

Oracle® Secure Backup

Administrator's Guide



Release 19.1

F89767-01

May 2024

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 Administrator's Guide, Release 19.1

F89767-01

Copyright © 2006, 2024, Oracle and/or its affiliates.

Primary Author: Manish Garodia

Contributing Authors: Aishwarya Minocha, Kathy Rich, Padmaja Potineni, Sarika Surampudi

Contributors: Anand Agrawal, Ashok Joshi, Ashwin Karnik, Basker Vedaraman, Chris Plakyda, Craig B. Foch, Cris Pedregal-Martin, Donna Cooksey, Geoff Hickey, George Claborn, George Stabler, Jack Swan, Janet Stern, Joe Wadleigh, Judy Ferstenberg Panock, Lance Ashdown, Malav Shah, Michael Chamberlain, Paul Gavin, Radhika Vullikanti, Rhonda Day, Roopesh Ashok Kumar, Senad Dizdar, Shailesh Sivasankaran, Steve Wertheimer, Steven Fried, Sumit Chougule, Tammy Bednar, Tony Dziedzic

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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	xv
Documentation Accessibility	xv
Related Documents	xv
Conventions	xvi

Changes in This Release for Oracle Secure Backup Administrator's Guide

Oracle Secure Backup 19.1 Release 1	xvii
-------------------------------------	------

Part I Oracle Secure Backup Concepts

1 Oracle Secure Backup Concepts

Overview of Oracle Secure Backup Features	1-1
Overview of Oracle Secure Backup Administrative Concepts	1-2
About the Administrative Domain	1-3
About the Oracle Secure Backup Catalog	1-4
About Importing Backup Catalog Data from Tape	1-6
About Configuration Files	1-7
About Defaults and Policies	1-7
Classification of Policy Classes	1-7
About Jobs and Requests	1-9
About Job Creation	1-10
About Job Logs	1-12
About Job Transcripts	1-12
About Job Summaries	1-12
About Users and Classes	1-13
About Oracle Secure Backup Daemons	1-13
Types of Daemons	1-13
Daemon Interaction in a File-System Backup	1-16
Overview of Backup Images and Backup Image Instances	1-17

Backup Images	1-17
Backup Image Instances	1-18
Relationship Between Backup Images and Backup Image Instances	1-19
Backup Image Instances and Catalog Data	1-19
Overview of Oracle Secure Backup Media Concepts	1-19
About Backup Containers	1-20
About Backup Sections	1-21
About Volumes	1-21
Backup Image Instances and Volume Labels	1-22
About Volume Sets	1-23
About Disk Pools	1-25
Storage Capacity on Disk Pools	1-25
Space Utilization in Disk Pools	1-26
Disk Pool Orphans	1-26
About Backup Image Instances and Tape Volumes	1-26
Backup Image Instances and Backup Sections	1-27
About Validating Backups by Computing Checksums	1-28
About Data Blocks and Blocking Factors	1-29
About Media Families	1-31
Media Family Attributes	1-31
Volumes in a Media Family	1-33
Volume Sets and Media Families	1-34
Volume Expiration Policies	1-35
About Cloud Storage Devices	1-37
Oracle Secure Backup Using Multipart Upload	1-38
About Client Direct to Cloud	1-39
About Backups in Immutable Buckets	1-40

2 Managing Users and Classes

Overview of Oracle Secure Backup Users	2-1
About Operating System Accounts	2-2
About NDMP Hosts	2-2
About User Configuration	2-3
About Oracle Secure Backup Password Policies	2-3
Overview of Oracle Secure Backup Classes and Rights	2-5
Managing Users	2-6
Displaying the Oracle Secure Backup Web Tool Home Page	2-7
Displaying the Users Page	2-7
Adding a User	2-8
Editing or Displaying User Properties	2-10
Changing a User Password	2-10

Configuring a User in an Administrative Domain	2-11
Assigning Windows Account Information	2-12
Removing a Windows Account	2-12
Assigning Preauthorized Access	2-13
Removing Preauthorized Access	2-14
Renaming a User	2-14
Removing a User	2-14
Managing Classes	2-15
Displaying the Classes Page	2-15
Adding a Class	2-16
Editing or Displaying Class Properties	2-16
Removing a Class	2-17
Renaming a Class	2-17
Managing Defaults and Policies	2-18
Viewing Configured Defaults and Policies Values	2-18
Setting a Policy	2-19
Resetting a Policy	2-19

