-c	-t	-x	-zz
-Xnostat (page B-26)	x			
-Xow (page B-26)	x			
-Xupdtu (page B-26)	x			
-Xuq (page B-27)	x			
-Xuse_ctime (page B-27)	x			
-Xverifyarchive (page B-27)	x			
-Xww (page B-27)	x			
-y (page B-27)	x			
-Z (page B-27)	x		x	

¹ when -G is also specified

² when -G is also specified

-A

Does not save Access Control Lists (ACLs), Context Dependent Files (CDFs), and other extended file-system attributes for files backed up on Hewlett-Packard platforms (HP-UX operating system). By default, `obtar` saves all file-system attributes for each file. When you restore these files on Hewlett-Packard platforms, the extended attributes are also restored.

When you restore these files on other platforms, `obtar` ignores the ACL information. On Windows, Linux, and UNIX platforms, the `-A` flag causes `obtar` to save only the primary data stream associated with each file, excluding the extended attributes and ACLs.

 **See also:**

"Oracle Secure Backup Support for Extended Attributes and Access Control Lists (page D-1)" for more information on performing backup and recovery with extended attributes and access control lists

-b blocking-factor

Writes data in block sizes of *blocking-factor* multiplied by 512 bytes. By default, `obtar` uses the [blocking factor](#) specified by the `blockingfactor` (page 7-25) media policy. When you restore files, `obtar` automatically determines the block size that was used when backing up the data.

-B

Performs multiple reads to fill a block. If you are using `obtar` with UNIX pipes or sockets, then the UNIX `read` function can return partial blocks of data even if more data is coming.

For example, suppose you want to restore data from a [tape device](#) that is attached to a host where Oracle Secure Backup is not installed. The following command restores the `/doc` directory from a tape device attached to the host named `logan`:

```
rsh logan cat /dev/nrst0 | obtar -x -B -f - /doc
```

If you specify a remote tape device with the `-f` option, then you are not required to use `-B` because the `obtar` network protocol guarantees reading and writing full blocks.

-C directory

Changes the directory structure associated with the files being backed up. With this option, `obtar` changes its working directory to *directory* and backs up files relative to it. `obtar` uses *directory* as its current directory until the next `-c` option on the command line. When you restore the files, they are restored relative to *directory*.

-e volume-id

Uses *volume-id* in the [volume label](#) for this [backup image](#) (when backing up) or looking for *volume-id* in the volume label (when restoring). A [volume ID](#) contains up to 31 characters, in any combination of alphabetic and numeric characters, although the last 6 characters must be numeric. If you do not specify a volume ID when backing up, then `obtar` uses the volume ID in the volume-sequence file in the administrative directory (the default) or the volume ID file specified with the `-E` option.

Typically, you use `-e` to verify that you are restoring the correct [volume](#) when running `obtar -x` or `obtar -t` from a script. `obtar` tries to match the volume ID with the volume ID in the label and exits if it does not find a match. If the [tape drive](#) from which you are indexing or restoring data is contained within a [tape library](#), then supplying `-e` on the command line directs `obtar` to attempt to load that volume into the tape drive before beginning the operation.

-E volume-id-file

Uses the volume ID from *volume-id-file* in the volume label. `obtar` looks for *volume-id-file* in the administrative directory on the [administrative server](#). If you do not specify this option, then `obtar` uses the volume ID from volume-sequence, the default volume ID file.

-f device

Specifies the name of the tape device on which you want the backup image created. The device argument to `-f` is the name that you have assigned to a tape drive in an [administrative domain](#).

If you do not specify the `-f` option, then Oracle Secure Backup uses the tape device specified by the `TAPE` environment variable, if it is defined.

When you are backing up a large amount of data, `obtar` might be required to continue a backup image from one volume to the next. If the tape drive resides in a tape library, then `obtar` automatically unloads the current volume and searches the inventory of the tape library for another eligible volume on which to continue the backup. The way that you install and configure `obtar` indicates whether it considers a tape device to reside inside a tape library.

If you are using a standalone tape drive, and if data still must be written at the end of a volume, then `obtar` rewinds the tape and unloads it. `obtar` displays a message like the following on the [operator host](#), where `vol-id` refers to the next volume in the [volume set](#):

```
End of tape has been reached. Please wait while I rewind and unload the tape. The
Volume ID of the next tape to be written is vol-id.
The tape has been unloaded.
```

```
Please insert new tape on device
and press <return> when ready:
```

The backup continues onto the next volume.

-F {cur | end | file-number}

Writes or reads a backup image at the indicated position in a volume set, instead of the current volume position (default). Use this option only when writing to or reading from a tape device. `obtar` positions the tape to the requested file in the volume set. If the file is on a volume that is not loaded, then `obtar` prompts you to load the necessary volume.

If you specify the position as `cur`, then `obtar` writes or reads the backup image at the current volume position.

If you specify `end`, then `obtar` writes the backup image immediately after the last existing backup image in the volume set.

If you specify `file-number`, then `obtar` writes the backup image at the specified file position. `obtar` numbers each backup image on a volume set sequentially, beginning with 1.

 **Note:**

When `obtar` creates a backup image at a specified volume position, the backup image becomes the last backup image, even if the volume previously contained additional backup images. For example, if you write a backup image at position 6 on a volume containing 11 backup images, then you effectively erase backup images 7 through 11. With `obtar -t` and `obtar -x`, you can use the `-q` option instead of this option.

-G

Writes an index of the backup image contents to the [catalog](#) and generates a volume label. The contents can include file-system backups or [Recovery Manager \(RMAN\)](#)

backups. `obtool` uses this information to find the backup image containing the data to be restored.

-h

When the data to be backed up includes symbolic links, `obtar` ordinarily backs up only the link text, not the data to which the link points. You can use the `-h` option to cause `obtar` to back up the data, not just the link text.

If you include an explicit link path name when using `obtar -c`, then `obtar` backs up the data specified by that link whether you have used the `-h` option or not. If you do not want `obtar` to follow explicitly mentioned links, then you can do so by specifying `-Xnochaselinks`.

-H host

Backs up data from or restores data to `host` instead of from the local host (default).

-J

Directs `obtar` to produce debugging output as it runs.

-k

Restores only the files that do not exist. That is, `obtar` does not [overwrite](#) any existing files with the version from the backup image. By default, `obtar` overwrites any existing files.

-K mask

Specify device driver debug options. `mask` is the bitwise inclusive or of the following values shown in [Table B-3](#) (page B-21).

Value	Meaning
800	Turn on debug modes before open
400	Allow only one write at BOT
200	Inject write error
100	Debug kernel driver
080	Enable time-outs
040	Disable time-outs
020	Enable debugging at EOM
010	Generate early EOT
008	Trace DMA activity
004	Trace miscellaneous info
002	Trace errors
001	Trace driver calls

Note:

This option can lead to voluminous output and should normally be used only when directed by Oracle Support Services.

-l

Forces `obtar` not to cross file-system mount points when backing up or restoring.

By default, `obtar` does not cross mount points unless you explicitly include mount point statements in a backup description file. If you specify `-l`, then `obtar` ignores these explicit override settings and does not cross mount points.

Note that if you also specify `-Xchkmnttab` (page B-25), then specifying `-l` causes `obtar` to consult the mount table (`/etc/mnttab`) to avoid crossing remote mount points. When backing up or restoring an **NT File System (NTFS)** partition under Windows 2000, name surrogate reparse points (for example, directory junctions) are treated as mount points.

If you use this option with the `-v` option, then `obtar` writes the names of any files it skips to standard error.

-L {full | incr | exincr | offsite | n | date-time}

Uses the specified **backup level** instead of a **full backup** (default).

`full` specifies a full backup, which saves all data that is specified in the `obtar -c` command.

`incr` specifies an **incremental backup**, which saves only the data that was modified since the last backup.

`exincr` specifies an extended incremental, which saves only the data that was modified since the last full backup.

`offsite` generates an **on-demand backup** that does not affect the subsequent scheduling of full and incremental backups.

You can also specify a numeric backup level, `n`, which can range from 0 to 9 and saves only the data that was modified since the last backup at a lower level. Backup level 0 is identical to `full`, and level 1 is identical to `exincr`.

If you use a `date-time` argument, then `obtar` saves only the data that was modified since that time. Note that using a `date-time` argument does not create a true incremental backup because it cannot be used as a reference point for later incremental backups. The `date-time` argument must be in the form appropriate to the locale in which you run `obtar`. For the U.S., specify `date-time` in the following format:

```
mm/dd[/yy] [hh[:mm[:ss]]]
```

If you supply `hh`, `hh:mm`, or `hh:mm:ss` as part of `date-time`, then you must enclose `date-time` in quotes. If you do not supply the year (`/yy`), then `obtar` uses the preceding 12 months. If you supply `hh:mm` but not `ss`, then `obtar` uses `hh:mm:59`.

-m

Uses the current time as the `last time modified` timestamp instead of the time that is saved with the backup image (default).

In the following example, the timestamp for all directories and files in the `/old` directory is changed to the current date and time:

```
obtar -x -m -f tape0 /old
```

-M parameter:value

You can use `-M` to turn hardware compression on or off for any tape device that supports hardware compression. `obtar` turns hardware compression on by default. To set hardware compression, specify `on` to turn hardware compression on, and specify `off` to turn hardware compression off:

```
-M compress:{on|off}
```

If you turn on hardware compression, then the tape device automatically decompresses data when you restore it. You should not use hardware compression at the same time as the `-z` option.

-O

Ends a restore operation after first occurrence of files being restored. Normally, `obtar -x` scans an entire backup image looking for multiple copies of each file to be restored. If you specify `-O`, then the restore stops after each file has been restored once.

-P

A sparse file is a file with areas that have never be written to. Ordinarily, `obtar` does not usually perform any special handling of sparse files. If you specify the `-P` option when you create a backup image with `obtar -c`, then `obtar` compacts any sparse files in the backup image. When you subsequently restore the backup image, `obtar` restores the sparse files to their original format.

 **Note:**

This option does not apply to sparse files under Windows 2000, which are always backed up and restored in sparse form.

-q position-string

If you are using a tape device that supports direct-to-block positioning, then you can use the `-q` option to rapidly locate particular data on a volume. The argument to `-q` is a position-string that you obtain from the `ls --backup --position` command in `obtool`. When you use `-q`, `obtar` positions the volume directly to the [location](#) you specify. For example, you can use the `ls` command in `obtool` to identify the position of the file `/home/gms/output/test001`:

```
obtool ls --backup --position /home/gms/output/test001
```

```
test001
```

```
Backup Date & Time ID Volume ID Volume Tag File Sect Level Position
2006/01/11.10:16:28 3 VOL000106 00000110 11 0 000045020008
```

After obtaining the position data, you can specify the `-q` option with `obtar -t` as shown in the following example:

```
obtar -t -f tape1 -q 000045020008
```

-R

Runs `obtar` with `root` access. To use `-R` you must be a member of a [class](#) with the [perform file system restores as privileged user](#) (page 8-6) or [perform file system backups as privileged user](#) (page 8-6) right. You are not required to specify `-R` if you are logged in as `root`.

-s,prefix,[replacement,]

Substitutes *replacement* for each occurrence of *prefix* in all path names that are being restored. *prefix* must include the first part of the original path name. If you omit *replacement*, then `obtar` removes all occurrences of *prefix* in all path names being restored. If the character does not occur in either the *prefix* or the *replacement* string, then you can use another delimiter character instead of a comma (,). You can use this option to extract files from a backup image and place them in a location different from where they were backed up.

-u

When restoring files, `obtar` overwrites existing files unless explicitly told not to. On systems that support file locking, this replacement of existing files occurs even for files that are currently in use. Specify `-u` on the `obtar` command line to avoid overwriting files that are currently in use.

-U

Updates backup dates file in the administrative directory. This option overrides the setting of the `autohistory` operations policy.

-v

Writes verbose information about files to standard output or standard error.

When used with `obtar -c`, this option writes the names of the files being backed up and the volume label (if one was created) to standard error.

When used with `obtar -t`, this option writes additional information about the files, which is similar to the output of the `ls -l` command, instead of writing just the filenames (default) to standard output.

When used with `obtar -x`, this option writes the names of the files being restored to standard output. If you specify `-vv`, then `obtar` writes verbose information about files, which is similar to the output of the `ls -l` command, to standard error (`obtar -c`), or standard output (`obtar -x`).

**Note:**

The user ID (UID) or group ID (GID) reported by the `-v` option might not match the actual UID or GID for a file. The maximum values for UID and GID are defined by the POSIX standard (extended tar format). During a [backup operation](#), if Oracle Secure Backup encounters a file whose UID or GID exceeds the maximum (2097151) that fits in a tar header, then it substitutes 60002 as the UID or GID and returns a warning. The exit status of the backup reflects the presence of such warnings.

-V

Prints the version of `obtar` and exits.

-w

Directs `obtar` to check for and honor advisory file locks before backing up or restoring a file. If a lock is set, then `obtar` displays a warning message and skips the file.

-Xallowdiffspldev

By default, you can restore a raw partition only to a block device that has the same major or minor number as the block device to which the partition was backed up. To restore a raw partition to a block device whose major or minor numbers are different from number of the block device to which the partition was backed up, use the `-Xallowdiffspldev` option.

**Note:**

The `Xallowdiffspldev` option is only available starting with Oracle Secure Backup 10.3.0.2.0.

-Xcatalog

Allows cataloging of a single instance from a disk pool or cloud container device. Use this option with the `-Xinstance` option to specify the instance UUID to be imported.

-Xchkmnttab

Causes `obtar` to consult the local mount table (`/etc/mnttab`) before performing `stat(2)` operations and to skip directories known to be remote mount points. Local mount points are not skipped. This option applies to Linux and UNIX only.

The `-Xchkmnttab` option can avoid hangs caused by remote hosts that are down or not responding. The `-Xchkmnttab` option is overridden by `-Xcrossmp` (page B-25).

 **See Also:**

"[backupoptions](#) (page 7-33)" for instructions on specifying the `-Xchkmnttab` option in the `backupoptions` operations policy

-Xcleara

Clears the archive file attribute bit for each file that is successfully backed up. In the absence of this option, `obtar` leaves the archive file bits unmodified. Windows only.

-Xcrossmp

Directs `obtar` to cross all mount points regardless of whether the `-l` (page B-21) or `-Xchkmnttab` (page B-25) options are specified. By default, `obtar` does not cross mount points.

Note that you can specify the `-Xcrossmp` option in the [backupoptions](#) (page 7-33) operations policy.

-Xdepth:levs

Specifies the maximum number of index levels to display.

-Xfamily[:family]

Specifies that the volume being labeled belongs to [media family](#) *family*.

-Xhighlatency

Causes `obtar` to fetch data pointed to by a reparse point. Normally, when confronted with a high latency reparse point, `obtar` backs up the reparse point, but not the underlying data. Windows only.

-Xhome:dir

Sets the home directory on the `client` host to `dir` before starting a backup.

-Xincrrestore

Performs an incremental [Network Data Management Protocol \(NDMP\)](#) restore for [Network Attached Storage \(NAS\)](#) devices.

-Xinstance

Specifies a single backup image instance UUID to be cataloged from a disk pool device or cloud container device. This option must be used in conjunction with the `-Xcatalog` option. The following is a sample command issued on the media server that uses the `Xinstance` option:

```
# obtar -Xcatalog -Xinstance:8d866afc-clcf-1034-a202-0021f618cfbf -f disk1
```

-Xkv:time_spec

Specifies the length of time a volume should be retained. *time_spec* is disabled (no retention time), *forever*, or *n tu*, where *tu* is one of *secs* (or seconds), *mins* (minutes), *hrs* (hours), *days*, *wks* (weeks), *mos* (months), or *yrs* (years). This option is effective only when writing to the first file of a volume.

-Xmarkerfiles

Directs *obtar* to honor index marker files encountered during a backup. Currently, there is a single index marker file defined: *.ob_no_backup*. If a file with this name appears in a directory, and if you specify *-Xmarkerfiles*, then *obtar* does not back up this directory or any of its subdirectories.

-Xnice:val

Directs *obtar* to set the *nice(1)* value for the backup or restore process to *val*. This value is propagated to any local and remote subprocesses spawned by *obtar* to perform the requested operation.

On Windows, the specified *val* is mapped to a Windows process priority value according to the following rules:

- If *val* \geq -20 and *val* \leq -6, then the value is translated into *ABOVE_NORMAL_PRIORITY_CLASS*.
- If *val* \geq -5 and *val* \leq 4 it is translated into *NORMAL_PRIORITY_CLASS*.
- If *val* \geq 5 and *val* \leq 19 it is translated into *BELOW_NORMAL_PRIORITY_CLASS*.
- If the value does not fall in the preceding ranges, then *obtar* issues a warning and ignores the value.

-Xno_mod_chk

Omits a modification check when backing up a file. Normally, after *obtar* has backed up a file, it checks whether the file was modified while it was being backed up. If the file was modified, then *obtar* prints a warning message. Setting this option can improve performance.

-Xnochaselinks

Avoids following links anywhere, even if they are explicitly mentioned on the command line.

-Xnostat

Does not include file stat data (ownership, permissions, size) in index file. By default, Oracle Secure Backup writes this data to the index file and subsequently imports it into the [catalog](#).

-Xow

Disregards any expiration date in the volume label. If you try to overwrite a volume that has not yet expired, then the operation fails unless you specify *-Xow*.

-Xupdtu

Does not reset a file's access time after backing it up. After *obtar* has backed up a file, it normally resets the file's access time (*atime*) back to what it was before the backup started. The act of backing of a file does not change the original *atime*. If you are not concerned with backups changing files' *atimes*, then specifying this option results in a slight increase in backup performance.

-Xuq:n

Specifies the size of the `utime` helper queue. When backing up data, `obtar` uses a helper process to run `utime(2)` calls to reset access times on files being backed up. This parameter controls the size of the input queue for the `utime` helper. Linux and UNIX only.

-Xuse_ctime

Directs `obtar`, when performing an incremental backup, to use the `ctimes` (inode change times) rather than `mtimes` (modified times) for files as the criteria for being included in the backup. Use of this option implies `-Xupdtu`.

-Xverifyarchive

Causes `obtar`, on completing a backup section, to backspace the tape to the beginning of the section and read the contents.

-Xww:time_spec

Specifies the [write window](#) expiration time for a volume. `time_spec` is specified as for the `-Xkv` option. The given time specification is added to the time at which the volume is created to determine a time after which further writes to the volume are disallowed. This option is effective only when writing to the first file of a volume.

-y status-file

Writes status information about the backup session to `status-file`. You can retain these statistics in the [media server](#) observed log file by setting the `retainbackupmetrics` policy.

**See Also:**

["retainbackupmetrics" \(page 7-41\)](#)

-Z

Compresses data (when backing up) or keeps data compressed (when restoring). When you use `-z` to create a backup image, `obtar` compresses files using the same algorithm as the UNIX `compress(1)` utility before writing them to the backup image. If the files are compressed or would not shrink if compressed, then `obtar` does not compress them. When you restore files that have been compressed, `obtar` automatically decompresses them unless you specify `-z` to suppress decompression. It is almost always preferable to rely on the tape drive's hardware compression capability, if it is available.

**Note:**

As of Oracle Secure Backup 12.2.0.1, new backups are not allowed to compress data using the `-z` option. The `-z` option is retained only for use in restoring older compressed legacy backups with the `restore` command.

C

RMAN Media Management Parameters

This appendix describes Oracle Secure Backup-specific media management parameters that you can specify in [Recovery Manager \(RMAN\)](#) backup and restore jobs. You can specify media management parameters in RMAN backup and restore jobs by the following means:

- Environment variables, which are specified with the `ENV` parameter of the `PARMS` option on the `CONFIGURE` or `ALLOCATE CHANNEL` commands
- The RMAN `SEND` command

This section describes Oracle Secure Backup parameters that are valid in RMAN jobs.

This section contains the following topics:

- [Database Backup Storage Selectors and RMAN Media Management Parameters](#) (page C-1)
- [About Setting the Job Priority for RMAN Operations](#) (page C-2)
- [OB_BACKUP_NAME](#) (page C-2)
- [OB_DEVICE](#) (page C-3)
- [OB_ENCRYPTION](#) (page C-4)
- [OB_IGNORE_NUMA](#) (page C-6)
- [OB_MEDIA_FAMILY](#) (page C-6)
- [OB_PRIORITY](#) (page C-7)
- [OB_RESOURCE_WAIT_TIME](#) (page C-8)
- [OB_RESTORE_DEVICE](#) (page C-10)

C.1 Database Backup Storage Selectors and RMAN Media Management Parameters

You can configure [tape device](#) and [media family](#) restrictions in both database backup storage selectors, which are created with the `mkssel` (page 3-54) command, and the `OB_DEVICE` and `OB_MEDIA_FAMILY` [Recovery Manager \(RMAN\)](#) media management parameters.

During a backup operation, Oracle Secure Backup first checks if tape device or media family restrictions are specified using RMAN media management parameters. If RMAN parameters are not set, then the values specified in the backup storage selector are used for the backup operation.

[Table C-1](#) (page C-2) explains the criteria used by Oracle Secure Backup when choosing the media family and tape device for an RMAN [backup job](#).

Table C-1 Determining Media Family and Device Settings

Matching Selector	Device Set in Selector	OB_DEVICE Set in Job	OB_MEDIA_FAMILY Set in Job	Result
Yes	Yes	No	No	Oracle Secure Backup uses the tape device and media family settings in the backup storage selector.
Yes	Yes or No	Yes	Yes	Oracle Secure Backup uses the tape device and media family settings in the RMAN channel parameters.
Yes	Yes or No	Yes	No	Oracle Secure Backup uses the <code>OB_DEVICE</code> setting and the media family specified in the selector.
Yes	Yes	No	Yes	Oracle Secure Backup uses the tape device settings in the selector and media family settings in the RMAN channel parameters.
Yes	No	No	Yes	Oracle Secure Backup does not restrict the tape device (that is, chooses any tape device in the domain) and uses the media family setting in the RMAN channel parameters.
No	N/A	Yes	No	Oracle Secure Backup uses the <code>OB_DEVICE</code> setting and <code>RMAN-DEFAULT</code> media family.
No	N/A	No	No	Oracle Secure Backup does not restrict the tape device (that is, chooses any tape device in the domain) and uses the <code>RMAN-DEFAULT</code> media family.

C.2 About Setting the Job Priority for RMAN Operations

If the `OB_PRIORITY` (page C-7) Media Management parameter is set for a backup job, then the specified job priority value is always used for the backup job.

Otherwise, if the RMAN priority is set in a storage selector that is associated with an RMAN backup job, then the job priority specified in the storage selector is used.

If neither the `OB_PRIORITY` Media Management parameter is specified, nor any storage selector is specified, then the job priority value specified in the `rmanpriority` (page 7-37) policy is used for the backup job.

C.3.1 OB_BACKUP_NAME

Purpose

Use the `OB_BACKUP_NAME` parameter to specify the format information for a backup image.

 **See Also:**

"[name-format](#) (page 4-19)" for information about the format used for naming backup images

Syntax

OB_BACKUP_NAME::=

OB_BACKUP_NAME [=] backupname

Semantics***backupname***

Specifies the format information for a backup name.

Example

This example uses the `SEND` command to specify the name format information `my_rman_backup_brhost2` for a backup image.

Example C-1 Backup Name with SEND Command

```
RUN
{
ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
SEND "OB_BACKUP_NAME my_rman_backup_brhost2";
BACKUP TABLESPACE users;
}
```

C.3.2 OB_DEVICE

Purpose

Use the `OB_DEVICE` parameter to define which backup container to use for backups.

Restrictions and Usage Notes

Before specifying `OB_DEVICE[_n]` in a [Recovery Manager \(RMAN\)](#) job, note the following:

- This parameter does not affect restore jobs.
- Channels can only be restricted to tape drives, not tape libraries.
- [Table C-1](#) (page C-2) explains the criteria used by Oracle Secure Backup when choosing the [media family](#) and [tape device](#) for an RMAN [backup job](#).

Syntax

OB_DEVICE::=

OB_DEVICE[_n] [=] { *device_name* | [*device_name*]@*hostname* }

Semantics

_n

Specifies the copy number of duplexed backups. For duplexed backups, `OB_DEVICE_1` is for the first copy, `OB_DEVICE_2` is for the second copy, and so on.

device_name

Specifies the name of the backup container to which the backup should be restricted.

host_name

Specifies the name of the host to which the backup should be restricted.

If `drive_name@host_name` is specified, then Oracle Secure Backup uses the specified tape device with the specified host. If `@host_name` is specified, then Oracle Secure Backup uses any tape device attached to the host with the name `host_name`.

Examples

Example C-2 SBT Backup with SEND Command

This example uses the `SEND` command to specify that RMAN backs up to any tape drive on host `brhost1`. Note that no equal sign is inserted between the parameter `OB_DEVICE` and the names of the tape drives.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
  SEND 'OB_DEVICE @brhost1';
  BACKUP TABLESPACE users;
}
```

Example C-3 SBT Backup with ENV Parameter

This example uses `PARMS` to set the Oracle Secure Backup media family and device parameters. This parameter instructs RMAN to back up to the device named `tape2` and use the media family `my_full_backups`. Note that an equal sign is inserted between the parameter `OB_DEVICE` and the value `tape2`.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt
  PARMS 'ENV=(OB_DEVICE=tape2, OB_MEDIA_FAMILY=my_full_backups)';
  BACKUP TABLESPACE users;
}
```

C.3.3 OB_ENCRYPTION

Purpose

Use the `OB_ENCRYPTION` parameter to control Oracle Secure Backup encryption.

Restrictions and Usage Notes

In all cases, if the backup data is already encrypted by RMAN, then Oracle Secure Backup performs no further encryption.

If Oracle Secure Backup applies encryption, then the encryption algorithm depends on the algorithm configured for the Oracle Secure Backup host being backed up.

Syntax

OB_ENCRYPTION::=

```
OB_ENCRYPTION[=]{ on | off | forcedoff | swencryption }
```

Semantics

on

Uses Oracle Secure Backup to encrypt the backup data unless it has already been encrypted by RMAN.

off

Does not use Oracle Secure Backup to encrypt the backup data unless either the host or global policy is set to *required*.

Setting `OB_ENCRYPTION` to *off* is equivalent to specifying no value for it. All the normal rules of Oracle Secure Backup encryption still apply regarding whether the data will be stored on tape in encrypted form.

forcedoff

Does not use Oracle Secure Backup to encrypt the database backup, overriding any host-specific encryption settings.

The *forcedoff* setting does not affect RMAN, which can encrypt the backup data.

swencryption

Forces Oracle Secure Backup to use software encryption instead of hardware encryption.

Examples

Example C-4 Encrypted Backup with SEND Command

This example uses the `SEND` command to specify Oracle Secure Backup encryption of the `users` tablespace backup. If RMAN is already encrypting the backup of `users`, then Oracle Secure Backup does not apply further encryption. Note that no equal sign is inserted between the parameter `OB_ENCRYPTION` and the value `on`.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
  SEND 'OB_ENCRYPTION on';
  BACKUP TABLESPACE users;
}
```

Example C-5 Persistent Encryption Configuration

This example persistently configures Oracle Secure Backup *not* to apply encryption to an RMAN backup under any circumstances. Note that there is an equal sign between the parameter `OB_ENCRYPTION` and the value `forcedoff`.

```
CONFIGURE CHANNEL DEVICE TYPE sbt PARMS
  'ENV=(OB_ENCRYPTION=forcedoff)';
```

C.3.4 OB_IGNORE_NUMA

Purpose

Use the `OB_IGNORE_NUMA` parameter to indicate if Oracle Secure Backup must enable Non-Uniform Memory Access (NUMA) awareness. Enabling NUMA awareness may result in improved performance for Oracle Database backup and restore operations on NUMA machines.



See Also:

Oracle Secure Backup Administrator's Guide for more information about NUMA

Restrictions and Usage

None

Syntax

OB_IGNORE_NUMA::=

```
OB_IGNORE_NUMA[=]{0|1}
```

Semantics

0

Oracle Secure Backup does not attempt to co-locate the Oracle shadow process and the Oracle Secure Backup data service. This setting is primarily used for testing.

1

Oracle Secure Backup ensures that, on NUMA machines, the Oracle shadow process and the Oracle Secure Backup data service are located in the same NUMA node. This is the default setting.

Example

Example C-6 Disabling NUMA-awareness

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
  SEND 'OB_IGNORE_NUMA 1';
  BACKUP TABLESPACE users;
}
```

C.3.5 OB_MEDIA_FAMILY

Purpose

Use the `OB_MEDIA_FAMILY` parameter to define which media to use for a backup job.

Restrictions and Usage Notes

Before specifying `OB_MEDIA_FAMILY[_n]` in a [Recovery Manager \(RMAN\) job](#), note the following:

- This parameter does not affect restore jobs.
- You can only specify a content-managed [media family](#). By default RMAN uses the `RMAN-DEFAULT` media family.
- [Table C-1](#) (page C-2) explains the criteria used by Oracle Secure Backup when choosing the media family and [tape device](#) for an RMAN backup job.

Syntax

OB_MEDIA_FAMILY::=

```
OB_MEDIA_FAMILY[_n][=]media_family_name
```

Semantics

_n

Specifies the copy number of duplexed backups. For duplexed backups, `OB_MEDIA_FAMILY_1` is for the first copy, `OB_MEDIA_FAMILY_2` is for the second one, and so on.

media_family_name

Specifies the name of the media family.

Examples

Example C-7 SBT Backup with SEND Command

This example uses the `SEND` command to specify the `my_full_backups` media family in an RMAN database backup. Note that there is no equal sign between the parameter `OB_MEDIA_FAMILY` and the value `datafile_mf`.

```
SEND 'OB_MEDIA_FAMILY datafile_mf';
BACKUP TABLESPACE users;
```

Example C-8 SBT Backup with ENV Parameter

This example makes the same backup as [Example C-7](#) (page C-7), but uses `PARMS` to set the Oracle Secure Backup media family parameter. Note that there is an equal sign between the parameter `OB_MEDIA_FAMILY` and the value `datafile_mf`.

```
CONFIGURE CHANNEL DEVICE TYPE sbt PARMS
  'ENV=(OB_MEDIA_FAMILY=datafile_mf)';
BACKUP TABLESPACE users;
```

C.3.6 OB_PRIORITY

This topic describes the `OB_PRIORITY` parameter.

Purpose

Use the `OB_PRIORITY` parameter to schedule the priority of occurrence for your backup and restore jobs.

The priority value set for a job using this parameter overrides any priority value specified within a database storage selector.



See Also:

[About Setting the Job Priority for RMAN Operations](#) (page C-2)

Syntax

OB_PRIORITY::=

```
OB_PRIORITY [=] priority_value
```

Semantics

priority_value

Specifies a positive integer value that sets the priority for backup and restore jobs. You can set this value between 1 and 2147483647, with 1 being the highest job priority. The default job schedule-priority value is 100.

Example

Example C-9 Setting Priority with SEND command

This example sets the priority to 10 for an RMAN backup job using the `SEND` command. Note that there is no equal sign between the parameter `OB_PRIORITY` and the value 10.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
  SEND "OB_PRIORITY 10"
  BACKUP TABLESPACE users;
}
```

Example C-10 Setting Priority with ENV Parameter

This example schedules the priority of a backup job to 25 using the `ENV` parameter. Note that there is an equal sign between the parameter `OB_PRIORITY` and the value 25.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt
  PARS 'ENV=(OB_DEVICE=tape2, OB_MEDIA_FAMILY=my_full_backups, OB_PRIORITY=25);
  BACKUP TABLESPACE users;
}
```

C.3.7 OB_RESOURCE_WAIT_TIME

Purpose

Use the `OB_RESOURCE_WAIT_TIME` parameter to specify the duration for which a backup or restore job should wait for the required resources to become available.

Restrictions and Usage Notes

Note that you can specify [Recovery Manager \(RMAN\)](#) resource wait times in the following locations, each of which overrides the preceding specifications in the list:

1. The `rmanresourcewaittime` policy



See Also:

["rmanresourcewaittime"](#) (page 7-38)

2. The `waittime` attribute in a [database backup storage selector](#) that matches an RMAN [backup job](#)
3. The RMAN channel configuration parameter `OB_RESOURCE_WAIT_TIME`

Syntax

OB_RESOURCE_WAIT_TIME::=

`OB_RESOURCE_WAIT_TIME=duration`

Semantics

duration

Specifies how long Oracle Secure Backup should wait for the tape resources to become available. For valid values, refer to the description of the *duration* placeholder in ["duration"](#) (page 4-14).

Examples

Example C-11 SBT Restore with SEND Command

This example uses the `SEND` command to specify that the restore job should wait no longer than 10 minutes for tape resources to become available. Note that there is no equal sign between the parameter `OB_RESOURCE_WAIT_TIME` and the value.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt;
  SEND 'OB_RESOURCE_WAIT_TIME 10minute';
  RESTORE ARCHIVELOG ALL;
}
```

Example C-12 SBT Restore with ENV Parameter

This example uses the `ENV` parameter to specify the wait time on a configured channel. Note that there is an equal sign between the parameter `OB_RESOURCE_WAIT_TIME` and the value.

```
CONFIGURE CHANNEL DEVICE TYPE sbt PARMS
  'ENV=(OB_RESOURCE_WAIT_TIME=10minute)';
RESTORE ARCHIVELOG ALL;
```

C.3.8 OB_RESTORE_DEVICE

Purpose

Use the `OB_RESTORE_DEVICE` parameter to define which tape drive to use for a restore job.

This parameter enables you to restrict a restore job to a particular tape device. You can use this parameter to restore Oracle Database backups.



Note:

The `OB_RESTORE_DEVICE` parameter is only available starting with Oracle Secure Backup 10.3.0.2.0.

Restrictions and Usage Notes

The device restriction is honoured above the location of the volume. If a volume required for the restore job is loaded into a drive other than the one specified by *devicename*, then the volume will be unloaded from the drive and loaded into *devicename*. However, this is possible only when the two drives, the one specified by `OB_RESTORE_DEVICE` and the drive with the required volume, are both in the same library.

The device specified in the `OB_RESTORE_DEVICE` parameter must be attached to the library where the volume resides. If the device is not attached, the restore job fails.

The volume must reside in the tape drive specified using `OB_RESTORE_DEVICE` or in the library that the specified tape drive belongs to. If a restore job is restricted to a device that is not in the same library as the volume required for restore, then the restore job will go into a state that is pending resource availability. The restore job does not fail.

The restore job will fail if the SE slot where the volume resides is not the `uselist` of the device specified in *devicename*. For more information about `uselist`, refer to its description in "[chdev](#) (page 2-30)".

Syntax

OB_RESTORE_DEVICE::=

```
OB_RESTORE_DEVICE[=]devicename
```

Semantics

devicename

Specifies the name of the tape device that the restore job is restricted to use.

For *devicename*, do not use the `device_name@hostname` or `@hostname` formats. You must specify only the device name.

For the complete description of *devicename*, see "[devicename](#) (page 4-12)".

For `OB_RESTORE_DEVICE`, *devicename* is restricted to tape devices.

Examples

Example C-13 Restore with Device Name Specified

This example restricts the restore job that restores the tablespace `my_tbs` to use the tape device `tape1`.

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE SBT;
  SEND 'OB_RESTORE_DEVICE=tape1';
  RESTORE TABLESPACE my_tbs;
  RECOVER TABLESPACE my_tbs;
}
```

D

Oracle Secure Backup Support for Extended Attributes and Access Control Lists

This appendix describes how Oracle Secure Backup backup and restore operations work with extended attributes and access control lists. It explains how to perform these operations by optionally saving or excluding extended attributes and access control lists.

This section contains the following topics:

- [Overview of Extended Attributes and Access Control Lists](#) (page D-1)
- [Supported Platforms](#) (page D-2)
- [Performing Backup and Recovery with Extended Attributes and Access Control Lists on Linux and Unix](#) (page D-3)

D.1 Overview of Extended Attributes and Access Control Lists

Oracle Secure Backup now enables you to perform backup and restore operations for files and directories associated with extended attributes and access control lists on UNIX like platforms. Oracle Secure Backup already supports this option on Windows platforms.