3 Managing Backup and Media Settings

Overview of Backup and Media Settings Configuration	3-1
Configuring Media Families	3-1
Displaying Defined Media Families	3-3
Adding a Media Family	3-3
Editing or Displaying Media Family Attributes	3-5
Renaming a Media Family	3-6
Removing a Media Family	3-6
Configuring Database Backup Storage Selectors	3-6
Displaying Defined Database Backup Storage Selectors	3-7
Adding a Database Backup Storage Selector	3-7
Editing a Database Backup Storage Selector	3-9
Renaming a Database Backup Storage Selector:	3-10
Removing a Database Backup Storage Selector	3-10
Configuring Job Summary Schedules	3-10
Displaying the Defined Job Summaries Page	3-11
Creating a Job Summary Schedule	3-11
Editing a Job Summary Schedule	3-14
Removing a Job Summary Schedule	3-14
Renaming a Job Summary Schedule	3-15

4 Using Recovery Manager with Oracle Secure Backup

About Recovery Manager and Oracle Secure Backup	4-1
RMAN Environment	4-2
Database Backups	4-3
Types of Backups	4-3
RMAN Backup Sets and Oracle Secure Backup Images	4-3
About RMAN Storage Parameters	4-4
Database Backup Storage Selectors	4-4
Duplexing Backups	4-6
RMAN and Oracle Secure Backup Encryption	4-6
RMAN Backup and Restore Policies	4-7
Database Restore and Recovery	4-8
Interfaces for Managing Database Backup and Recovery	4-8
RMAN Command-Line Client	4-8
Oracle Enterprise Manager Cloud Control	4-8
RMAN and the Oracle Secure Backup Administrative Domain	4-8
How RMAN Accesses Oracle Secure Backup	4-10
Oracle Secure Backup Support for Non-Uniform Memory Access (NUMA)	4-12
Configuring Oracle Secure Backup for Use with RMAN	4-12
Configuring RMAN Access to the Oracle Secure Backup SBT Library	4-13
Creating a Preauthorized Oracle Secure Backup User	4-14
How Oracle Secure Backup Preauthorizes SBT Backups	4-14
Configuring an RMAN Preauthorization	4-16
Creating Media Families for RMAN Backups	4-16
Creating a Database Backup Storage Selector in Enterprise Manager	4-17
Setting Media Management Parameters in RMAN	4-18
Performing Backups with RMAN and Oracle Secure Backup	4-18
Performing Recovery with RMAN and Oracle Secure Backup	4-19
RMAN Backup Metadata in Oracle Secure Backup	4-20
About RMAN and Oracle Secure Backup Metadata	4-20
Expiration of RMAN Backups on Tape	4-21
Displaying RMAN Job Information in Oracle Secure Backup	4-21
Displaying Job Transcripts	4-22
Displaying SBT Errors	4-23
Displaying Backup Piece Information	4-23
Using RMAN and Oracle Secure Backup in an Oracle RAC Environment	4-24
Installing Oracle Secure Backup in an Oracle RAC Environment	4-24

5 Backing Up File-System Data

About File-System Backups	5-1
File-System Backup Types	5-1
Backup Datasets	5-2
Scheduled Backups	5-4
On-Demand Backups	5-4
About Transferring Ownership of Backups	5-5
Restartable Backups	5-5
Preparing to Perform File-System Backups	5-6
Choosing a Backup Strategy	5-6
Choosing a Backup Schedule	5-7
Steps to Perform File-System Backups	5-8
Creating Dataset Files	5-8
Dataset File Examples	5-9
Displaying the Datasets Page	5-10
Adding a Dataset File	5-11
Checking a Dataset File	5-12
Editing a Dataset File	5-12
Renaming a Dataset File	5-13
Removing a Dataset File	5-13
Configuring Backup Windows	5-13
Displaying the Backup Windows Page	5-14
Adding a Backup Window	5-14
Removing a Backup Window	5-15
Configuring Backup Schedules	5-16
Displaying the Schedules Page	5-16
Adding a Backup Schedule	5-16
Editing or Viewing Backup Schedule Properties	5-17
Removing a Backup Schedule	5-18
Renaming a Backup Schedule	5-18
Configuring Triggers	5-19
Displaying the Triggers Page	5-19
Creating a One-Time Backup Trigger	5-20
Creating a Daily Backup Trigger	5-21
Creating a Monthly Backup Trigger	5-23
Creating a Quarterly Backup Trigger	5-24
Creating a Yearly Backup Trigger	5-25
Editing a Trigger	5-26
Removing a Trigger	5-26

Displaying a Trigger Schedule	5-27
Performing Scheduled File-System Backups	5-27
Performing On-Demand File-System Backups	5-28
Steps to Perform On-Demand File-System Backups	5-28
Displaying the Backup Now Page	5-30
Adding an On-Demand Backup Request	5-30
Removing a Backup Request	5-33
Sending Backup Requests to the Scheduler	5-33
Backing Up Critical Data on the Administrative Server	5-34

6 Restoring File-System Data

About File-System Restore Operations	6-1
About Browsing the Oracle Secure Backup Catalog	6-2
Catalog Data Selectors	6-2
Example: Usage of Oracle Secure Backup Data Selectors	6-3
Catalog View Modes	6-4
About Oracle Secure Backup Wildcard Pattern Matching	6-5
Performing a Catalog-Based Restore Operation	6-7
Steps to Perform Catalog-Based File-System Restore Operations	6-7
Displaying the Backup Catalog Page	6-9
Browsing the Backup Catalog Page	6-9
Specifying the Backup Catalog Browse Options	6-10
Specifying the Backup Catalog Search Options	6-11
Creating a Catalog-Based Restore Request	6-11
Removing a Catalog-Based Restore Request	6-13
Sending Catalog-Based Restore Requests to the Scheduler	6-14
Listing All Backups of a Client	6-14
Performing a Raw Restore Operation	6-15
Displaying the Directly From Media Page	6-15
Creating a Raw Restore Request	6-15
Steps to Perform Raw Restore Operations	6-17
Removing a Raw Restore Request	6-19
Sending Raw Restore Requests to the Scheduler	6-19

Part III Managing Operations

7 Managing Backups

Managing Backup Images	7-1
Displaying Backup Images	7-1
Renaming Backup Images	7-2

Managing Backup Image Instances	7-2
Creating Backup Image Instances	7-3
Displaying Backup Image Instances	7-4
Editing Backup Image Instances	7-4
Copying or Moving Backup Image Instances	7-4
Removing Backup Image Instances	7-5

8 Managing Backup Containers

Overview of Managing Backup Containers	8-1
Managing Tape Drives	8-1
Displaying Tape Drive Properties	8-2
Mounting a Volume in a Tape Drive	8-2
Automatically Unloading Volumes	8-3
Managing Tape Libraries	8-4
Displaying the Libraries Page	8-4
Displaying Library Properties	8-5
Displaying Library Volumes	8-5
Running Library Commands	8-5
Updating an Inventory	8-7
Importing a Volume	8-8
Exporting a Volume	8-8
Inserting a Volume	8-9
Extracting a Volume	8-10
Moving a Volume	8-10
Opening a Door	8-11
Closing a Door	8-11
Identifying a Volume	8-11
Loading a Volume	8-12
Unloading a Volume	8-13
Labeling a Volume	8-13
Unlabeling a Volume	8-14
Cleaning a Tape Drive	8-14
Borrowing a Tape Drive	8-14
Returning a Tape Drive	8-15
Reusing a Volume	8-15
Displaying the Error Log	8-15
Managing Disk Pools	8-16
Displaying Disk Pool Properties	8-16
Monitoring Disk Pool Space Utilization	8-16
Moving Disk Pools between Domains	8-17
Moving Disk Pools to a New Hardware Within the Same Domain	8-18

Moving Disk Pools to a New Hardware in a New Domain	8-19
Deleting Expired Backup Image Instances from Disk Pools	8-20
Managing Device Reservations	8-21
Managing Cloud Storage Devices	8-21
Displaying Cloud Storage Device Properties	8-21
Monitoring Cloud Storage Device Space Utilization	8-22
Deleting Expired Backup Image Instances from Cloud Storage Devices	8-22
Enabling Client Direct to Cloud	8-23
Using Immutable Buckets of Oracle Cloud Infrastructure	8-27

9 Managing Backup and Restore Jobs

Overview of Managing Backup and Restore Jobs	9-1
Displaying the Jobs Page	9-1
Displaying Jobs	9-2
Displaying Job Properties	9-4
Displaying Job Transcripts	9-4
Backup Statistics	9-6
Removing a Job	9-8
Running a Job	9-9
Canceling a Job	9-10

10 Performing Maintenance

Managing Volumes	10-1
Displaying the Manage: Volumes Page	10-1
Displaying Volume Details	10-4
Displaying Backup Sections	10-4
Changing Volume Properties	10-6
Duplicating Volumes	10-7
Recalling and Releasing Volumes	10-8
Removing Volumes	10-9
Managing Catalog Imports	10-10
Displaying the Catalog Imports Page	10-10
Importing and Cataloging Backups	10-10
Importing Backup Catalog Data from Disk	10-11
Importing Backup Catalog Data from Tape	10-11
Managing Checkpoints	10-12
Displaying the Checkpoints Page	10-12
Removing a Checkpoint	10-12
Managing Daemons	10-13
Displaying the Daemons Page	10-13

Performing Daemon Operations	10-14
Viewing Daemon Properties	10-15
Suspending and Resuming Job Dispatching	10-15