Extended attributes contain information associated with a file or directory defined in a name value format. These attributes may be associated to one particular application or the entire file system. Access control lists implement a finer grained permission model for files and directories on Unix like systems, which allows granting or denying access of a file or a directory to a specific set of users or groups.

In some cases, Oracle Secure Backup domains cannot read backup images containing extended attributes or access control lists. In such scenarios, Oracle Secure Backup gives you the option to perform the backup without saving the associated extended attributes and access control lists.



See Also:

["-A \(page B-18\)"](#) for more information on the `obtar` option.

D.2 Supported Platforms

Table D-1 (page D-2) lists the platforms that support Oracle Secure Backup backup and recovery operations with extended attributes and access control lists.

If you backup a file or directory on a platform that doesn't support extended attributes and access control lists, Oracle Secure Backup will continue to perform the backup operation without saving the associated extended attributes and access control lists.

Table D-1 Supporting Platforms for Extended Attributes and Access Control Lists

Platform	File System
Linux	ext2, ext3, JFS, XFS, ASM Cluster File System
Solaris	UFS, ASM Cluster File System, ZFS
AIX	JFS, GPFS, JFS2, VxFS
Windows	FAT, NTFS



Note:

On Linux platforms, Oracle Secure Backup supports any file system that implement POSIX access control lists interface.

Oracle Secure Backup does not perform cross-platform restore of extended attributes and access control lists as it may threaten security of the file. Ensure that you restore your backup consisting extended attributes and access control lists on the same platform version as the one used to perform the backup.

D.3 Requirements

To successfully backup and restore extended attributes and access control lists, keep the following points in mind:

- Oracle Automatic Storage Management cluster file system uses extended attributes to store tags associated with files and directories. It also supports access control lists. Ensure that Oracle Secure Backup is compatible with the cluster file system and its functions.
- While performing incremental backups, Oracle Secure Backup notes the `mtime` of each file being backed up. You can use `obtar` to change this setting to note the `ctime`, instead. The same setting is applied to extended attributes and access control lists.
- In any situation, if you don't want to save extended attributes and access control lists then you must use the `obtar -A` option while performing a backup. This option ignores the existing extended attributes and access control lists and proceeds to backup the file or directory without saving them.
- To save your extended attributes and access control lists, ensure that your [backupoptions](#) (page 7-33) policy is not set to the `obtar -A` option set.

 **See Also:**

- "[backup](#) (page 2-4)" for more information on how to use the `backup` command
- "[Changing Criteria for Incremental Backups](#) (page B-4)" for more information on how to change the `mtime` setting
- `-A` (page B-18) for more information on the `obtar -A` option

D.4 Security Practices

In some cases, a file may have been created first and an access control list applied at the restore stage. Such scenarios may lead to a security breach. It is recommended that you perform a restore by applying the access control list earlier.

You must also encrypt extended attributes and access control lists if they are not contained in the data being backed up, to eliminate unauthorized access.

D.5 Performing Backup and Recovery with Extended Attributes and Access Control Lists on Linux and Unix

This section lists the steps you must complete to successfully perform backup and recovery for files and directories with extended attributes and access control lists on UNIX like platforms.

To perform backup and recovery with extended attributes and access control lists:

1. Set up extended attributes and access control lists for the file or directory that you need to back up.
2. Create a dataset that includes the path to the file or directory that consists the extended attributes and access control lists.

 **See:**

"[mkds](#) (page 3-21)" for information on how to create a dataset

3. Create a disk pool, if required, to store the backup that you will be performing for this dataset.

 **See:**

"[mkdev](#) (page 3-6)" for information on how to create a disk pool

4. Backup the dataset you created, which consists the file or directory with its associated extended attributes and access control lists. Unless specified otherwise

by using the `obtar -A` command, the backup command will save the extended attributes and access control lists automatically.

 **See:**

"[backup](#) (page 2-4)" for information on how to perform a backup

"[-A](#) (page B-18)" for more information on the `obtar -A` option

5. Restore this data that you backed up on the same platform as the one on which the backup was performed.

 **See:**

"[restore](#) (page 3-99)" for information on how to restore data

6. Verify that your data has been restored successfully along with its extended attributes and access control lists by checking the restore log file.

E

Startup and Shutdown of Oracle Secure Backup Services

You can manually start or stop Oracle Secure Backup services by using the scripts shown in [Table E-1](#) (page E-1). The best practice is to stop Oracle Secure Backup when there are no active backup or restore jobs.

Table E-1 Oracle Secure Backup Service Shutdown and Startup

Operating System	Required Privileges	Startup and Shutdown Commands
Red Hat and Suse Linux	root	<code>/etc/init.d/observed stop</code> <code>/etc/init.d/observed start</code>
Solaris	root	<code>/lib/svc/method/observed stop</code> <code>/lib/svc/method/observed start</code>
AIX	root	<code>/etc/rc.d/init.d/observed stop</code> <code>/etc/rc.d/init.d/observed start</code>
HP-UX	root	<code>/sbin/init.d/observed stop</code> <code>/sbin/init.d/observed start</code>
Windows	Membership in Administrators group	<code>net stop observed</code> <code>net start observed</code>

Glossary

active location

A [location](#) in a [tape library](#) or [tape drive](#).

administrative domain

A group of computers on your network that you manage as a common unit to perform backup and restore operations. An administrative domain must include one and only one [administrative server](#). It can include the following:

- One or more [client](#) hosts
- One or more [media server](#) hosts

An administrative domain can consist of a single host that assumes the [roles](#) of administrative server, media server, and client.

administrative server

The host that stores configuration information and [catalog](#) files for hosts in the [administrative domain](#). There must be one and only one administrative server for each [administrative domain](#). One administrative server can service every [client](#) on your network. The administrative server runs the [scheduler](#), which starts and monitors backups within the administrative domain.

Apache Web server

A public-domain Web server used by the Oracle Secure Backup [Web tool](#).

attachment

The physical or logical connection (the path in which data travels) of a [tape device](#) to a host in the [administrative domain](#).

automated certificate provisioning mode

A mode of [certificate](#) management in which the [Certification Authority \(CA\)](#) signs and then transfers [identity certificates](#) to hosts over the network. This mode of issuing certificates is vulnerable to a possible, although extremely unlikely, man-in-the-middle attack. Automated mode contrasts with [manual certificate provisioning mode](#).

backup encryption

The process of obscuring backup data so that it is unusable unless decrypted. Data can be encrypted at rest, in transit, or both.

backup ID

An integer that uniquely identifies a [backup section](#).

backup image

The product of a [backup operation](#). A single backup image can span multiple volumes in a [volume set](#). The part of a backup image that fits on a single volume is called a [backup section](#).

backup image file

The logical container of a [backup image](#). A [backup image](#) consists of one file. One backup image consists of one or more [backup sections](#).

backup image label

The data on a tape that identifies file number, [backup section](#) number, and owner of the [backup image](#).

backup job

A backup that is eligible for execution by the Oracle Secure Backup [scheduler](#). A backup job contrasts with a [backup request](#), which is an [on-demand backup](#) that has not yet been forwarded to the scheduler with the `backup --go` command.

backup level

The level of an [incremental backup](#) of file-system data. Oracle Secure Backup supports 9 different incremental backup levels for a [file-system backup](#).

backup operation

A process by which data is copied from primary media to secondary media. You can use Oracle Secure Backup to make a [file-system backup](#), which is a backup of any file or files on the file system. You can also use the Oracle Secure Backup SBT library with [Recovery Manager \(RMAN\)](#) to back up the database to tape.

backup piece

A backup file generated by [Recovery Manager \(RMAN\)](#). Backup pieces are stored in a logical container called a backup set.

backup request

An [on-demand backup](#) that is held locally in [obtool](#) until you run the `backup` command with the `--go` option. At this point Oracle Secure Backup forwards the requests to the [scheduler](#), at which time each backup request becomes a [backup job](#) and is eligible to run.

backup schedule

A description of when and how often Oracle Secure Backup should back up the files specified by a [dataset](#). The backup schedule contains the names of each [dataset file](#) and the name of the [media family](#) to use. The part of the schedule called the [trigger](#) defines the days and times when the backups should occur. In [obtool](#), you create a backup schedule with the `mksched` command.

backup section

A portion of a [backup image file](#) that exists on a single tape. One backup image can contain one or more backup sections. Each backup section is uniquely identified by a [backup ID](#).

backup transcript

A file that contains the standard output from a particular backup dispatched by the Oracle Secure Backup [scheduler](#).

backup window

A time frame in which a [backup operation](#) can be processed.

barcode

A symbol code, also called a tag, that is physically applied to a [volume](#) for identification purposes. Oracle Secure Backup supports the use of tape libraries that have an automated means to read barcodes.

blocking factor

The number of 512-byte blocks to include in each block of data written to each [tape drive](#). By default, Oracle Secure Backup writes 64K blocks to tape, which is a blocking factor of 128. Because higher blocking factors usually result in better performance, you can try a blocking factor larger than the [obtar](#) default. If you pick a value larger than is supported by the operating system of the server, then Oracle Secure Backup fails with an error.

CA

See [Certification Authority \(CA\)](#)

catalog

A repository that records backups in an Oracle Secure Backup [administrative domain](#). You can use the Oracle Secure Backup [Web tool](#) or [obtool](#) to browse the catalog and determine what files you have backed up. The catalog is stored on the [administrative server](#).

certificate

A digitally signed statement from a [Certification Authority \(CA\)](#) stating that the [public key](#) (and possibly other information) of another entity has a value. The X.509 standard specifies the format of a certificate and the type of information contained in it: certificate version, serial number, algorithm ID, issuer, validity, subject, subject [public key](#) information, and extensions such as key usage (signing, encrypting, and so on). A variety of methods are used to encode, identify, and store the certificate.

Certification Authority (CA)

An authority in a network that performs the function of binding a [public key](#) pair to an identity. The CA certifies the binding by digitally signing a certificate that contains a representation of the identity and a corresponding [public key](#). The [administrative server](#) is the CA for an Oracle Secure Backup [administrative domain](#).

CIFS (Common Internet File System)

An Internet file-system protocol that runs on top of [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#).

class

A named set of [rights](#) for [Oracle Secure Backup users](#). A class can have multiple users, but each user can belong to one and only one class.

client

Any computer or server whose files Oracle Secure Backup backs up or restores.

content-managed expiration policy

A [volume](#) with this type of [expiration policy](#) expires when each [backup piece](#) on the volume is marked as deleted. You can make [Recovery Manager \(RMAN\) backups](#), but not [file-system backups](#), to content-managed volumes. You can use RMAN to delete backup pieces.

cumulative incremental backup

A type of [incremental backup](#) in which Oracle Secure Backup copies only data that has changed at a lower [backup level](#). For example, a level 3 incremental backup copies only that data that has changed since the most recent backup that is level 2 or lower.

daemons

Background processes that are assigned a task by Oracle Secure Backup during the execution of backup and restore operations. Some daemons run continually and others are started and stopped as required.

data management application (DMA)

An application that controls a backup or restore operation over the [Network Data Management Protocol \(NDMP\)](#) through connections to a [data service](#) and [tape service](#). The DMA is the session master, whereas the NDMP services are the slaves. In an Oracle Secure Backup [administrative domain](#), [obtar](#) is an example of a DMA.

data service

An application that runs on a client and provides [Network Data Management Protocol \(NDMP\)](#) access to database and file-system data on the primary storage system.

data transfer element (DTE)

A secondary storage device within a [tape library](#). In libraries that contain multiple tape drives, DTEs are sequentially numbered starting with 1.

database backup storage selector

An Oracle Secure Backup configuration object that specifies characteristics of [Recovery Manager \(RMAN\) SBT backups](#). The storage selector act as a layer between RMAN, which accesses the database, and the Oracle Secure Backup software, which manages the backup media.

database ID (DBID)

An internal, uniquely generated number that differentiates databases. Oracle creates this number automatically when you create the database.

dataset

The contents of a [file-system backup](#). A [dataset file](#) describes dataset. For example, you could create the dataset file `my_data.ds` to describe a dataset that includes the `/home` directory on host `brhost2`.

dataset directory

A directory that contains dataset files. The directory groups dataset files as a set for common reference.

dataset file

A text file that describes a [dataset](#). The Oracle Secure Backup dataset language provides a text-based means to define file-system data to back up.

defaults and policies

A set of configuration data that specifies how Oracle Secure Backup runs in an [administrative domain](#).

device discovery

The process by which Oracle Secure Backup automatically detects devices accessed through [Network Data Management Protocol \(NDMP\)](#) and configuration changes for such devices.

device special file

A file name in the `/dev` file system on UNIX or Linux that represents a hardware [tape device](#). A device special file does not specify data on disk, but identifies a hardware unit and the device driver that handles it. The inode of the file contains the device number, permissions, and ownership data. An [attachment](#) consists of a host name and the device special file name by which that device is accessed by Oracle Secure Backup.

differential incremental backup

A type of [incremental backup](#) in which Oracle Secure Backup copies only data that has changed at the same or lower [backup level](#). This backup is also called a level 10 backup. Oracle Secure Backup does not support the level 10 backup on some platforms, including [Network Attached Storage \(NAS\)](#) devices such as a Network Appliance [filer](#).

disk pool orphans

Backup files that do not have corresponding entries in the disk pool catalog. These arise when a disk pool imported in a domain is not cataloged. In this scenario, the automatic disk-pool clean-up sees uncataloged backup files as orphans and deletes them.

DMA

See [data management application \(DMA\)](#)

domain

A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

error rate

The number of recovered write errors divided by the total blocks written, multiplied by 100.

exclusion statement

Specifies a file or path to be excluded from a [backup operation](#).

expiration policy

The means by which Oracle Secure Backup determines how volumes in a [media family](#) expire, that is, when they are eligible to be overwritten. A media family can either have a [content-managed expiration policy](#) or [time-managed expiration policy](#).

Fiber Distributed Data Interface (FDDI)

A set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps. FDDI networks are typically used as backbones for wide-area networks.

Fibre Channel

A protocol used primarily among devices in a [Storage Area Network \(SAN\)](#).

file-system backup

A backup of files on the file system initiated by Oracle Secure Backup. A file-system backup is distinct from a [Recovery Manager \(RMAN\)](#) backup made through the Oracle Secure Backup [SBT interface](#).

filer

A network-attached appliance that is used for data storage.

firewall

A system designed to prevent unauthorized access to or from a private network.

full backup

An operation that backs up all of the files selected on a [client](#). Unlike in an [incremental backup](#), files are backed up whether they have changed since the last backup or not.

identity certificate

An X.509 [certificate](#) signed by the [Certification Authority \(CA\)](#) that uniquely identifies a host in an Oracle Secure Backup [administrative domain](#).

incremental backup

An operation that backs up only the files on a [client](#) that changed after a previous backup. Oracle Secure Backup supports 9 different incremental [backup levels](#) for file-system backups. A [cumulative incremental backup](#) copies only data that changed since the most recent backup at a lower level. A [differential incremental backup](#), which is equivalent to a level 10 backup, copies data that changed since an incremental backup at the same or lower level.

An incremental backup contrasts with a [full backup](#), which always backs up all files regardless of when they last changed. A full backup is equivalent to an incremental backup at level 0.

job list

A catalog created and maintained by Oracle Secure Backup that describes past, current, and pending [backup jobs](#).

job summary

A text file report produced by Oracle Secure Backup that describes the status of selected backup and restore jobs. Oracle Secure Backup generates the report according to a user-specified [job summary schedule](#).

job summary schedule

A user-defined schedule for generating job summaries. You create job summary schedules with the `mksum` command in [obtool](#).

location

A location is a place where a [volume](#) physically resides; it can be the name of a [tape library](#), a data center, or an offsite storage facility.

manual certificate provisioning mode

A mode of certificate management in which you must manually export the signed [identity certificate](#) for a host from the [administrative server](#), transfer it to the host, and manually import the certificate into the [wallet](#) of the host. Unlike [automated certificate provisioning mode](#), this mode is not vulnerable to a possible (if extremely unlikely) man-in-the-middle attack.

media family

A named classification of backup volumes that share the same [volume sequence file](#), [expiration policy](#), and [write window](#).

media server

A computer or server that has at least one [tape device](#) connected to it. A media server is responsible for transferring data to or from the tape devices that are attached to it.

mount mode

The mode indicates the way in which Oracle Secure Backup can use a [volume](#) physically loaded into a [tape drive](#). Valid values are read-only, write/append, overwrite, and not mounted.

NAS

See [Network Attached Storage \(NAS\)](#)

native access mode

A synonym for [primary access mode](#).

NDMP

See [Network Data Management Protocol \(NDMP\)](#)

NDMP access mode

The mode of access for a [filer](#) or other host that uses [Network Data Management Protocol \(NDMP\)](#) for communications within the [administrative domain](#). NDMP access mode contrasts with [primary access mode](#), which uses the Oracle Secure Backup network protocol. Note that Oracle Secure Backup uses NDMP for data transfer among hosts regardless of whether a host is accessed through the primary or NDMP access modes.

Network Attached Storage (NAS)

A NAS server is a computer on a network that hosts file systems. The server exposes the file systems to its clients through one or more standard protocols, most commonly [Network File System \(NFS\)](#) and [CIFS \(Common Internet File System\)](#).

Network Data Management Protocol (NDMP)

An open standard protocol that defines a common architecture for backups of heterogeneous file servers on a network. This protocol allows the creation of a common agent used by the central backup application, called a [data management application \(DMA\)](#), to back up servers running different operating systems. With NDMP, network congestion is minimized because the data path and control path are separated. Backup can occur locally—from file servers direct to tape drives—while management can occur centrally.

Network File System (NFS)

A client/server application that gives all network users access to shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#). Users can manipulate shared files as if they were stored on local disk. With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

NT File System (NTFS)

One of the file systems for the Windows operating system. NTFS has features to improve reliability, such as transaction logs to help restore from disk failures.