Part IV Advanced Topics

11 Vaulting

Overview of Vaulting	11-1
About Locations	11-2
About Rotation Policies	11-2
About Vaulting Scans	11-3
About Media Movement Jobs	11-3
About Reports	11-3
Location Report	11-4
Schedule Report	11-4
Pick Report	11-4
Distribution Report	11-4
Exception Report	11-5
Missing Volumes Report	11-5
About The Vaulting Process	11-5
About Volume Duplication	11-6
About Volume Duplication Policies	11-6
About Volume Duplication Schedules	11-7
About Volume Duplication Jobs	11-7
About Volume Duplication Widows	11-8
About NDMP Copy-Enabled Virtual Tape Library	11-8
Setting Up a Vaulting Environment	11-9
Adding Locations	11-9
Adding Rotation Policies	11-11
Associating Rotation Policies with Media Families	11-14
Adding a Vaulting Scan Schedule	11-15
Performing an On-Demand Vaulting Scan	11-18
Running Media Movement Jobs	11-19
In-Transit Flags	11-21
Minimum Writable Volumes	11-22
Ejecting Volumes from Libraries	11-23
Automatic Library Ejection	11-23
On Demand Library Ejection	11-24
Manual Library Ejection	11-24
Viewing Location Reports	11-26

Recalling a Volume	11-26
Releasing a Volume	11-27
Viewing Pick and Distribution Reports	11-28
Adding Volume Duplication Policies	11-29
Associating Volume Duplication Policies with Media Families	11-31
Adding Volume Duplication Windows	11-32
Adding Volume Duplication Schedules	11-33
Running Volume Duplication Jobs	11-34
Volume Duplication Job Failures	11-35
On-Demand Volume Duplication	11-36
Exporting Duplicate Volumes to Another Domain	11-36
NDMP Volume Duplication	11-37
Tracking Volumes Through a Vaulting Environment	11-37
Managing an Existing Vaulting Environment	11-38
Managing Locations	11-39
Editing or Viewing the Properties of a Storage Location	11-39
Removing a Storage Location	11-40
Renaming a Storage Location	11-40
Managing Rotation Policies	11-41
Editing or Viewing the Properties of a Rotation Policy	11-41
Removing a Rotation Policy	11-42
Renaming a Rotation Policy	11-42
Managing Rotation Policy/Media Family Associations	11-42
Managing Vaulting Scan Schedules	11-43
Editing or Viewing the Properties of a Vaulting Scan Schedule	11-43
Removing a Vaulting Scan Schedule	11-44
Renaming a Vaulting Scan Schedule	11-44
Managing Volume Duplication Policies	11-45
Editing or Viewing the Properties of a Volume Duplication Policy	11-45
Removing a Volume Duplication Policy	11-45
Renaming a Volume Duplication Policy	11-46
Managing Volume Duplication Policy and Media Family Associations	11-46
Managing Volume Duplication Windows	11-47
Managing Volume Duplication Schedules	11-47
Editing or Viewing the Properties of a Volume Duplication Schedule	11-48
Removing a Volume Duplication Schedule	11-48
Renaming a Volume Duplication Schedule	11-48
Changing Global Vaulting Policies	11-49
Changing Global Volume Duplication Policies	11-50
Recovery Manager and Vaulting	11-51
Troubleshooting Vaulting	11-54
Misplaced Volumes	11-54

Volumes Outside Their Rotation Policies	11-55
Viewing Exception Reports	11-55

12 Managing Backup Encryption

Overview of Backup Encryption	12-1
Types of Backup Encryption	12-2
About Backup Encryption Policies	12-2
About Backup Encryption Setting Levels	12-3
About Backup Encryption Options	12-3
About Backup Encryption Algorithms	12-4
About Backup Encryption Security Control	12-4
About Backup Encryption Key Management	12-4
About Backup Encryption for File-System Backups	12-5
About Backup Encryption for Oracle Database Backups	12-5
Overview of Software-Based Encryption	12-7
About Transient Backup Encryption	12-7
Overview of Hardware-Based Encryption	12-7
About Hardware-Encrypted Transient Backups	12-8
About Hardware Encryption Reports and Logging	12-9
About Hardware Encryption Algorithm	12-9
About Hardware Encryption Policies	12-10
Example: Performing a One-Time Unencrypted Backup	12-10
Example: Performing Day-to-Day Backup Encryption	12-11
Example: Performing Transient Backup Encryption	12-12
Enabling Backup Encryption	12-12
Enabling Encryption for the Administrative Domain	12-12
Enabling Encryption for a Client	12-13
Encrypting Data for Backups	12-14
Enabling Encryption for a Scheduled Backup	12-14
Enabling Encryption for an On-Demand Backup	12-14
Enabling Transient Backup Encryption	12-14
Enabling Hardware Encryption	12-14

13 Disaster Recovery of Oracle Secure Backup Administrative Data

Overview of Catalog Recovery Concepts	13-1
About Catalog Recovery Schedule Object	13-2
About Catalog Recovery Media Family Object	13-2
About Catalog Recovery Dataset Object	13-3
About Catalog Recovery Summary Object	13-3
Overview of Catalog Backup Jobs	13-4