OB access mode

A synonym for [primary access mode](#).

obfuscated wallet

A [wallet](#) whose data is scrambled into a form that is extremely difficult to read if the scrambling algorithm is unknown. The wallet is read-only and is not protected by a password. An obfuscated wallet supports single sign-on (SSO).

object

An instance configuration data managed by Oracle Secure Backup: [class](#), [Oracle Secure Backup user](#), [host](#), [tape device](#), [tape library](#), [backup schedule](#), and so on. Objects are stored as files in subdirectories of `admin/config` in the [Oracle Secure Backup home](#).

obtar

The underlying engine of Oracle Secure Backup that moves data to and from tape. [obtar](#) is a descendent of the original Berkeley UNIX `tar(2)` command. Although [obtar](#) is typically not accessed directly, you can use it to back up and restore files or directories specified on the command line. [obtar](#) enables the use of features not exposed through [obtool](#) or the [Web tool](#).

obtool

The principal command-line interface to Oracle Secure Backup. You can use this tool to perform all Oracle Secure Backup configuration, backup and restore, maintenance, and monitoring operations. The [obtool](#) utility is an alternative to the [Web tool](#).

obdup

The underlying engine of Oracle Secure Backup that moves data during backup image copy operations.

off-site backup

A backup that is equivalent to a [full backup](#) except that it does not affect the full/incremental [backup schedule](#). An off-site backup is useful when you want to create an backup image for off-site storage without disturbing your [incremental backup](#) schedule.

on-demand backup

A file-system backup initiated through the `backup` command in [obtool](#) or the Oracle Secure Backup [Web tool](#). The backup is one-time-only and either runs immediately or at a specified time in the future. An on-demand backup contrasts with a [scheduled backup](#), which is initiated by the Oracle Secure Backup [scheduler](#).

operator

A person whose duties include [backup operation](#), [backup schedule](#) management, tape swaps, and error checking.

operator host

When using [obtar](#), this is the host on which you run the obtar command.

Oracle Secure Backup home

The directory in which the Oracle Secure Backup software is installed. The Oracle Secure Backup home is typically `/usr/local/oracle/backup` on UNIX/Linux and `c:\Program Files\Oracle\Backup` on Windows. This directory contains binaries and configuration files. The contents of the directory differ depending on which role is assigned to the host within the [administrative domain](#).

Oracle Secure Backup logical unit number

A number between 0 and 31 used to generate unique [device special file](#) names during device configuration (for example: `/dev/obt0`, `/dev/obt1`, and so on). Although it is not a requirement, unit numbers typically start at 0 and increment for each additional [tape device](#) of a given type, whether [tape library](#) or [tape drive](#).

The Oracle Secure Backup logical unit number should not be confused with the [SCSI LUN](#). The SCSI LUN is part of the hardware address of the device, whereas the Oracle Secure Backup logical unit number is part of the name of the device special file.

Oracle Secure Backup-style wildcard syntax

A set of [wildcard](#) characters used in searches on UNIX and Linux operating systems. The asterisk symbol (*) represents any string of 0 or more characters. The question mark symbol (?) represents any single character. Brackets ([]) define a character class for a single character. A backslash (\) escapes any of the previous special characters. Use \\ to match a backslash.

Oracle Secure Backup user

A defined account within an Oracle Secure Backup [administrative domain](#). Oracle Secure Backup users exist in a separate namespace from operating system users.

Oracle Secure Backup wildcard pattern matching

A technique used on UNIX-based and Linux-based operating systems to filter output using a set of wildcard character patterns, while browsing the backup catalog through the Oracle Secure Backup [obtool](#).

original volume

The [volume](#) from which a duplicate is made.

originating location

A [location](#) where a [volume](#) was first written.

overwrite

The process of replacing a file on your system by restoring a file that has the same file name.

password grace time

The length of time, after an [Oracle Secure Backup user's](#) password has expired, during which the user is allowed to log in without changing the password.

password lifetime

The length of time, measured in number of days, for which an [Oracle Secure Backup user's](#) password is valid.

password reuse time

The length of time which must elapse before a previously-used [Oracle Secure Backup user's](#) password may be reused.

PNI (Preferred Network Interface)

The network interface that is necessary to transmit data to be backed up or restored. A network can have multiple physical connections between a [client](#) and the server performing a backup or restore on behalf of that client. For example, a network can have both Ethernet and [Fiber Distributed Data Interface \(FDDI\)](#) connections between a pair of hosts. PNI enables you to specify, on a client-by-client basis, which of the server's network interfaces is necessary.

preauthorization

An optional attribute of an Oracle Secure Backup user. A preauthorization gives an operating system user access to specified Oracle Secure Backup resources.

primary access mode

The mode of access for a host that uses the Oracle Secure Backup network protocol for communications within the [administrative domain](#). Oracle Secure Backup must be installed on hosts that use primary access mode. In contrast, hosts that use [NDMP access mode](#) do not require Oracle Secure Backup to be installed. Note that Oracle Secure Backup uses [Network Data Management Protocol \(NDMP\)](#) for data transfer among hosts regardless of whether a host is accessed through the primary or NDMP access modes.

private key

A number that corresponds to a specific [public key](#) and is known only to the owner. Private and public keys exist in pairs in all public key cryptography systems. In a typical public key cryptosystem, such as RSA, a private key corresponds to exactly one public key. You can use private keys to compute signatures and decrypt data.

privileged backup

File-system [backup operations](#) initiated with the `--privileged` option of the `backup` command. On UNIX and Linux systems, a privileged backup runs under the `root` user

identity. On Windows systems, the backup runs under the same account (usually `Local System`) as the Oracle Secure Backup service on the Windows [client](#).

public key

A number associated with a particular entity intended to be known by everyone who must have trusted interactions with this entity. A public key, which is used with a corresponding [private key](#), can encrypt communication and verify signatures.

restore operation

Copies files from the [volumes](#) in a [tape device](#) to the designated system.

retention period

The length of time that data in a [volume set](#) is not eligible to be overwritten. The retention period is an attribute of a time-managed [media family](#). The retention period begins at the [write window close time](#). For example, if the [write window](#) for a media family is 7 days, then a retention period of 14 days indicates that the data is eligible to be overwritten 21 days from the first write to the first [volume](#) in the volume set.

Recovery Manager (RMAN)

A utility supplied with Oracle Database used for database backup, restore, and recovery. RMAN is a separate application from Oracle Secure Backup. Unlike RMAN, you can use Oracle Secure Backup to back up any file on the file system—not just database files. Oracle Secure Backup includes an [SBT interface](#) that RMAN can use to back up database files directly to tape.

rights

Privileges within the [administrative domain](#) that are assigned to a [class](#). For example, the `perform backup as self` right is assigned to the `operator` class by default. Every [Oracle Secure Backup user](#) that belongs to a class is granted the rights associated with this class.

roles

The functions that hosts in your network can have during backup and restore operations. There are three roles in Oracle Secure Backup: [administrative server](#), [media server](#), and [client](#). A host in your network can serve in any of these roles or any combination of them. For example, the [administrative server](#) can also be a [client](#) and media server.

rotation policy

A rotation policy defines the physical management of backup media throughout the media life cycle. It determines in what sequence and at which times each [volume](#) moves from the initial [active location](#) where it is written, through another [location](#), and so on, until it is reused.

SAN

See [Storage Area Network \(SAN\)](#)

SBT interface

A media management software library that [Recovery Manager \(RMAN\)](#) can use to back up to tertiary storage. An SBT interface conforms to a published API and is supplied by a media management vendor. Oracle Secure Backup includes an SBT interface for use with RMAN.

schedule

A user-defined time period for running [scheduled backup](#) operations. File-system backups are triggered by a schedule, which you can create with the `mksched` command in [obtool](#). In contrast, [on-demand backups](#) are one-time-only backups created with the `backup` command.

scheduled backup

A file-system backup that is scheduled through the `mksched` command in [obtool](#) or the Oracle Secure Backup [Web tool](#) (or is modified by the `runjob` command). A backup [schedule](#) describes which files should be backed up. A [trigger](#) defined in the schedule specifies when the [backup job](#) should run.

scheduler

A daemon (obscheduled) that runs on an [administrative server](#) and is responsible for managing all backup scheduling activities. The scheduler maintains a [job list](#) of [backup jobs](#) scheduled for execution.

service daemon

A daemon (observed) that runs on each host in the [administrative domain](#) that communicates through [primary access mode](#). The service daemon provides a wide variety of services, including [certificate](#) operations.

SCSI

See [Small Computer System Interface \(SCSI\)](#)

SCSI LUN

Logical unit number of a [Small Computer System Interface \(SCSI\) tape device](#). Logical unit numbers make it possible for several tape devices to share a single SCSI ID. Do not confuse with [Oracle Secure Backup logical unit number](#).

Secure Sockets Layer (SSL)

A cryptographic protocol that provides secure network communication. SSL provides endpoint authentication through a [certificate](#). Data transmitted over SSL is protected from eavesdropping, tampering or message forgery, and replay attacks.

Small Computer System Interface (SCSI)

A parallel I/O bus and protocol that permits the connection of a variety of peripherals to host computers. Connection to the SCSI bus is achieved through a host adapter and a peripheral controller.

snapshot

A consistent copy of a [volume](#) or a file system. Snapshots are supported only for Network Appliance filers running Data ONTAP 6.4 or later.

SSL

See [Secure Sockets Layer \(SSL\)](#)

Storage Area Network (SAN)

A high-speed subnetwork of shared storage devices. A SAN is designed to assign data backup and restore functions to a secondary network where so that they do not interfere with the functions and capabilities of the server.

storage elements

Physical locations with a [tape library](#) where a [volume](#) can be stored and retrieved by the library's robotic arm.

storage location

A [location](#) outside of a [tape library](#) or [tape drive](#) where a [volume](#) can be stored.

super-directory

A fictitious directory displayed when browsing file-system backups, that contains all files and directories saved from the top-most file-system level.

tape device

A [tape drive](#) or [tape library](#) identified by a user-defined device name.

tape drive

A [tape device](#) that reads and writes data stored on a tape. Tape drives are sequential-access, which means that they must read all preceding data to read any particular piece of data. Tape drives are accessible through various protocols, including [Small Computer System Interface \(SCSI\)](#) and [Fibre Channel](#). A tape drive can exist standalone or in a [tape library](#).

tape library

A medium changer that accepts [Small Computer System Interface \(SCSI\)](#) commands to move a [volume](#) between [storage elements](#) and a [tape drive](#).

tape service

A [Network Data Management Protocol \(NDMP\)](#) service that transfers data to and from secondary storage and allows the [data management application \(DMA\)](#) to manipulate and access secondary storage.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The suite of protocols used to connect hosts for transmitting data over networks.

time-managed expiration policy

A [media family expiration policy](#) in which every [volume](#) in a [volume set](#) can be overwritten when they reach their [volume expiration time](#). Oracle Secure Backup

computes the volume expiration time by adding the [volume creation time](#) for the first volume in the set, the [write window time](#), and the [retention period](#).

For example, you set the [write window](#) for a media family to 7 days and the retention period to 14 days. Assume that Oracle Secure Backup first wrote to the first volume in the set on January 1 at noon and subsequently wrote data on 20 more volumes in the set. In this scenario, all 21 volumes in the set expire on January 22 at noon.

You can make [Recovery Manager \(RMAN\)](#) backups or [file-system backups](#) to volumes that use a time-managed expiration policy.

trigger

The part of a [backup schedule](#) that specifies the days and times at which the backups should occur.

Universal Unique Identifier (UUID)

An identifier used for tagging objects across an Oracle Secure Backup [administrative domain](#).

UNIX-style wildcard syntax

A set of [wildcard](#) characters used in searches on UNIX and Linux operating systems. The asterisk symbol (*) represents any string of 0 or more characters. The question mark symbol (?) represents any single character. Brackets ([]) define a character class for a single character. A backslash (\) escapes any of the previous special characters. Use \\ to match a backslash.

unprivileged backup

File-system backups created with the `--unprivileged` option of the `backup` command. When you create or modify an [Oracle Secure Backup user](#), you associate operating system accounts with this user. Unprivileged backups of a host run under the operating system account associated with Oracle Secure Backup user who initiates the backup.

volume

A volume is a unit of media, such as an 8mm tape. A volume can contain multiple backup images.

volume creation time

The time at which Oracle Secure Backup wrote [backup image file](#) number 1 to a [volume](#).

volume expiration time

The date and time on which a volume in a [volume set](#) expires. Oracle Secure Backup computes this time by adding the [write window](#) duration, if any, to the [volume creation time](#) for the first volume in the set, then adding the volume [retention period](#).

For example, assume that a volume set belongs to a [media family](#) with a retention period of 14 days and a write window of 7 days. Assume that the [volume creation time](#) for the first volume in the set was January 1 at noon and that Oracle Secure Backup

subsequently wrote data on 20 more volumes in the set. In this scenario, the volume expiration time for all 21 volumes in the set is January 22 at noon.

volume ID

A unique alphanumeric identifier assigned by Oracle Secure Backup to a [volume](#) when it was labeled. The volume ID usually includes the [media family](#) name of the volume, a dash, and a unique [volume sequence number](#). For example, a volume ID in the `RMAN-DEFAULT` media family could be `RMAN-DEFAULT-000002`.

volume label

The first block of the first [backup image](#) on a volume. It contains the [volume ID](#), the owner's name, the [volume creation time](#), and other information.

volume sequence file

A file that contains a unique [volume ID](#) to assign when labeling a [volume](#).

volume sequence number

A number recorded in the [volume label](#) that indicates the [volume](#) order in a [volume set](#). The first volume in a set has sequence number 1. The [volume ID](#) for a volume usually includes the [media family](#) name of the volume, a dash, and a unique volume sequence number. For example, a volume ID for a volume in the `RMAN-DEFAULT` media family could be `RMAN-DEFAULT-000002`.

volume set

A group of [volumes](#) spanned by a [backup image](#). The part of the backup image that fits on a single volume is a [backup section](#).

volume tag

A field that is commonly used to hold the [barcode](#) identifier, also called a volume tag, for the [volume](#). The volume tag is found in the [volume label](#).

wallet

A password-protected encrypted file. An Oracle wallet is primarily designed to store a X.509 [certificate](#) and its associated [public key/private key](#) pair. The contents of the wallet are only available after the wallet password has been supplied, although with an [obfuscated wallet](#) no password is required.

Web tool

The browser-based GUI that enables you to configure an [administrative domain](#), manage backup and restore operations, and browse the backup [catalog](#).

wildcard

A wildcard is a character that can represent many other characters. For example, the asterisk symbol (*) is almost universally used to mean "any".

write date

Defines the period, starting from the [volume creation time](#), during which updates to a [volume](#) are allowed.

write-protect

To mark a file or media so that its contents cannot be modified or deleted. To write-protect a [volume](#), you can mount a volume read-only in Oracle Secure Backup or alter the physical media with a write-protect tab.

write window

The period for which a [volume set](#) remains open for updates, usually by appending an additional [backup image](#). The write window opens at the [volume creation time](#) for the first [volume](#) in the set and closes after the write window period has elapsed. After the [write window close time](#), Oracle Secure Backup does not allow further updates to the volume set until it expires (as determined by its [expiration policy](#)), or until it is relabeled, reused, unlabeled, or forcibly overwritten.

A write window is associated with a [media family](#). All volume sets that are members of the media family remain open for updates for the same time period.

write window close time

The date and time that a [volume set](#) closes for updates. Oracle Secure Backup computes this time when it writes [backup image file](#) number 1 to the first [volume](#) in the set. If a volume set has a [write window close time](#), then this information is located in the volume section of the [volume label](#).

write window time

The length of time during which writing to a [volume set](#) is permitted.

Index

Symbols

- c mode, of obtar, [B-6](#)
- t mode, of obtar, [B-11](#)
- x mode, of obtar, [B-8](#)
- zz mode, of obtar, [B-14](#)
- .obtoolrc
 - location, [1-3](#)

A

- access Oracle backups right, [8-3](#)
- ACSLS
 - maxacsejectwaittime policy, [7-16](#)
- ACSLS tape drives
 - configuring, [3-15](#)
- ACSLS tape libraries
 - associating symbolic name with CAP, [3-16](#)
 - configuring, [3-15](#)
- adding
 - backup windows, [2-1](#)
 - duplication windows, [2-2](#)
 - file-system backup request, [2-4](#)
 - hosts, [3-26](#)
 - name/value pair to policy, [2-3](#)
- admin class, [8-1](#), [8-2](#)
- adminlogevents policy, [7-22](#)
- adminlogfile policy, [7-22](#)
- after backup statement, [6-5](#)
- algorithm policy, [7-3](#)
- Apache Web server
 - webautostart policy, [7-11](#)
 - webpass policy, [7-12](#)
- applybackupsfrequency policy, [7-40](#)
- asciindexrepository policy, [7-19](#)
- aspec placeholder, [4-1](#)
- assistance
 - responding to job request for, [3-137](#)
- attachments
 - placeholder, [4-1](#)
 - testing, [3-73](#)
- attributes
 - changing for host, [2-43](#)
 - changing for media families, [2-52](#)
 - changing for tape devices, [2-30](#)

- attributes (*continued*)
 - changing for user classes, [2-28](#)
 - changing for users, [2-72](#)
 - changing for volumes, [2-75](#)
 - listing for checkpoints, [2-126](#)
 - listing for devices, [2-133](#)
 - listing for hosts, [2-143](#)
 - listing for media families, [2-156](#)
 - listing for user classes, [2-128](#)
- auditlogins policy, [7-10](#)
- authenticationtype policy, [7-28](#)
- authtype placeholder, [4-3](#)
- autocertissue policy, [7-42](#)
- autohistory policy, [7-32](#)
- autoindex policy, [7-19](#)
- autolabel policy, [7-32](#)
- automaticreleaseofrecalledvolumes policy, [7-49](#)
- autorunmmjobs policy, [7-47](#)
- autovolumerelease policy, [7-48](#)

B

- backup
 - priority placeholders, [4-26](#)
- backup commands
 - about, [1-10](#)
 - backup, [2-4](#)
 - lsbackup, [2-117](#)
 - rmbbackup, [3-108](#)
- backup compression policies
 - about, [7-1](#)
 - buffersize, [7-2](#)
 - excludeformats, [7-3](#)
 - option, [7-2](#)
- backup encryption policies
 - about, [7-3](#)
 - algorithm, [7-3](#)
 - encryption, [7-4–7-6](#)
 - keytype, [7-5](#)
 - rekeyfrequency, [7-6](#)
- backup image instance commands
 - about, [1-11](#)
- backup image instances
 - listing, [2-146](#)
 - modifying, [2-47](#)

- backup images
 - autolabel policy, [7-32](#)
 - catalog identifier placeholder, [4-21](#)
 - creating with obtar -c, [B-6](#)
 - displaying contents of, [2-25](#)
 - extracting files from with obtar -x, [B-8](#)
 - filenumber placeholders, [4-16](#)
 - listing, [2-114](#), [2-119](#)
 - listing with obtar -t, [B-11](#)
 - names, [2-8](#)
 - renaming, [3-81](#)
 - using tar with obtar, [B-2](#)
 - backup jobs
 - listing, [2-149](#)
 - backup levels
 - level variable, [5-3](#)
 - maxlevel variable, [5-3](#)
 - backup piece commands
 - about, [1-11](#)
 - lspiece, [2-160](#)
 - rpmiece, [3-123](#)
 - backup pieces
 - catalog identifier placeholder, [4-21](#)
 - listing, [2-160](#)
 - removing, [3-123](#)
 - backup requests
 - listing, [2-117](#)
 - removing, [3-108](#)
 - backup schedules
 - creating, [3-44](#)
 - listing, [2-167](#)
 - removing, [3-128](#)
 - backup sections
 - backupimagerechecklevel policy, [7-32](#)
 - listing, [2-170](#)
 - removing, [3-129](#)
 - undoing remove, [3-151](#)
 - backup window commands
 - about, [1-11](#)
 - addbw, [2-1](#)
 - chkbw, [2-48](#)
 - lsbw, [2-125](#)
 - rmbw, [3-110](#)
 - setbw, [3-140](#)
 - backup windows
 - adding, [2-1](#)
 - changing settings, [3-140](#)
 - checking for, [2-48](#)
 - listing, [2-125](#)
 - removing, [3-110](#)
 - backup-container placeholder, [4-4](#)
 - backup-level placeholder, [4-4](#)
 - backupev policy, [7-28](#)
 - backupimagerechecklevel policy, [7-32](#)
 - backuptype policy, [7-32](#)
 - backuptype policy, [7-28](#)
 - backuptype policy, [7-29](#)
 - backups
 - listing cataloged backups, [2-122](#)
 - barcodesrequired policy, [7-25](#)
 - barcodes
 - barcodesrequired policy, [7-25](#)
 - batch mode
 - running obtool commands in, [1-5](#)
 - before backup statement, [6-6](#)
 - blocking factor
 - blockingfactor policy, [7-25](#)
 - maxblockingfactor policy, [7-26](#)
 - blockingfactor policy, [7-25](#)
 - browse backup catalogs with this access right, [8-3](#)
 - browsemode variable, [5-1](#)
 - browser commands
 - about, [1-12](#)
 - cd, [2-25](#)
 - ls, [2-114](#)
 - lsbu, [2-122](#)
 - pwd, [3-76](#)
 - buffersize policy, [7-2](#)
- ## C
-
- cancelling
 - jobs, [2-14](#)
 - catalog
 - asciindexrepository policy, [7-19](#)
 - autoindex policy, [7-19](#)
 - browsemode variable, [5-1](#)
 - changing directory, [2-25](#)
 - data-selector placeholders, [4-6](#)
 - displaying current directory, [3-76](#)
 - earliestindexcleanup policy, [7-19](#)
 - generatendmpindexdata policy, [7-20](#)
 - importing information from tape, [2-15–2-17](#), [4-19](#)
 - include catalog dataset statement, [6-15](#)
 - indexcleanupfrequency policy, [7-20](#)
 - latestindexcleanup policy, [7-20](#)
 - listing backups, [2-122](#)
 - listing contents, [2-114](#)
 - listing contents with obcleanup, [A-3](#)
 - listing volumes, [2-182](#)
 - maxindexbuffer policy, [7-20](#)
 - obixdmaxupdaters policy, [7-10](#)
 - obixdrechecklevel policy, [7-11](#)
 - removing unneeded records with obcleanup, [A-3](#)
 - saveasciindexfiles policy, [7-21](#)
 - updating manually, [3-129](#)
 - viewmode variable, [5-5](#)
 - certificates

- certificates (*continued*)
 - autocertissue policy, 7-42
- certkeysize policy, 7-43
- changing
 - backup window settings, 3-140
 - duplication policies, 2-41
- checkpoint commands
 - about, 1-12
 - lscheckpoint, 2-126
 - rmcheckpoint, 3-110
- checkpoints
 - fullbackupcheckpointfrequency policy, 7-34
 - incrbackupcheckpointfrequency policy, 7-34
 - listing, 2-126
 - maxcheckpointrestarts policy, 7-36
 - removing, 3-110
 - restartablebackups policy, 7-36
- class commands
 - about, 1-13
 - chclass, 2-28
 - lsclass, 2-128
 - mkclass, 3-2
 - renclass, 3-83
 - rmclass, 3-111
- class rights
 - access Oracle backups, 8-3
 - browse backup catalogs with this access, 8-3
 - display administrative domain's configuration, 8-4
 - list any backup, regardless of its owner, 8-4
 - list any backups owned by user, 8-4
 - list any job, regardless of its owner, 8-5
 - list any jobs owned by user, 8-5
 - manage devices and change device state, 8-5
 - modify administrative domain's configuration, 8-4
 - modify any backup, regardless of its owner, 8-5
 - modify any backups owned by user, 8-5
 - modify any job, regardless of its owner, 8-5
 - modify any jobs owned by user, 8-5
 - modify own name and password, 8-6
 - perform backups as privileged user, 8-6
 - perform backups as self, 8-6
 - perform Oracle backups and restores, 8-6
 - perform restores as privileged user, 8-6
 - perform restores as self, 8-7
 - query and display information about devices, 8-7
 - receive email describing expired passphrase keys, 8-7
 - receive email describing internal errors, 8-7
 - receive email requesting operator assistance, 8-7
- classes
 - admin class, 8-1, 8-2
 - operator class, 8-1, 8-2
 - oracle class, 8-1, 8-2
 - reader class, 8-1, 8-2
 - user class, 8-1, 8-2
- cleaning
 - tape drives, 2-79
- clientlogevents policy, 7-23
- cloud storage device policies
 - about, 7-8
 - proxyserver, 7-8
 - proxyuser, 7-8
 - segmentsize, 7-9
 - streamsperjob, 7-9
 - transfertimeout, 7-9
 - usepersistentcon, 7-9
- cloud storage devices
 - configuring, 3-16
 - deleting expired backups, 3-1
 - managing, 3-1
 - removing backup image instances, 3-118
 - restriction placeholders, 4-25
- cloud storage device policies
 - proxypassword, 7-9
- compression
 - hardware, B-22
 - of on-demand backup jobs, 2-4
 - software, 2-4
 - with obtar, B-8, B-14
- concjobs placeholder, 4-5
- configuring
 - ACSLs tape drives, 3-15
 - ACSLs tape libraries, 3-15
 - cloud storage devices, 3-16
 - devices, 3-6
 - disk pools, 3-12
 - tape drives, 3-7
 - tape libraries, 3-10
- content placeholder, 4-5
- content-managed expiration policies, 3-36
- controlling
 - daemons, 2-83
 - job processing, 3-138
- copy instance policies
 - defaultjobpriority, 7-7
 - encryption, 7-7
 - obdoptions, 7-8
- creating
 - database backup storage selectors, 3-54
 - dataset directories, 3-21
 - dataset files, 3-21
 - file-system restore requests, 3-99
 - job summary schedules, 3-61
 - locations, 3-34

creating (*continued*)

- media families, [3-36](#)
- rotation policies, [3-42](#)
- schedules, [3-44](#)
- snapshots, [3-53](#)
- users, [3-64](#)
- volume duplication policies, [3-24](#)

cross all mountpoints statements, [6-7](#)

cross local mountpoints statement, [6-8](#)

cross remote mountpoints statement, [6-9](#)

customeridstring policy, [7-49](#)

D

daemon commands

- about, [1-13](#)
- ctldaemon, [2-83](#)
- lsdaemon, [2-131](#)

daemon policies, [7-9](#)

- auditlogins, [7-10](#)
- obixdmaxupdaters, [7-10](#)
- obixdrechecklevel, [7-11](#)
- obixdupdaternicevalue, [7-11](#)
- webautostart, [7-11](#)
- webpass, [7-12](#)
- windowscontrolcertificatesservice, [7-13](#)

daemons

- controlling, [2-83](#)
- listing, [2-131](#)

Data ONTAP operating system, [3-53](#)

data transfer elements, [2-183](#)

data-selector placeholder, [4-6](#)

database backup storage selector commands

- about, [1-14](#)
- chssel, [2-65](#)
- lsssel, [2-175](#)
- mkssel, [3-54](#)
- renssel, [3-93](#)
- rmssel, [3-132](#)

database backup storage selectors

- changing, [2-65](#)
- content placeholders, [4-5](#)
- creating, [3-54](#)
- listing, [2-175](#)
- removing, [3-132](#)
- renaming, [3-93](#)

dataset

- change directory, [2-26](#)
- checking syntax, [2-49](#)
- listing contents, [2-19](#)

dataset commands

- about, [1-14](#)
- catds, [2-19](#)
- cdds, [2-26](#)
- chkds, [2-49](#)

dataset commands (*continued*)

- edds, [2-92](#)
- lsds, [2-139](#)
- mkds, [3-21](#)
- pwdds, [3-77](#)
- rends, [3-85](#)
- rmds, [3-114](#)

dataset directories

- creating, [3-21](#)
- displaying current directory, [3-77](#)
- listing names, [2-139](#)
- name placeholders, [4-7](#)
- removing, [3-114](#)
- renaming, [3-85](#)

dataset files

- creating, [3-21](#)
- editing, [2-92](#)
- examples, [6-2](#)
- listing names, [2-139](#)
- name placeholders, [4-7](#)
- removing, [3-114](#)
- renaming, [3-85](#)

dataset language

- nested block, [6-1](#)
- overview, [6-1](#)

dataset statements

- about, [6-4](#)
- after backup, [6-5](#)
- backward compatibility, [6-4](#)
- before backup, [6-6](#)
- cross all mountpoints, [6-7](#)
- cross local mountpoints, [6-8](#)
- cross remote mountpoints, [6-9](#)
- exclude dir, [6-10](#)
- exclude file, [6-11](#)
- exclude name, [6-11](#)
- exclude oracle database files, [6-13](#)
- exclude path, [6-14](#)
- include catalog, [6-15](#)
- include dataset, [6-16](#)
- include host, [6-16](#)
- include path, [6-17](#)
- wildcards, [6-4](#)

dataset-dir-name placeholder, [4-7](#)

dataset-file-name placeholder, [4-7](#)

dataset-name placeholder, [4-8](#)

date

- obtool format, [1-7](#)

date-range placeholder, [4-8](#)

date-time placeholder, [4-9](#)

date/time

- obtool format, [1-7](#)

day-date placeholder, [4-9](#)

day-specifier placeholder, [4-12](#)

defaultjobpriority policy, [7-7](#)

defaults and policies

- about, [7-1](#)
- adminlogevents, [7-22](#)
- adminlogfile, [7-22](#)
- algorithm, [7-3](#)
- applybackupsfrequency, [7-40](#)
- asciiindexrepository, [7-19](#)
- auditlogins, [7-10](#)
- authenticationtype, [7-28](#)
- autocertissue, [7-42](#)
- autohistory, [7-32](#)
- autoindex, [7-19](#)
- autolabel, [7-32](#)
- autorunmmjobs, [7-47](#)
- autovolumerelease, [7-48](#)
- backup compression, [7-1](#)
- backup encryption policies, [7-3](#)
- backupev, [7-28](#)
- backupimagerechecklevel, [7-32](#)
- backuptypes, [7-33](#)
- backuptype, [7-29](#)
- barcodesrequired, [7-25](#)
- blockingfactor, [7-25](#)
- buffersize, [7-2](#)
- certkeysize, [7-43](#)
- clientlogevents, [7-23](#)
- cloud storage device policies, [7-8](#)
- customeridstring, [7-49](#)
- daemon policies, [7-9](#)
- defaultjobpriority, [7-7](#)
- defaultscanjobpriority, [7-46](#)
- defaultstarttime, [7-40](#)
- device policies, [7-13](#)
- disableasyncio, [7-15](#)
- discovereddevicestate, [7-15](#)
- duplicateovernetwork, [7-17](#)
- duplication policies, [7-17](#)
- duplicationjobpriority, [7-18](#)
- earliestindexcleanuptime policy, [7-19](#)
- enablerds, [7-34](#)
- encryptdataintransit, [7-44](#)
- encryption, [7-4–7-7](#)
- errorrate, [7-15](#)
- excludeformats, [7-3](#)
- freedstucktapethreshold, [7-25](#)
- fullbackupcheckpointfrequency, [7-34](#)
- generatendmpindexdata, [7-20](#)
- incrbackupcheckpointfrequency, [7-34](#)
- index policies, [7-19](#)
- indexcleanupfrequency, [7-20](#)
- jobretaintime, [7-23](#)
- keytype, [7-5](#)
- latestindexcleanuptime, [7-20](#)
- listing, [2-157](#)
- log policies, [7-22](#)

defaults and policies (*continued*)

- loginduration, [7-44](#)
- logretaintime, [7-23](#)
- mailport, [7-35](#)
- mailserver, [7-35](#)
- maxacsejectwaittime, [7-16](#)
- maxblockingfactor, [7-26](#)
- maxcheckpointrestarts, [7-36](#)
- maxdataretries, [7-41](#)
- maxdriveidletime, [7-15](#)
- maxindexbuffer, [7-20](#)
- media policies, [7-24](#)
- minwritablevolumes, [7-49](#)
- naming policies, [7-27](#)
- NDMP policies, [7-28](#)
- obdupoptions, [7-8](#)
- obixdmaxupdaters, [7-10](#)
- obixdrechecklevel, [7-11](#)
- obixdupdaternicevalue, [7-11](#)
- obstagescandebuglevel, [7-47](#)
- operations policies, [7-31](#)
- option, [7-2](#)
- overwriteblanktape, [7-26](#)
- overwriteforeigntape, [7-26](#)
- overwriteunreadabletape, [7-27](#)
- password, [7-29](#)
- passwordgracetime, [7-44](#)
- passwordlifetime, [7-45](#)
- passwordreusetime, [7-45](#)
- pollfrequency, [7-41](#)
- poolfreespacegoal, [7-17](#)
- port, [7-30](#)
- positiondatainterval, [7-21](#)
- progressupdatefrequency, [7-36](#)
- protocolversion, [7-30](#)
- proxypassword, [7-9](#)
- proxyserver, [7-8](#)
- proxyuser, [7-8](#)
- rekeyfrequency, [7-6](#)
- removing a policy setting, [3-122](#)
- reportretaintime, [7-49](#)
- restartablebackups, [7-36](#)
- restoreev, [7-30](#)
- restoreoptions, [7-37](#)
- retainbackupmetrics, [7-41](#)
- rmanresourcewaittime, [7-38](#)
- rmanrestorestartdelay, [7-38](#)
- saveasciiindexfiles, [7-21](#)
- scheduler policies, [7-39](#)
- securecomms, [7-45](#)
- security policies, [7-42](#)
- segmentsize, [7-9](#)
- setting policy values, [3-142](#)
- staging policies, [7-46](#)
- streamsperjob, [7-9](#)

- defaults and policies (*continued*)
 - tcpbufsize, 7-38
 - transcriptretaintime, 7-24
 - transfertimeout, 7-9
 - trustedhosts, 7-45
 - unixclientlogfile, 7-24
 - usepersistentcon, 7-9
 - username, 7-31
 - vaulting policies, 7-47
 - volumeretaintime, 7-27
 - webautostart, 7-11
 - webinactivity timeout, 7-46
 - webpass, 7-12
 - windowsclientlogfile, 7-24
 - windowscontrolcertificateservice, 7-13
 - windowsskipcds, 7-39
 - windowsskiplockedfiles, 7-39
 - winsserver, 7-27
 - writewindowtime, 7-27
- defaultscanjobpriority policy, 7-46
- defaultstarttime policy, 7-40
- defining
 - PNI for existing host, 3-40
 - user classes, 3-2
- device commands
 - about, 1-15
 - chdev, 2-30
 - discoverdev, 2-85
 - dumpdev, 2-88
 - lsdev, 2-133
 - mkdev, 3-6
 - mountdev, 3-69
 - pingdev, 3-73
 - rendev, 3-84
 - resdev, 3-96
 - rmdev, 3-112
 - unmountdev, 3-149
 - unresdev, 3-150
- device discovery
 - defaults and policies, 7-13
- device files, 3-10
- device policies
 - about, 7-13
 - disableasyncio, 7-15
 - discovereddevicestate, 7-15
 - errorrate, 7-15
 - maxacsejectwaittime, 7-16
 - maxdriveidletime, 7-15
 - poolfreospacegoal, 7-17
- devicename placeholder, 4-12
- devices
 - configuring, 3-6
 - data transfer elements, 2-183
 - defining position interval, 3-9
- devices (*continued*)
 - error rate, 3-9
 - import/export elements, 2-183
 - listing attributes, 2-133
 - medium transport elements, 2-183
 - pinging, 3-73
 - removing, 3-112
 - renaming, 3-84
 - testing attachments, 3-73
 - unreserving, 3-150
- disableasyncio policy, 7-15
- discovereddevicestate policy, 7-15
- disk pools
 - capacity, 3-13
 - configuring, 3-12
 - deleting contents, 3-112
 - deleting expired backups, 3-1
 - managing, 3-1
 - modifying file-system path, 2-33
 - reconfiguring, 2-32
 - removing, 3-112
 - removing backup image instances, 3-118
 - restriction placeholders, 4-25
- display administrative domain's configuration right, 8-4
- displaying
 - current catalog directory, 3-76
 - current dataset directory, 3-77
 - current policy, 3-77
 - job transcripts, 2-22
 - name of current obtool user, 2-100
 - obtool variable values, 3-144
- distribution reports
 - listing, 2-166
- drive variable, 5-1
- dupevent placeholder, 4-12
- duplicateovernetwork policy, 7-17
- duplication
 - duplicateovernetwork policy, 7-17
 - duplicationjobpriority policy, 7-18
- duplication jobs
 - listing, 2-149
- duplication policies
 - about, 7-17
 - changing, 2-41
 - duplicateovernetwork, 7-17
 - duplicationjobpriority, 7-18
 - event placeholders, 4-12
 - listing, 2-140
 - name placeholders, 4-22
 - removing, 3-115
 - renaming, 3-86
 - rule placeholder, 4-13
- duplication policy commands
 - lsdup, 2-140

duplication policy commands (*continued*)
 rendup, [3-86](#)
 rmdup, [3-115](#), [3-127](#)

duplication scan
 priority placeholders, [4-26](#)

duplication scan schedules
 creating, [3-44](#)
 listing, [2-167](#)
 removing, [3-128](#)
 renaming, [3-90](#)

duplication window commands
 about, [1-15](#)
 adddw, [2-2](#)
 lsdw, [2-141](#)

duplication windows
 adding, [2-2](#)
 listing, [2-141](#)

duplicationjobpriority policy, [7-18](#)

duration placeholder, [4-14](#)