Recovering the Oracle Secure Backup Administrative Domain	13-4
Restoring the Oracle Secure Backup Catalog in a Tape Domain	13-5
Preparing to Restore the Oracle Secure Backup Catalog	13-5
Making the Administrative Domain Operational	13-11
Restoring the Oracle Secure Backup Catalog in a Disk Pool Domain	13-12

14 Staging

About Staging	14-1
About the Oracle Secure Backup Default Stage Rule	14-3
Setting Up Staging	14-4

A NDMP Special Characteristics

NDMP and IPv6	A-1
NDMP and Constrained Error Reporting	A-1
Limitations Using Network Appliances Data ONTAP	A-1

Glossary

Index

Preface

This preface contains these topics:

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

Audience

This book is intended for system administrators and database administrators who manage backup and restore of file-system data or Oracle databases using 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 about using Oracle Secure Backup, see the following Oracle resources:

- *Oracle Secure Backup Installation and Configuration Guide*
This book explains how to install, upgrade and uninstall Oracle Secure Backup on different platforms, and Oracle Secure Backup administrative domain management and network security concepts and tasks.
- *Oracle Secure Backup Reference*

This book describes the commands supported by the `obtool` command line client, defaults and policies used to configure Oracle Secure Backup, the language used to create datasets that specify backup targets, and user classes and rights.

For more information about database backup and recovery, including the Recovery Manager (RMAN) utility, see the following Oracle resources:

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

This guide covers Oracle database backup and recovery techniques, both with Recovery Manager and user-managed backup and recovery.

The Oracle Secure Backup product Web site is located at the following URL:

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

See the product Web site for a direct link to the Oracle Secure Backup product download site.

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 Administrator's Guide

This section highlights new features, fixes, and enhancements in Oracle Secure Backup for the current release.

Oracle Secure Backup 19.1 Release 1

The following are the changes in this document for Oracle Secure Backup 19.1.

New Features, Enhancements, and Updates

- Supports immutable buckets feature of Oracle Cloud Infrastructure.
This feature enables Oracle Secure Backup to store backups in object storage and archive storage but prevents any modification or deletion of data. You can apply retention rules on these buckets to protect your data.
See [About Backups in Immutable Buckets](#) and [Using Immutable Buckets of Oracle Cloud Infrastructure](#).
- Upload backups from client host directly to the Oracle Cloud Infrastructure object storage.
Oracle Secure Backup provides a new feature for uploading backups from client hosts to the Oracle Cloud Infrastructure object storage. With this feature, a client host can upload backup data directly to object storage without using media servers, thereby improving throughput of backup jobs.
See [About Client Direct to Cloud](#) and [Enabling Client Direct to Cloud](#).

Deprecated Functionality

- Support for physical tape drives and libraries, including VTLs emulating libraries and tape drives is deprecated. These may not be supported in future releases of Oracle Secure Backup.
- Support for administrative server and media server on non-Linux platforms is deprecated. Future releases of Oracle Secure Backup will support administrative server and media server only on Linux platform.
- Support for Oracle Secure Backup client will continue on all platforms, that is, Linux, Solaris, Windows, HP-UX, and AIX.

Desupported Functionality

The Oracle Secure Backup 19.1 software is not interoperable with Oracle Secure Backup 12.2 and earlier version clients.

Other Changes

Minor editorial changes to this section for language and grammar improvements.

- [Overview of Hardware-Based Encryption](#)

Part I

Oracle Secure Backup Concepts

This part provides an architectural and conceptual overview of Oracle Secure Backup.

This part contains these chapters:

- [Oracle Secure Backup Concepts](#)
- [Managing Users and Classes](#)
- [Managing Backup and Media Settings](#)

1

Oracle Secure Backup Concepts

This chapter introduces concepts related to backup and recovery using Oracle Secure Backup.

This chapter contains these sections:

- [Overview of Oracle Secure Backup Features](#)
- [Overview of Oracle Secure Backup Administrative Concepts](#)
- [Overview of Oracle Secure Backup Media Concepts](#)

Overview of Oracle Secure Backup Features

Oracle Secure Backup is a centralized, network based backup management application that backs up both Oracle Databases and file-system data across most popular Linux, Unix, and Windows operating systems. Oracle Secure Backup acts as a [SBT interface](#) for use with [Recovery Manager \(RMAN\)](#). Oracle Secure Backup has ongoing support added for most major brand tape drives and libraries in [Storage Area Network \(SAN\)](#) and [SCSI](#) environments. A current list of supported hardware is available at the following URL:

<http://www.oracle.com/technetwork/database/database-technologies/secure-backup/learnmore/index.html>

Oracle Secure Backup enables you to do the following:

- Centrally manage backup and restore operations of distributed, mixed-platform environments to tape, disk pool, and cloud storage devices.

You can access local and remote file systems and any [tape device](#) from any location in a network without using [Network File System \(NFS\)](#) or [Common Internet File System \(CIFS\)](#).