E

earliestindexcleanuptime policy, [7-19](#)

editing

dataset files, [2-92](#)

element-spec placeholder, [4-14](#)

enablerds policy, [7-34](#)

encryptdataintransit policy, [7-44](#)

encryption

algorithm policy, [7-3](#)

encryptdataintransit policy, [7-44](#)

encryption policy, [7-4–7-6](#)

file-system backup, [2-7](#)

keytype policy, [7-5](#)

rekeyfrequency policy, [7-6](#)

encryption policy, [7-4–7-7](#)

error rate

errorate policy, [7-15](#)

tape devices, [3-9](#)

errorate policy, [7-15](#)

errors

displaying for tape devices, [2-88](#)

errors variable, [5-2](#)

escape variable, [5-2](#)

event placeholder, [4-15](#)

exclude dir statement, [6-10](#)

exclude file statement, [6-11](#)

exclude name statement, [6-11](#)

exclude oracle database files statement, [6-13](#)

exclude path statement, [6-14](#)

excludeformats policy, [7-3](#)

exit codes

obtool, [1-24](#)

exiting

obtool, [2-113](#)

expiration policies
 content-managed, [3-36](#)
 time-managed, [3-36](#)

expired backups

deleting

cloud storage devices, [3-1](#)

disk pools, [3-1](#)

exporting

identity certificates with obcm, [A-5](#)

F

file systems

creating restore requests, [3-99](#)

listing on NDMP devices, [2-141](#)

file-system backup

adding request, [2-4](#)

encryption, [2-7](#)

privileged, [2-6](#)

unprivileged, [2-6](#)

file-system backups

about dataset statements, [6-4](#)

dataset examples, [6-2](#)

dataset language backward compatibility, [6-4](#)

dataset language overview, [6-1](#)

file-system commands

about, [1-16](#)

filename placeholder, [4-13](#), [4-16](#)

filename-list placeholder, [4-16](#)

freedstucktapethreshold policy, [7-25](#)

fs variable, [5-2](#)

fullbackupcheckpointfrequency policy, [7-34](#)

G

generatendmpindexdata policy, [7-20](#)

GID

value 60002, [B-6](#), [B-24](#)

glossary

obtool, [1-9](#)

H

hardware compression

with obtar, [B-22](#)

help

obtool, [1-1](#), [1-7](#)

host commands

about, [1-16](#)

chhost, [2-43](#)

lshost, [2-143](#)

mkhost, [3-26](#)

pinghost, [3-75](#)

renhost, [3-87](#)

host commands (*continued*)
 rmhost, [3-117](#)
 updatehost, [3-153](#)

host variable, [5-3](#)

hosts
 adding, [3-26](#)
 changing attributes, [2-43](#)
 defining PNI for, [3-40](#)
 host variable, [5-3](#)
 include host dataset statement, [6-16](#)
 IP addresses testing, [3-75](#)
 listing attributes, [2-143](#)
 listing daemons on, [2-131](#)
 pinging, [3-75](#)
 removing, [3-117](#)
 renaming, [3-87](#)
 role placeholders, [4-25](#)
 synchronizing with administrative server,
[3-153](#)
 trustedhosts policy, [7-45](#)
 updating, [3-153](#)

I

identity certificates
 certkeysize policy, [7-43](#)
 importing and exporting with obcm, [A-5](#)

iee-range placeholder, [4-16](#)

iee-spec placeholder, [4-17](#)

import/export
 elements, [2-183](#)
 opening door, [3-72](#)

importing
 identity certificates with obcm, [A-5](#)
 volumes into tape libraries, [2-102](#)

include catalog statement, [6-15](#)

include dataset statement, [6-16](#)

include host statement, [6-16](#)

include path statement, [6-17](#)

incrbackupcheckpointfrequency policy, [7-34](#)

incremental backups
 autohistory policy, [7-32](#)
 level variable, [5-3](#)

index daemon
 asciiindexrepository policy, [7-19](#)
 autoindex policy, [7-19](#)
 earliestindexcleanuptime policy, [7-19](#)
 generatendmpindexdata policy, [7-20](#)
 indexcleanupfrequency policy, [7-20](#)
 latestindexcleanuptime policy, [7-20](#)
 maxindexbuffer policy, [7-20](#)
 obixdupdaternicevalue policy, [7-11](#)
 saveasciiindexfiles policy, [7-21](#)

index policies
 about, [7-19](#)

index policies (*continued*)
 asciiindexrepository, [7-19](#)
 autoindex, [7-19](#)
 earliestindexcleanuptime, [7-19](#)
 generatendmpindexdata, [7-20](#)
 indexcleanupfrequency, [7-20](#)
 latestindexcleanuptime, [7-20](#)
 maxindexbuffer, [7-20](#)
 saveasciiindexfiles, [7-21](#)

indexcleanupfrequency policy, [7-20](#)

input file
 redirecting obtool commands from, [1-5](#)

inserting
 volumes into tape libraries, [2-105](#)

interactive mode
 obtool, [1-3](#)

inventory
 scanning tape libraries, [2-108](#)

IP addresses
 format of, [2-44](#), [3-28](#)
 testing for host, [3-75](#)

J

job commands
 about, [1-16](#)
 canceljob, [2-14](#)
 catxcr, [2-22](#)
 lsjob, [2-149](#)
 rmjob, [3-119](#)
 rpyjob, [3-137](#)
 runjob, [3-138](#)

job summaries
 changing, [2-70](#)

job summary schedules
 creating, [3-61](#)
 listing, [2-178](#)
 removing, [3-133](#)
 renaming, [3-94](#)

job transcripts
 displaying, [2-22](#)

job-type placeholder, [4-17](#)

jobretaintime policy, [7-23](#)

jobs
 autovolumerelease policy, [7-47](#)
 backup placeholder, [4-18](#)
 cancelling, [2-14](#)
 controlling, [3-138](#)
 dataset placeholder, [4-18](#)
 duplication job placeholder, [4-19](#)
 listing, [2-149](#)
 media movement job placeholder, [4-19](#)
 removing, [3-119](#)
 responding to request for assistance, [3-137](#)
 restore placeholder, [4-18](#)

jobs (*continued*)

- RMAN backup placeholder, [4-18](#)
- RMAN restore placeholder, [4-18](#)
- scan control placeholder, [4-18](#)
- starting, [3-138](#)
- superseded, [3-62](#)
- type placeholder, [4-17](#)

K

keytype policy, [7-5](#)

L

labeling

- manually labeling volumes, [2-110](#)

large number format, [4-21](#)

latestindexcleanuptime policy, [7-20](#)

level variable, [5-3](#)

library commands

- about, [1-16](#)
- borrowdev, [2-12](#)
- clean, [2-79](#)
- closedoor, [2-80](#)
- exportvol, [2-94](#)
- extractvol, [2-96](#)
- identifyvol, [2-100](#)
- importvol, [2-102](#)
- insertvol, [2-105](#)
- inventory, [2-108](#)
- labelvol, [2-110](#)
- loadvol, [2-112](#)
- lsvol, [2-182](#)
- movevol, [3-71](#)
- opendoor, [3-72](#)
- returndev, [3-105](#)
- reusevol, [3-106](#)
- unlabelvol, [3-146](#)
- unloadvol, [3-148](#)

library variable, [1-17](#), [5-3](#)

list any backup, regardless of its owner, [8-4](#)

list any backups owned by user, [8-4](#)

list any job, regardless of its owner right, [8-5](#)

list any jobs owned by user right, [8-5](#)

listing

- backup image instances, [2-146](#)
- backup images with obtar -t, [B-11](#)
- backup requests, [2-117](#)
- backup sections, [2-170](#)
- backup windows, [2-125](#)
- cataloged backups, [2-122](#)
- checkpoints, [2-126](#)
- daemons, [2-131](#)
- database backup storage selectors, [2-175](#)
- dataset directory names, [2-139](#)

listing (*continued*)

- dataset names, [2-139](#)
- defaults and policies, [2-157](#)
- device attributes, [2-133](#)
- duplication policies, [2-140](#)
- duplication windows, [2-141](#)
- file systems on NDMP devices, [2-141](#)
- host attributes, [2-143](#)
- job summary schedules, [2-178](#)
- jobs, [2-149](#)
- locations, [2-155](#)
- media families, [2-156](#)
- namewidth variable, [5-4](#)
- numberformat variable, [5-4](#)
- PNI definitions, [2-162](#)
- reports, [2-166](#)
- restore requests, [2-164](#)
- RMAN backup pieces, [2-160](#)
- rotation policies, [2-166](#)
- schedules, [2-167](#)
- snapshots, [2-173](#)
- user classes, [2-128](#)
- users, [2-180](#)
- verbose variable, [5-4](#)
- volumes, [2-182](#)
- width variable, [5-5](#)

location commands

- about, [1-17](#)
- chloc, [2-50](#)
- lsmf, [2-155](#)
- mkloc, [3-34](#)
- renloc, [3-88](#)
- rmloc, [3-120](#)

locations

- creating, [3-34](#)
- listing, [2-155](#)
- modifying, [2-50](#)
- removing, [3-120](#)
- renaming, [3-88](#)

log policies

- about, [7-22](#)
- adminlogevents, [7-22](#)
- adminlogfile, [7-22](#)
- clientlogevents, [7-23](#)
- jobretaintime, [7-23](#)
- logretaintime, [7-23](#)
- transcriptretaintime, [7-24](#)
- unixclientlogfile, [7-24](#)
- windowsclientlogfile, [7-24](#)

logging in

- auditlogins policy, [7-10](#)
- loginduration policy, [7-44](#)

logging out

- obtool, [1-6](#)

login token, [1-2](#)

login token (*continued*)
 destroyed, [1-6](#)
 destroying, [2-113](#)
 loginduration policy, [7-44](#)
 preserved, [1-6](#)
 loginduration policy, [1-2](#), [7-44](#)
 logout command, [1-6](#)
 logretaintime policy, [7-23](#)

M

mailport policy, [7-35](#)
 mailserv policy, [7-35](#)
 makedev program, [A-1](#)
 manage devices and change device state right,
[8-5](#)
 managing
 cloud storage devices, [3-1](#)
 disk pools, [3-1](#)
 manual certificate provisioning mode
 and obcm, [A-5](#)
 maxacsejectwaittime policy, [7-16](#)
 maxblockingfactor policy, [7-26](#)
 maxcheckpointresetarts policy, [7-36](#)
 maxdataretries policy, [7-41](#)
 maxdriveidletime policy, [7-15](#)
 maximum blocking factor, [3-8](#)
 maxindexbuffer policy, [7-20](#)
 maxlevel variable, [5-3](#)
 md5 authorization type for NDMP server, [4-3](#)
 media families
 changing attributes, [2-52](#)
 characteristics, [1-17](#)
 creating, [3-36](#)
 listing, [2-156](#)
 removing, [3-121](#)
 renaming, [3-88](#)
 restricting with RMAN parameters, [C-1](#)
 RMAN-DEFAULT, [1-18](#)
 selecting with RMAN parameters, [C-4](#), [C-6](#)
 media family commands
 about, [1-17](#)
 chmf, [2-52](#)
 lsmf, [2-156](#)
 mkmf, [3-36](#)
 renmf, [3-88](#)
 rmmf, [3-121](#)
 media life cycle
 autovolumerelease policy, [7-48](#)
 changing duplication policies, [2-41](#)
 changing rotation policy settings, [2-56](#)
 creating duplication job summary schedules,
[3-61](#)
 creating duplication scan schedules, [3-44](#)
 creating rotation policies, [3-42](#)

media life cycle (*continued*)
 creating vaulting scan schedules, [3-44](#)
 creating volume duplication policies, [3-24](#)
 customeridstring policy, [7-49](#)
 duplicateovernetwork policy, [7-17](#)
 duplication job placeholder, [4-19](#)
 duplication policy event placeholders, [4-12](#)
 duplication policy name placeholders, [4-22](#)
 duplication policy rule placeholders, [4-13](#)
 duplication scan priority placeholders, [4-26](#)
 duplication window commands, [1-15](#)
 duplicationjobpriority policy, [7-18](#)
 listing distribution reports, [2-166](#)
 listing duplication jobs, [2-149](#)
 listing duplication policies, [2-140](#)
 listing duplication windows, [2-141](#)
 listing locations, [2-155](#)
 listing media movement jobs, [2-149](#)
 listing pick reports, [2-166](#)
 listing rotation policies, [2-166](#)
 listing scan control jobs, [2-149](#)
 location commands, [1-17](#)
 media movement job placeholder, [4-19](#)
 minwritablevolumes policy, [7-49](#)
 modifying locations, [2-50](#)
 recalling volumes from offsite storage, [3-79](#)
 releasing volumes, [3-80](#)
 removing duplication policies, [3-115](#)
 removing duplication scan schedules, [3-128](#)
 removing rotation policies, [3-127](#)
 removing storage locations, [3-120](#)
 removing vaulting scan schedules, [3-128](#)
 renaming duplication policies, [3-86](#)
 renaming duplication scan schedules, [3-90](#)
 renaming rotation policies, [3-89](#)
 renaming storage locations, [3-88](#)
 renaming vaulting scan schedules, [3-90](#)
 reportretaintime, [7-49](#)
 reports commands, [1-19](#)
 rotation policy commands, [1-20](#)
 rotation policy name placeholders, [4-22](#)
 rotation rule event placeholders, [4-15](#)
 rotation rule placeholders, [4-26](#)
 vaulting scan job placeholder, [4-18](#)
 vaulting scan priority placeholders, [4-26](#)
 volume duplication commands, [1-22](#)
 volume rotation commands, [1-22](#)
 media movement
 displaying reports, [2-20](#)
 listing jobs, [2-149](#)
 media policies
 about, [7-24](#)
 barcodesrequired, [7-25](#)
 blockingfactor, [7-25](#)
 freedstucktapethreshold, [7-25](#)

media policies (*continued*)

- maxblockingfactor, [7-26](#)
- overwriteblanktape, [7-26](#)
- overwriteforeigntape, [7-26](#)
- overwriteunreadabletape, [7-27](#)
- volumeretaintime, [7-27](#)
- writewindowtime, [7-27](#)

medium transport elements, [2-183](#)

minimumwriteablevolumes policy, [7-49](#)

minuserpasswordlen, [7-44](#)

miscellaneous commands

- about, [1-18](#)
- exit, [2-93](#)
- id, [2-100](#)
- logout, [2-113](#)
- quit, [3-79](#)

miscellaneous programs, [A-1](#)

- makedev, [A-1](#)
- obcleanup, [A-3](#)
- obcm, [A-5](#)
- uninstallob, [A-9](#)

modify administrative domain's configuration

- right, [8-4](#)

modify any backup, regardless of its owner, [8-5](#)

modify any backups owned by user, [8-5](#)

modify any job, regardless of its owner right, [8-5](#)

modify any jobs owned by user right, [8-5](#)

modify own name and password right, [8-6](#)

modifying

- backup image instances, [2-47](#)

mount points

- backing up across mount points with obtar, [B-5](#)

mounting

- volume, [3-69](#)

moving

- volumes in tape libraries, [3-71](#)

N

name-format placeholder, [4-19](#)

names

- listing for dataset directories, [2-139](#)
- listing for dataset files, [2-139](#)

namewidth variable, [5-4](#)

naming

- backup images, [2-8](#)

naming policies

- about, [7-27](#)
- winsserver, [7-27](#)

NDMP devices

- discovering, [2-85](#)
- listing file systems on, [2-141](#)

NDMP hosts

- adding, [3-26](#)

NDMP hosts (*continued*)

- listing snapshots on, [2-173](#)
- protocol version placeholders, [4-24](#)

NDMP policies

- about, [7-28](#)
- authenticationtype, [7-28](#)
- backupev, [7-28](#)
- backuptype, [7-29](#)
- password, [7-29](#)
- port, [7-30](#)
- protocolversion, [7-30](#)
- restoreev, [7-30](#)
- username, [7-31](#)

NDMP server

- authenticationtype policy, [7-28](#)
- authorization type placeholder, [4-3](#)
- backupev policy, [7-28](#)
- backuptype policy, [7-29](#)
- md5 authorization type for, [4-3](#)
- negotiated authorization type for, [4-3](#)
- password policy, [7-29](#)
- port policy, [7-30](#)
- protocolversion policy, [7-30](#)
- restoreev policy, [7-30](#)
- text authorization type for, [4-3](#)
- username policy, [7-31](#)

ndmp-backup-type placeholder, [4-20](#)

negotiated authorization type for NDMP server, [4-3](#)

nested block, [6-1](#)

Network Appliance filer, [3-53](#)

noninteractive mode

- obtool, [1-4](#)

number format for large numbers, [4-21](#)

numberformat placeholder, [4-21](#)

numberformat variable, [5-4](#)

O

OB_IGNORE_NUMA parameter, [C-6](#)

obcleanup program, [A-3](#)

obcm program, [A-5](#)

obdupoptions policy, [7-8](#)

obixdmaxupdaters policy, [7-10](#)

obixdrechecklevel policy, [7-11](#)

obixdupdaternicevalue policy, [7-11](#)

obstagescandebuglevel policy, [7-47](#)

obtar

- c mode, [B-6](#)
- t mode, [B-11](#)
- x mode, [B-8](#)
- zz mode, [B-14](#)
- backing up across mount points, [B-5](#)
- backing up raw file systems, [B-3](#)
- basic modes, [B-1](#)

- obtar (*continued*)
 - improving performance, [B-2](#)
 - incremental backups, [B-4](#)
 - overview, [B-1](#)
 - permissions when restoring, [B-8](#)
 - syntax, [B-1](#)
 - using tar with, [B-2](#)
- obtool
 - backup commands, [1-10](#)
 - backup image instance commands, [1-11](#)
 - backup piece commands, [1-11](#)
 - backup window commands, [1-11](#)
 - batch mode, [1-5](#)
 - browser commands, [1-12](#)
 - checkpoint commands, [1-12](#)
 - class commands, [1-13](#)
 - command categories, [1-9](#)
 - command syntax, [1-9](#)
 - conventions, [1-23](#)
 - daemon commands, [1-13](#)
 - database backup storage selector
 - commands, [1-14](#)
 - dataset commands, [1-14](#)
 - date/time format, [1-7](#)
 - device commands, [1-15](#)
 - duplication window commands, [1-15](#)
 - escaping special characters, [1-5](#)
 - exit codes, [1-24](#)
 - exit command, [1-6](#)
 - exiting, [1-6](#), [2-93](#), [2-113](#)
 - file-system commands, [1-16](#)
 - glossary, [1-9](#)
 - help, [1-1](#)
 - host commands, [1-16](#)
 - interactive mode, [1-3](#)
 - invoking, [1-1](#)
 - job commands, [1-16](#)
 - library commands, [1-16](#)
 - location commands, [1-17](#)
 - logging in, [1-1](#)
 - logging out, [1-6](#)
 - media family commands, [1-17](#)
 - miscellaneous commands, [1-18](#)
 - noninteractive mode, [1-4](#)
 - online help, [1-7](#)
 - policy commands, [1-18](#)
 - preauthorization, [1-2](#)
 - preferred network interface commands, [1-19](#)
 - quit command, [1-6](#)
 - quitting, [3-79](#)
 - redirecting from input file, [1-5](#)
 - report commands, [1-19](#)
 - restore commands, [1-19](#)
 - rotation policy commands, [1-20](#)
 - schedule commands, [1-20](#)
- obtool (*continued*)
 - section commands, [1-20](#)
 - setting variables, [3-140](#)
 - snapshot commands, [1-21](#)
 - staging commands, [1-21](#)
 - starting as specific user, [1-6](#)
 - summary commands, [1-21](#)
 - topics, [1-8](#)
 - unsetting variables, [3-153](#)
 - user commands, [1-22](#)
 - version number, [1-7](#)
 - volume duplication commands, [1-22](#)
 - volume rotation commands, [1-22](#)
- obtool commands
 - adbbw, [2-1](#)
 - adddw, [2-2](#)
 - addp, [2-3](#)
 - backup, [2-4](#)
 - borrowdev, [2-12](#)
 - canceljob, [2-14](#)
 - catds, [2-19](#)
 - catrpt, [2-20](#)
 - catxcr, [2-22](#)
 - cd, [2-25](#)
 - cdds, [2-26](#)
 - cdp, [2-27](#)
 - chclass, [2-28](#)
 - chdev, [2-30](#)
 - chdup, [2-41](#)
 - chhost, [2-43](#)
 - chkbw, [2-48](#)
 - chkds, [2-49](#)
 - chloc, [2-50](#)
 - chmf, [2-52](#)
 - chrot, [2-56](#)
 - chsched, [2-58](#)
 - chssel, [2-65](#)
 - chsum, [2-70](#)
 - chuser, [2-72](#)
 - chvol, [2-75](#)
 - clean, [2-79](#)
 - closedoor, [2-80](#)
 - ctldaemon, [2-83](#)
 - discoverdev, [2-85](#)
 - dumpdev, [2-88](#)
 - edds, [2-92](#)
 - exit, [2-93](#)
 - exportvol, [2-94](#)
 - extractvol, [2-96](#)
 - id, [2-100](#)
 - identifyvol, [2-100](#)
 - importvol, [2-102](#)
 - insertvol, [2-105](#)
 - inventory, [2-108](#)
 - labelvol, [2-110](#)

obtool commands (*continued*)

loadvol, [2-112](#)
 logout, [2-113](#)
 ls, [2-114](#)
 lsbackup, [2-117](#)
 lsbu, [2-122](#)
 lsbw, [2-125](#)
 lscheckpoint, [2-126](#)
 lsclass, [2-128](#)
 lsdaemon, [2-131](#)
 lsdev, [2-133](#)
 lsds, [2-139](#)
 lsdup, [2-140](#)
 lsdw, [2-141](#)
 lsfs, [2-141](#)
 lshost, [2-143](#)
 lsjob, [2-149](#)
 lsloc, [2-155](#)
 lsmf, [2-156](#)
 lsp, [2-157](#)
 lspiece, [2-160](#)
 lspni, [2-162](#)
 lsrestore, [2-164](#)
 lsrot, [2-166](#)
 lsrpt, [2-166](#)
 lssched, [2-167](#)
 lssection, [2-170](#)
 lssnap, [2-173](#)
 lsssel, [2-175](#)
 lsstage, [2-177](#)
 lssum, [2-178](#)
 lsuser, [2-180](#)
 lsvol, [2-182](#)
 mkclass, [3-2](#)
 mkdev, [3-6](#)
 mkds, [3-21](#)
 mkdup, [3-24](#)
 mkhost, [3-26](#)
 mkloc, [3-34](#)
 mkmf, [3-36](#)
 mkpni, [3-40](#)
 mkrot, [3-42](#)
 mksched, [3-44](#)
 mksnap, [3-53](#)
 mkssel, [3-54](#)
 mkstage, [3-57](#)
 mksum, [3-61](#)
 mkuser, [3-64](#)
 mountdev, [3-69](#)
 movevol, [3-71](#)
 opendoor, [3-72](#)
 pingdev, [3-73](#)
 pinghost, [3-75](#)
 pwd, [3-76](#)
 pwdds, [3-77](#)

obtool commands (*continued*)

pwdp, [3-77](#)
 quit, [3-79](#)
 recallvolume, [3-79](#)
 releasevolume, [3-80](#)
 renclass, [3-83](#)
 rendev, [3-84](#)
 rends, [3-85](#)
 rendup, [3-86](#)
 renhost, [3-87](#)
 renloc, [3-88](#)
 renmf, [3-88](#)
 renrot, [3-89](#)
 rensched, [3-90](#)
 rensnap, [3-91](#)
 rensel, [3-93](#)
 rensun, [3-94](#)
 renuser, [3-95](#)
 resdev, [3-96](#)
 resetp, [3-97](#)
 restore, [3-99](#)
 returndev, [3-105](#)
 reusevol, [3-106](#)
 rmbbackup, [3-108](#)
 rmbw, [3-110](#)
 rmcheckpoint, [3-110](#)
 rmclass, [3-111](#)
 rmdev, [3-112](#)
 rmds, [3-114](#)
 rmdup, [3-115](#),
 [3-127](#)
 rmhost, [3-117](#)
 rmjob, [3-119](#)
 rmloc, [3-120](#)
 rmmf, [3-121](#)
 rmp, [3-122](#)
 rmpiece, [3-123](#)
 rmpni, [3-124](#)
 rmrestore, [3-127](#)
 rmsched, [3-128](#)
 rmsection, [3-129](#)
 rmsnap, [3-130](#)
 rmssel, [3-132](#)
 rmstage, [3-133](#)
 rmsum, [3-133](#)
 rmuser, [3-134](#)
 rpyjob, [3-137](#)
 runjob, [3-138](#)
 set, [3-140](#)
 setbw, [3-140](#)
 setp, [3-142](#)
 show, [3-144](#)
 stagescan, [3-145](#)
 unlabelvol, [3-146](#)
 unloadvol, [3-148](#)

- obtool commands (*continued*)
 - unmountdev, [3-149](#)
 - unresdev, [3-150](#)
 - unrmsection, [3-151](#)
 - unset, [3-153](#)
 - updatehost, [3-153](#)
 - obtool formats
 - date-range, [4-8](#)
 - date/time, [1-7](#)
 - obtoolrc
 - location, [1-3](#)
 - offsite storage
 - recalling volumes from, [3-79](#)
 - oid placeholder, [4-21](#)
 - oid-list placeholder, [4-22](#)
 - online help
 - obtool, [1-7](#)
 - opening
 - import/export door, [3-72](#)
 - operations policies
 - about, [7-31](#)
 - autohistory, [7-32](#)
 - autolabel, [7-32](#)
 - backupimagerechecklevel, [7-32](#)
 - backuptoptions, [7-33](#)
 - enablerds, [7-34](#)
 - fullbackupcheckpointfrequency, [7-34](#)
 - incrbackupcheckpointfrequency, [7-34](#)
 - mailport, [7-35](#)
 - mailserver, [7-35](#)
 - maxcheckpointrestarts, [7-36](#)
 - positiondatainterval, [7-21](#)
 - progressupdatefrequency, [7-36](#)
 - restartablebackups, [7-36](#)
 - restoreoptions, [7-37](#)
 - rmanresourcewaittime policy, [7-38](#)
 - rmanrestorestartdelay, [7-38](#)
 - tcpbufsize, [7-38](#)
 - windowsskipcdfs, [7-39](#)
 - windowsskiplockedfiles, [7-39](#)
 - operator class, [8-1](#), [8-2](#)
 - option policy, [7-2](#)
 - oracle class, [8-1](#), [8-2](#)
 - overwriteblanktape policy, [7-26](#)
 - overwriteforeigntape policy, [7-26](#)
 - overwriteunreadabletape policy, [7-27](#)
- ## P
-
- password management
 - forcing a password change, [2-73](#)
 - setting the password grace time, [2-73](#), [3-66](#)
 - setting the password lifetime, [2-73](#), [3-66](#)
 - setting the password reuse time, [2-73](#), [3-66](#)
 - password policy, [7-29](#)
 - passwordgracetime policy, [7-44](#)
 - passwordlifetime policy, [7-45](#)
 - passwordreusetime policy, [7-45](#)
 - passwords
 - forcing password change, [2-75](#)
 - NDMP password policy, [7-29](#)
 - security policy, [2-159](#), [3-98](#), [3-144](#)
 - webpass policy, [7-12](#)
 - perform backups as privileged user right, [8-6](#)
 - perform backups as self right, [8-6](#)
 - perform Oracle backups and restores right, [8-6](#)
 - perform restores as privileged user right, [8-6](#)
 - perform restores as self right, [8-7](#)
 - pick reports
 - listing, [2-166](#)
 - pinging
 - devices, [3-73](#)
 - hosts, [3-75](#)
 - placeholders, in obtool commands
 - aspec, [4-1](#)
 - authtype, [4-3](#)
 - backup-container, [4-4](#)
 - backup-level, [4-4](#)
 - concjobs, [4-5](#)
 - content, [4-5](#)
 - data-selector, [4-6](#)
 - dataset-dir-name, [4-7](#)
 - dataset-file-name, [4-7](#)
 - dataset-name, [4-8](#)
 - date-range, [4-8](#)
 - date-time, [4-9](#)
 - day-date, [4-9](#)
 - day-specifier, [4-12](#)
 - devicename, [4-12](#)
 - dupevent, [4-12](#)
 - duplicationrule, [4-13](#)
 - duration, [4-14](#)
 - element-spec, [4-14](#)
 - event, [4-15](#)
 - filenumber, [4-16](#)
 - filenumber-list, [4-16](#)
 - iee-range, [4-16](#)
 - iee-spec, [4-17](#)
 - job-type, [4-17](#)
 - name-format, [4-19](#)
 - ndmp-backup-type, [4-20](#)
 - numberformat, [4-21](#)
 - oid, [4-21](#)
 - oid-list, [4-22](#)
 - policyname, [4-22](#)
 - preauth-spec, [4-23](#)
 - produce-days, [4-24](#)
 - protover, [4-24](#)
 - restriction, [4-25](#)
 - role, [4-25](#)

placeholders, in obtool commands (*continued*)

- rotationrule, [4-26](#)
- schedule-priority, [4-26](#)
- se-range, [4-27](#)
- se-spec, [4-27](#)
- summary-start-day, [4-28](#)
- time, [4-29](#)
- time-range, [4-29](#)
- vid, [4-30](#)
- vol-range, [4-30](#)
- vol-spec, [4-31](#)
- wwn, [4-32](#)

PNI

- listing definitions, [2-162](#)
- removing definitions, [3-124](#)

policy

- about classes, [1-18](#)
- adding name/value pair, [2-3](#)
- displaying identity, [3-77](#)
- obtool commands, [1-18](#)
- removing name-value pair, [3-122](#)
- reset to default, [3-97](#)
- set identity of current policy, [2-27](#)
- setting password policies, [3-98](#), [3-142](#)
- setting value, [3-142](#)

policy classes

- about, [7-1](#)

policy commands

- addp, [2-3](#)
- cdp, [2-27](#)
- isp, [2-157](#)
- pwdp, [3-77](#)
- resetp, [3-97](#)
- rmp, [3-122](#)
- setp, [3-142](#)

polycname placeholder, [4-22](#)

pollfrequency policy, [7-41](#)

poolfreespacegoal policy, [7-17](#)

port policy, [7-30](#)

position interval

- defining for devices, [3-9](#)

positiondatainterval policy, [7-21](#)

preauth-spec placeholder, [4-23](#)

preauthorization

- about, [1-2](#)
- new user, [3-67](#)

preauthorizations

- preauth-spec placeholders, [4-23](#)

preferred network interface commands

- about, [1-19](#)
- ispni, [2-162](#)
- mkpni, [3-40](#)
- rmpni, [3-124](#)

private key

- certkeysize policy, [7-43](#)

private key (*continued*)

- keytype policy, [7-5](#)
- rekeyfrequency policy, [7-6](#)

privileged backup

- requesting, [2-6](#)

produce-days placeholder, [4-24](#)

programs, miscellaneous, [A-1](#)

progressupdatefrequency policy, [7-36](#)

protocolversion policy, [7-30](#)

protover placeholder, [4-24](#)

proxypassword policy, [7-9](#)

proxyserver policy, [7-8](#)

proxyuser policy, [7-8](#)

public key

- certkeysize policy, [7-43](#)
- keytype policy, [7-5](#)
- rekeyfrequency policy, [7-6](#)

Q

query and display information about devices

- right, [8-7](#)

R

raw file systems, backing up with obtar, [B-3](#)

raw restore operations, [3-99](#)

reader class, [8-1](#), [8-2](#)

recalling

- volumes from offsite storage, [3-79](#)

receive email describing expired passphrase

- keys right, [8-7](#)

receive email describing internal errors right, [8-7](#)

receive email requesting operator assistance

- right, [8-7](#)

reconfiguring

- disk pools, [2-32](#)

recycling

- volumes, [3-106](#)

rekeyfrequency policy, [7-6](#)

releasing

- volumes, [3-80](#)

removing

- backup pieces, [3-123](#)
- backup requests, [3-108](#)
- backup sections, [3-129](#)
- backup windows, [3-110](#)
- checkpoints, [3-110](#)
- database backup storage selectors, [3-132](#)
- dataset directories, [3-114](#)
- dataset files, [3-114](#)
- devices, [3-112](#)
- duplication policies, [3-115](#)
- hosts, [3-117](#)
- job summary schedules, [3-133](#)

- removing (*continued*)
 - jobs, [3-119](#)
 - locations, [3-120](#)
 - media families, [3-121](#)
 - name-value pair from policy, [3-122](#)
 - PNI definitions, [3-124](#)
 - restore requests, [3-127](#)
 - rotation policies, [3-127](#)
 - schedules, [3-128](#)
 - snapshots, [3-130](#)
 - user classes, [3-111](#)
 - users, [3-134](#)
- renaming
 - backup images, [3-81](#)
 - database backup storage selectors, [3-93](#)
 - dataset directories, [3-85](#)
 - dataset files, [3-85](#)
 - devices, [3-84](#)
 - duplication policies, [3-86](#)
 - hosts, [3-87](#)
 - job summary schedules, [3-94](#)
 - locations, [3-88](#)
 - media families, [3-88](#)
 - rotation policies, [3-89](#)
 - schedules, [3-90](#)
 - snapshots, [3-91](#)
 - user classes, [3-83](#)
 - users, [3-95](#)
- reports
 - customeridstring policy, [7-49](#)
 - listing, [2-166](#)
 - reportretaintime policy, [7-49](#)
- reports commands
 - about, [1-19](#)
 - catrpt, [2-20](#)
 - lsrpt, [2-166](#)
- reserving
 - tape devices, [3-96](#)
- resetting
 - policy to default, [3-97](#)
- responding
 - job request for assistance, [3-137](#)
- restartable backups
 - fullbackupcheckpointfrequency policy, [7-34](#)
 - incrbackupcheckpointfrequency policy, [7-34](#)
 - maxcheckpointrestarts policy, [7-36](#)
 - removing checkpoints, [3-110](#)
 - restartablebackups policy, [7-36](#)
- restartablebackups policy, [7-36](#)
- restore
 - listing requests, [2-164](#)
 - priority placeholders, [4-26](#)
 - using wildcard pattern matching, [3-100](#)
- restore commands
 - about, [1-19](#)
- restore commands (*continued*)
 - lsrestore, [2-164](#)
 - restore, [3-99](#)
 - rmrestore, [3-127](#)
- restore jobs
 - listing, [2-149](#)
- restore operations
 - catalog-based, [3-99](#)
 - raw, [3-99](#)
- restore requests
 - creating for file-system restore, [3-99](#)
 - listing, [2-164](#)
 - removing, [3-127](#)
- restoreev policy, [7-30](#)
- restoreoptions policy, [7-37](#)
- restriction placeholders, [4-25](#)
- retainbackupmetrics policy, [7-41](#)
- returning
 - tape drives, [3-105](#)
- reusing
 - volumes, [3-106](#)
- RMAN
 - listing backup pieces, [2-160](#)
 - parameters overview, [C-1](#)
 - removing backup pieces, [3-123](#)
 - rmanresourcewaittime policy, [7-38](#)
 - rmanrestorestartdelay policy, [7-38](#)
- RMAN parameters
 - OB_BACKUP_NAME, [C-2](#)
 - OB_DEVICE, [C-1](#), [C-3](#)
 - OB_MEDIA_FAMILY, [C-1](#), [C-4](#), [C-6](#)
 - OB_RESOURCE_WAIT_TIME, [C-8](#)
- RMAN-DEFAULT
 - media family, [1-18](#)
- rmanpriority policy, [7-37](#)
- rmanresourcewaittime policy, [7-38](#)
- rmanrestorestartdelay policy, [7-38](#)
- role placeholder, [4-25](#)
- roles
 - role placeholders, [4-25](#)
- rotation policies
 - changing settings for, [2-56](#)
 - creating, [3-42](#)
 - listing, [2-166](#)
 - name placeholders, [4-22](#)
 - removing, [3-127](#)
 - renaming, [3-89](#)
 - rotation rule placeholders, [4-26](#)
- rotation policy commands
 - about, [1-20](#)
 - chrot, [2-56](#)
 - lsrot, [2-166](#)
 - mkdup, [3-42](#)
 - renrot, [3-89](#)
- rotation rules

rotation rules (*continued*)
 event placeholders, [4-15](#)
 rotationrule placeholder, [4-26](#)