See Also:

Oracle Secure Backup Installation and Configuration Guide for information on supported computer architectures

- Back up to and restore data from Oracle Cluster File System (OCFS) on Linux and Windows
- Enables efficient utilization of storage resources

You can initially store your backups to disk and periodically move them to tape devices thus reducing contention caused by writing backups only to tape devices.

- Encrypt all stored data

See Also:

[Managing Backup Encryption](#)

- Use wildcards and exclusion lists to specify what you want to back up
- Perform a multilevel [incremental backup](#)
- Duplex database backups so that the same data stream goes to multiple devices
You can specify a different [media family](#), tape device, or [disk pool](#) for each copy of the data.
- Create backups that span multiple volumes
A [volume](#) is a unit of media, such as an LTO5 tape cartridge.
- Optimize tape resources with automatic tape drive sharing
- Restore data rapidly
Oracle Secure Backup uses direct-to-block positioning and direct access restore to avoid unnecessarily reading tape blocks to locate files. Oracle Secure Backup maintains a record of the tape position of all backup data in its [catalog](#) for rapid retrieval.
- Maintain security and limit the users who are authorized to perform data management operations
By default, [Secure Sockets Layer \(SSL\)](#) is used for [host authentication](#) and communication in the [administrative domain](#).
- Manage media rotation from one [location](#) to another
- Automate tape duplication with user-defined policies
- Temporarily use a disk pool as an interim container for a backup image that is ultimately destined to be written to another container, usually tape. See [Copying or Moving Backup Image Instances](#).
- Back up data to Oracle Cloud Infrastructure Object Storage Classic by configuring individual containers as cloud storage devices. See Oracle Secure Backup Installation and Configuration Guide.
- Compress backup data, choosing from various levels of compression based on the desired compression ratio, backup speed, and computing resources available. Compression requirements can be set at the backup job level, host level, or domain level. For more information, see *Oracle Secure Backup Reference* for a description of the `--compression` option of the `backup` command.

Overview of Oracle Secure Backup Administrative Concepts

Oracle Secure Backup manages the backup and restore operations for heterogeneous environments by organizing the host computers into an administrative domain. The administrative domain consists of one administrative server, one or more media servers, and one or more clients.

After you create a request for a backup or restore operation, Oracle Secure Backup creates a job corresponding to this request when the request is eligible to run. Information about each job is maintained in job logs, job transcripts, and job summaries.

You can use configuration settings called policies to manage the operations in the administrative domain. Policies are maintained on the administrative server. Defaults enable you to provide default values for a configuration setting.

Oracle Secure Backup maintains a consistent user identity across the administrative domain by storing information about users, rights, and classes. You can grant individual rights to users or assign a class, which is a named set of rights. Oracle Secure Backup provides a set of preconfigured classes.

This section contains the following topics:

- [About the Administrative Domain](#)
- [About the Oracle Secure Backup Catalog](#)
- [About Configuration Files](#)
- [About Defaults and Policies](#)
- [About Jobs and Requests](#)
- [About Users and Classes](#)
- [About Oracle Secure Backup Daemons](#)

About the Administrative Domain

The **administrative domain** is a network of hosts that are managed as a common unit to perform backup and restore operations. Each host in the administrative domain must be assigned one of the following roles:

- **Administrative server**
The administrative server contains configuration information about all hosts in the domain. It also stores the backup catalog that contains metadata about the backup and restore operations. You can have only one administrative server in an administrative domain.
- **Media server**
A media server is a host that has secondary storage devices attached to it. It manages the movement of data to and from the secondary storage devices. Media servers can be directly attached to SAN-attached disk pools or tape drives that are either standalone or contained in tape libraries.
- **Client**
Any host in the administrative domain containing data that needs to be backed up is referred to as a client. Clients can include Oracle Databases and file-system data, they can be NDMP NAS servers, Linux, Unix, or Windows hosts. The administrative server can also act as a client if its data is backed up.

Hosts can be assigned multiple roles in an administrative domain. A media server can also act as a client because it contains an Oracle Database that needs to be backed up. Data that needs to be backed up can exist either on the client or on media servers.



See Also:

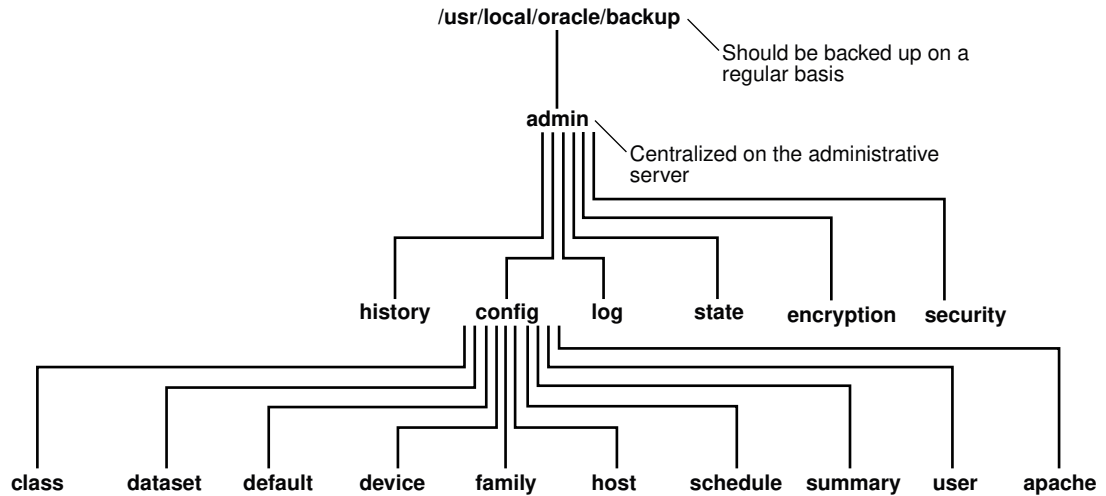
Oracle Secure Backup Installation and Configuration Guide for more information about and examples of the administrative domain

Oracle Secure Backup Home: Directory Structure

Oracle Secure Backup organizes information about the administrative domain as a hierarchy of files in the [Oracle Secure Backup home](#) on the [administrative server](#). The Oracle Secure Backup Home directory is the install location for the software. The files which define the administrative domain, are organized in a structured hierarchy on the administrative server in the Oracle Secure Backup Home directory.

Figure 1-1 shows the directory structure of an Oracle Secure Backup home. This directory structure is the same for all platforms, but the default Oracle Secure Backup home is `/usr/local/oracle/backup` for UNIX and Linux and `C:\Program Files\Oracle\Backup` for Windows.

Figure 1-1 Directories on the Administrative Server



About the Oracle Secure Backup Catalog

The administrative server maintains a [catalog](#) in which it stores metadata relating to backup and restore operations for the administrative domain. You can use `obtool` or the Web tool to browse the catalog to review what you have backed up and search for items to restore.

The Oracle Secure Backup catalog is integrated to share backup metadata with RMAN, but is separate from the [RMAN recovery catalog](#). The RMAN recovery catalog is stored as an Oracle Database file and is maintained independently by RMAN.

When Oracle Secure Backup performs a file-system backup or a database backup through the SBT, it records the name and attributes of the objects it backs up. It writes this data to the catalog stored on the administrative server. It also stores information about the [backup image instances](#) that are associated with each [backup image](#).



See Also:

["Database Backups"](#)

Backup Catalog: Directory Structure

Oracle Secure Backup maintains a discrete backup catalog for every client in the administrative domain. The catalog for each host is stored in a subdirectory of `admin/history/host` named after the client. For example, `admin/history/host/brhost2` stores the catalog for the client named `brhost2`. The catalog itself is a binary file named `indices.cur`.

When Oracle Secure Backup acts in the role of the SBT media manager for RMAN backups, piece data is stored in database files located in the directory `admin/state/general/` called `sbtpiece.dat` and `sbtpiece.idx`.

 **See Also:**

"[Overview of Oracle Secure Backup Classes and Rights](#)" for more information about user [rights](#)

When you browse the 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. At the root of the file system appears a fictitious directory, called the [super-directory](#), that contains all files and directories saved from the top-most file-system level. Oracle Secure Backup uses this directory as a starting point from which you can access every top-level file-system object stored in the catalog.

The catalog super-directory usually contains only the root directory on UNIX and Linux systems. On Windows systems, it contains each top-level file system that you backed up, each identified by a drive letter and a colon.

The Oracle Secure Backup catalog contains a record of each file-system object saved in each backup. Directories come and go and their contents change over time. For example, the name of an object backed up yesterday as a directory might refer to a file in a backup today and a symbolic link in a backup tomorrow. Oracle Secure Backup tracks all such changes in object types properly.

The Oracle Secure Backup [catalog](#) contains backup-related information. The `admin/history/host` directory contains subdirectories named after the hosts in the administrative domain. Each subdirectory has a file in which the catalog data is stored. Oracle Secure Backup supports catalog files larger than 2 GB. This support is restricted to operating systems and file systems that themselves support files of over 2 GB.

The amount of space consumed by the catalog is different for native and NDMP hosts. The sum of the following three components gives an estimate in bytes for expected growth of the catalog for a native Oracle Secure Backup backup:

- (number of new files and directories) * (43 + average file leaf name length)
- (number of modified existing files) * (27 bytes for statistics record)
- (number of unmodified existing files) * 0.5

The sum of the following three components gives an estimate in bytes for expected growth of the catalog when backing up a third-party NDMP filer:

- (number of new files and directories) * (53 + average file leaf name length)
- (number of modified existing files) * (35 bytes for statistics record)
- (number of unmodified existing files) * 0.5

An NDMP backup also consumes 16 bytes in the NDMP position file for every file backed up regardless of whether it is new, modified, or unmodified.