S

saveasciindexfiles policy, [7-21](#)

scan control jobs
 listing, [2-149](#)

schedule commands
 about, [1-20](#)
 chsched, [2-58](#)
 lssched, [2-167](#)
 mksched, [3-44](#)
 rensched, [3-90](#)
 rmsched, [3-128](#)

schedule-priority placeholder, [4-26](#)

scheduler
 applybackupsfrequency policy, [7-40](#)
 backupoptions policy, [7-33](#)
 defaultstarttime policy, [7-40](#)
 maxdataretries policy, [7-41](#)
 pollfrequency policy, [7-41](#)
 restoreoptions policy, [7-37](#)
 retainbackupmetrics policy, [7-41](#)
 rmanresourcewaittime policy, [7-38](#)

scheduler policies
 about, [7-39](#)
 applybackupsfrequency, [7-40](#)
 defaultstarttime, [7-40](#)
 maxdataretries, [7-41](#)
 pollfrequency, [7-41](#)
 retainbackupmetrics, [7-41](#)

schedules
 changing properties of, [2-58](#)
 priority placeholders, [4-26](#)
 removing, [3-128](#)
 renaming, [3-90](#)

se-range placeholder, [4-27](#)

se-spec placeholder, [4-17](#), [4-27](#)

section commands
 about, [1-20](#)
 lssection, [2-170](#)
 rmsection, [3-129](#)
 unrmsection, [3-151](#)

securecomms policy, [7-45](#)

security policies
 about, [7-42](#)
 autocertissue, [7-42](#)
 certkeysize, [7-43](#)
 encryptdataintransit, [7-44](#)
 loginduration, [7-44](#)
 passwordgracetime, [7-44](#)
 passwordlifetime, [7-45](#)
 passwordreusetime, [7-45](#)

security policies (*continued*)
 securecomms, [7-45](#)
 trustedhosts, [7-45](#)
 untrustedhostjobs, [7-46](#)

segmentsize policy, [7-9](#)

setting
 policy value, [3-142](#)

snapshot commands
 about, [1-21](#)
 lssnap, [2-173](#)
 mksnap, [3-53](#)
 rensnap, [3-91](#)
 rmsnap, [3-130](#)

snapshot variable, [5-4](#)

snapshots
 browsemode variable, [5-1](#)
 creating, [3-53](#)
 defined, [3-53](#)
 listing, [2-173](#)
 removing, [3-130](#)
 renaming, [3-91](#)
 snapshot variable, [5-4](#)

special characters
 escape variable, [5-2](#)
 escaping in obtool, [1-5](#)

SSL
 encryptdataintransit policy, [7-44](#)
 securecomms policy, [7-45](#)
 webpass policy, [7-12](#)

staging
 defaultscanjobpriority policy, [7-46](#)
 obstagescanlevel, [7-47](#)

staging commands
 about, [1-21](#)
 lsstage, [2-177](#)
 mkstage, [3-57](#)
 rmstage, [3-133](#)
 stagescan, [3-145](#)

staging policies
 about, [7-46](#)
 defaultscanjobpriority, [7-46](#)
 obstagescandebuglevel, [7-47](#)

starting
 jobs, [3-138](#)
 obtool as specific user, [1-6](#)

storage elements
 moving volumes from, [2-112](#)
 number placeholder, [4-27](#)
 placeholder, [4-17](#)
 range placeholders, [4-27](#)

storage locations
 creating, [3-34](#)
 removing, [3-120](#)
 renaming, [3-88](#)

streamsperjob policy, [7-9](#)

summary commands

- about, [1-21](#)
- chsum, [2-70](#)
- lssum, [2-178](#)
- mksum, [3-61](#)
- rensum, [3-94](#)
- rmsum, [3-133](#)

summary reports

- produce-days placeholders, [4-24](#)

summary-start-day placeholder, [4-28](#)superseded jobs, [3-62](#)

syntax

- checking in dataset file, [2-49](#)
- obtool, [1-9](#)

T

tape devices

- attachment placeholders, [4-1](#)
- barcodesrequired policy, [7-25](#)
- configuring with makedev, [A-1](#)
- defaults and policies, [7-13](#)
- defining position interval, [3-9](#)
- discovereddevicestate policy, [7-15](#)
- drive variable, [5-1](#)
- element name placeholders, [4-14](#)
- element placeholders, [4-16](#)
- error rate, [3-9](#)
- errorate policy, [7-15](#)
- import/export element placeholders, [4-17](#)
- maxacsejectwaittime policy, [7-16](#)
- maxdriveidletime policy, [7-15](#)
- name placeholders, [4-12](#)
- removing, [3-112](#)
- reserving, [3-96](#)
- restricting with RMAN parameters, [C-1](#)
- restriction placeholders, [4-25](#)
- storage element name placeholders, [4-27](#)
- storage element range placeholders, [4-27](#)
- World Wide Name placeholders, [4-32](#)

tape drives

- attachment placeholders, [4-1](#)
- barcodesrequired policy, [7-25](#)
- borrowing, [2-12](#)
- changing attributes, [2-30](#)
- cleaning, [2-79](#)
- configuring, [3-7](#)
- configuring with makedev, [A-1](#)
- discovering, [2-85](#)
- displaying errors, [2-88](#)
- drive variable, [5-1](#)
- identifying volumes, [2-100](#)
- mounting volumes, [3-69](#)
- moving volumes to, [2-112](#)
- name placeholder, [4-12](#)

tape drives (*continued*)

- positiondatainterval policy, [7-21](#)
- removing, [3-112](#)
- renaming, [3-84](#)
- reserving, [3-96](#)
- restriction placeholders, [4-25](#)
- returning, [3-105](#)
- selecting with RMAN parameters, [C-3](#)
- unloading volumes, [3-148](#)
- unmounting volumes, [3-149](#)
- unreserving, [3-150](#)
- World Wide Name placeholders, [4-32](#)

tape libraries

- attachment placeholders, [4-1](#)
- barcodesrequired policy, [7-25](#)
- changing attributes, [2-30](#)
- closing import/export door, [2-80](#)
- configuring, [3-10](#)
- configuring with makedev, [A-1](#)
- discovering, [2-85](#)
- displaying errors, [2-88](#)
- drive variable, [5-1](#)
- element name placeholders, [4-14](#)
- element placeholders, [4-16](#)
- exporting volume, [2-94](#)
- import/export element placeholders, [4-17](#)
- importing volumes, [2-102](#)
- library variable, [5-3](#)
- listing volumes, [2-182](#)
- manually inserting volumes, [2-105](#)
- manually removing volume, [2-96](#)
- minwritablevolumes policy, [7-49](#)
- moving volumes in, [3-71](#)
- moving volumes to tape drives, [2-112](#)
- name placeholder, [4-12](#)
- opening import/export door, [3-72](#)
- removing, [3-112](#)
- renaming, [3-84](#)
- restriction placeholders, [4-25](#)
- scanning contents, [2-108](#)
- storage element name placeholders, [4-27](#)
- storage element range placeholders, [4-27](#)
- vol-spec placeholders, [4-31](#)
- World Wide Name placeholders, [4-32](#)

TCP/IP

- mailport policy, [7-35](#)
- tcpbufsize policy, [7-38](#)

tcpbufsize policy, [7-38](#)

testing

- IP addresses for host, [3-75](#)

text authorization type for NDMP server, [4-3](#)

time

- obtool format, [1-7](#)

time placeholder, [4-29](#)time-managed expiration policies, [3-36](#)

time-range placeholder, [4-29](#)
 transcriptretainpolicy, [7-24](#)
 transfertimeout policy, [7-9](#)
 triggers
 configuring, [3-44](#)
 definition, [3-44](#)
 trustedhosts policy, [7-45](#)

U

UID
 value 60002, [B-6](#), [B-24](#)
 uninstalling
 OSB with uninstallob, [A-9](#)
 uninstallob program, [A-9](#)
 unixclientlogfile policy, [7-24](#)
 unlabeled
 volumes, [3-146](#)
 unloading
 volumes, [3-148](#)
 unmounting
 volumes, [3-149](#)
 unprivileged backup
 requesting, [2-6](#)
 unreserving
 devices, [3-150](#)
 unsetting
 obtool variables, [3-153](#)
 untrustedhostjobs, [7-46](#)
 updating
 hosts, [3-153](#)
 usepersistentcon policy, [7-9](#)
 user class, [8-1](#), [8-2](#)
 user classes
 changing attributes, [2-28](#)
 defining, [3-2](#)
 listing attributes, [2-128](#)
 removing, [3-111](#)
 renaming, [3-83](#)
 user commands
 about, [1-22](#)
 chuser, [2-72](#)
 lsuser, [2-180](#)
 mkuser, [3-64](#)
 renuser, [3-95](#)
 rmuser, [3-134](#)
 username
 NDMP username policy, [7-31](#)
 username policy, [7-31](#)
 users
 changing attributes, [2-72](#)
 creating, [3-64](#)
 displaying name of current obtool user, [2-100](#)
 listing, [2-180](#)
 NDMP username policy, [7-31](#)

users (*continued*)
 preauth-spec placeholders, [4-23](#)
 preauthorizations, [3-67](#)
 removing, [3-134](#)
 renaming, [3-95](#)
 starting obtool as specific user, [1-6](#)

V

variable commands
 set, [3-140](#)
 show, [3-144](#)
 unset, [3-153](#)
 variables
 browsemode, [5-1](#)
 displaying values of obtool variable, [3-144](#)
 drive, [5-1](#)
 errors, [5-2](#)
 escape, [5-2](#)
 fs, [5-2](#)
 host, [5-3](#)
 level, [5-3](#)
 library, [1-17](#), [5-3](#)
 maxlevel, [5-3](#)
 namewidth, [5-4](#)
 numberformat, [5-4](#)
 setting in obtool, [3-140](#)
 snapshot, [5-4](#)
 unsetting in obtool, [3-153](#)
 verbose, [5-4](#)
 viewmode, [5-5](#)
 width, [5-5](#)
 vaulting
 autorunmmjobs policy, [7-47](#)
 autovolumerelease policy, [7-48](#)
 changing duplication policies, [2-41](#)
 changing rotation policy settings, [2-56](#)
 creating duplication job summary schedules,
 [3-61](#)
 creating duplication scan schedules, [3-44](#)
 creating rotation policies, [3-42](#)
 creating vaulting scan schedules, [3-44](#)
 creating volume duplication policies, [3-24](#)
 customeridstring policy, [7-49](#)
 displaying reports, [2-20](#)
 duplicateovernetwork policy, [7-17](#)
 duplication job placeholder, [4-19](#)
 duplication policy event placeholders, [4-12](#)
 duplication policy name placeholders, [4-22](#)
 duplication policy rule placeholders, [4-13](#)
 duplication scan priority placeholders, [4-26](#)
 duplication window commands, [1-15](#)
 duplicationjobpriority policy, [7-18](#)
 listing distribution reports, [2-166](#)
 listing duplication jobs, [2-149](#)

- vaulting (*continued*)
 - listing duplication policies, [2-140](#)
 - listing duplication windows, [2-141](#)
 - listing locations, [2-155](#)
 - listing media movement jobs, [2-149](#)
 - listing pick reports, [2-166](#)
 - listing rotation policies, [2-166](#)
 - listing scan control jobs, [2-149](#)
 - location commands, [1-17](#)
 - media movement job placeholder, [4-19](#)
 - minwritablevolumes policy, [7-49](#)
 - modifying locations, [2-50](#)
 - recalling volumes from offsite storage, [3-79](#)
 - releasing volumes, [3-80](#)
 - removing duplication policies, [3-115](#)
 - removing duplication scan schedules, [3-128](#)
 - removing rotation policies, [3-127](#)
 - removing storage locations, [3-120](#)
 - removing vaulting scan schedules, [3-128](#)
 - renaming duplication policies, [3-86](#)
 - renaming duplication scan schedules, [3-90](#)
 - renaming rotation policies, [3-89](#)
 - renaming storage locations, [3-88](#)
 - renaming vaulting scan schedules, [3-90](#)
 - reportretaintime policy, [7-49](#)
 - reports commands, [1-19](#)
 - rotation policy commands, [1-20](#)
 - rotation policy name placeholders, [4-22](#)
 - rotation rule event placeholders, [4-15](#)
 - rotation rule placeholders, [4-26](#)
 - scan control job placeholder, [4-18](#)
 - vaulting scan priority placeholders, [4-26](#)
 - volume duplication commands, [1-22](#)
 - volume rotation commands, [1-22](#)
- vaulting policies
 - about, [7-47](#)
 - automaticreleaseofrecalledvolumes, [7-49](#)
 - autorunmmjobs, [7-47](#)
 - autovolumerelease, [7-48](#)
 - customeridstring, [7-49](#)
 - minimumwriteablevolumes, [7-49](#)
- vaulting scan
 - priority placeholders, [4-26](#)
- vaulting scan schedules
 - creating, [3-44](#)
 - listing, [2-167](#)
 - removing, [3-128](#)
 - renaming, [3-90](#)
- verbose variable, [5-4](#)
- version number
 - obtool, [1-7](#)
- vid placeholder, [4-30](#)
- viewmode variable, [5-5](#)
- vol-range placeholder, [4-30](#)
- vol-spec placeholder, [4-31](#)
- volume commands
 - chvol, [2-75](#)
- volume duplication commands
 - about, [1-22](#)
 - chdup, [2-41](#)
 - mkdup, [3-24](#)
- volume duplication policies
 - creating, [3-24](#)
- volume labels
 - listing with obtar -zz, [B-14](#)
 - removing, [3-146](#)
- volume movement commands
 - releasevolume, [3-80](#)
- volume rotation commands
 - about, [1-22](#)
 - recallvolume, [3-79](#)
- volume sets
 - filenumber placeholders, [4-16](#)
- volumeretaintime policy, [7-27](#)
- volumes
 - autolabel policy, [7-32](#)
 - autovolumerelease policy, [7-48](#)
 - barcodesrequired policy, [7-25](#)
 - catalog identifier placeholders, [4-21](#)
 - changing attributes, [2-75](#)
 - erasing, [2-110](#)
 - exporting from tape libraries, [2-94](#)
 - exporting from tape library, [2-94](#)
 - identifying in tape drive, [2-100](#)
 - importing to tape libraries, [2-102](#)
 - inserting into tape library manually, [2-105](#)
 - listing, [2-182](#)
 - listing labels on a volume with obtar -zz, [B-14](#)
 - manually removing from tape libraries, [2-96](#)
 - minwritablevolumes policy, [7-49](#)
 - mounting, [3-69](#)
 - moving in tape libraries, [3-71](#)
 - moving to tape drives, [2-112](#)
 - overwriteblanktape policy, [7-26](#)
 - overwriteforeigntape policy, [7-26](#)
 - overwriteunreadabletape policy, [7-27](#)
 - recalling from offsite storage, [3-79](#)
 - recycling, [3-106](#)
 - releasing, [3-80](#)
 - removing backup data, [3-146](#)
 - reusing, [3-106](#)
 - rewinding, [3-148](#)
 - undoing remove backup section, [3-151](#)
 - unlabeling, [3-146](#)
 - unloading, [3-148](#)
 - unmounting, [3-149](#)
 - vid placeholders, [4-30](#)
 - vol-range placeholders, [4-30](#)
 - vol-spec placeholders, [4-31](#)
 - volumeretaintime policy, [7-27](#)

volumes (*continued*)
write new label, [2-110](#)
writewindowtime policy, [7-27](#)

W

webautostart policy, [7-11](#)
webpass policy, [7-12](#)
width variable, [5-5](#)
Windows CD-ROM file systems
windowsskipcdfs policy, [7-39](#)
Windows firewall, disabling, [3-26](#)
Windows locked files

Windows locked files (*continued*)
windowsskiplockedfiles policy, [7-39](#)
Windows Server 2003, [3-26](#)
Windows XP Service Pack 2, [3-26](#)
windowsclientlogfile policy, [7-24](#)
windowscontrolcertificateservice policy, [7-13](#)
windowsskipcdfs policy, [7-39](#)
windowsskiplockedfiles policy, [7-39](#)
winsserver policy, [7-27](#)
World Wid Name
placeholders for, [4-32](#)
writewindowtime policy, [7-27](#)
wwn placeholder, [4-32](#)