 **Note:**

Oracle Secure Backup makes a temporary copy of the catalog during the processing of a backup. Planning for storage space on the Oracle Secure Backup administrative server must take the temporary copy and catalog updates into consideration.

Oracle Secure Backup automates the protection of the contents of the catalog and configuration files. During installation, Oracle Secure Backup schedules the necessary [backup job](#) to back up these files to a backup container. If the catalog data is lost, for example because a disk fails, then you can restore the most recently backed up catalog and then restore the rest of your data.

In general, you should access configuration data and the catalog through [obtool](#) or the Oracle Secure Backup [Web tool](#). Avoid accessing the files containing this data directly on the file system.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for details on the contents of the files and directories in the Oracle Secure Backup home

About Importing Backup Catalog Data from Tape

Oracle Secure Backup supports importing and cataloging backups from tape using the `importvol` and `obtar` commands. The catalog on tape feature makes this process more efficient.

As of Oracle Secure Backup 12.1, you can import and catalog backups from tape into your Oracle Secure Backup domain through a much faster process. As a result, you can browse the Oracle Secure Backup catalog and select files for restore from volumes that were previously not known to the current administrative domain. [Example 1-1](#) explains how to import and catalog a volume.

As a result of cataloging the volume, you can now view the information about the backup as though it had been originally created in the current domain.

 **See Also:**

- *Oracle Secure Backup Reference* for more information about the `importvol` and `obtar` commands
- "[Managing Catalog Imports](#)" for more information about how to import and catalog backups

About Catalog Import Encryption

As a part of [import catalog](#), you can import file information from tape into the Oracle Secure Backup domain without an encryption key. However, it is mandatory to have an encryption key while performing the restore operation.

To obtain the encryption key for a new Oracle Secure Backup domain, you must specify the `passphrase` option while performing restore. This option stores the restore passphrase for all future restore operations.

 **See Also:**

Oracle Secure Backup Reference for more information about the `restore` command options

Example 1-1 Cataloging a Volume

In this example, Oracle Secure Backup scans the tape drive `vt1` and catalogs the volume with the volume ID `VOL000001`. This example assumes that all volumes in the volume set are a part of the Oracle Secure Backup volumes database.

```
ob> catalog --vid VOL000001 --drive vt1
Info: catalog import request 1 submitted; job id is admin/21.
```

About Configuration Files

Oracle Secure Backup administrative data includes domain-wide entities related to backups. These include users, classes, tape devices, disk pools and media families. [Figure 1-1](#) shows the `config` directory which contains several subdirectories, each of which represents an object that defines the administrative domain. Each object directory contains Oracle Secure Backup files describing the object's characteristics.

About Defaults and Policies

Oracle Secure Backup [defaults and policies](#) are configuration settings that determine the way an Oracle Secure Backup operates administrative domain will function. Policy settings are maintained on the administrative server. The policy defaults are set conservatively and are sufficient to maintain security and protect data on most corporate networks. But if you have special requirements, environments, or backup strategies, then it is recommended that you review these settings during install to confirm that they meet your requirements.

Oracle Secure Backup policies are grouped into several classes. Each policy class contains parameters related to a particular aspect of Oracle Secure Backup operations.

 **Note:**

Do not confuse policy classes, which are only an organizational convenience, with user classes.

Classification of Policy Classes

Policy classes related to managing Oracle Secure Backup backup and restore functions are as follows:

- Backup compression Policies
These policies, if set, control the compression related settings of file system backups on Oracle Secure Backup clients if compression is not set at the host or job level.
- Backup encryption policies

These policies control the encryption of backups written to a backup container. For example, you can specify whether encryption of backups is mandatory, key size, and aspects of key management.

- Cloud Policies

These policies control the behavior of various operations when the target is a cloud storage device.

- Copy backup image instance policies

These policies control how [backup image instance](#) copies are created. For example, you can specify a default priority for copy instance jobs.

- 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.

- Device Policies

These policies control how backup containers are automatically detected during device discovery. They also control when tape device write warnings are generated.

- Duplication policies

These policies control how Oracle Secure Backup performs volume duplication. For example, you can control whether duplication should be performed over the network or only on one local host.

- 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.

- 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 on.

- Media policies

These policies control media management for the administrative domain. For example, you can choose whether tapes are required to have [barcode](#) labels and set the [retention period](#) and [write window](#) for volumes in the default [media family](#).

- Naming policies

This class contains one policy which specifies the IP address of an Windows Internet Name Service (WINS) Server for the administrative domain.

- NDMP policies

These policies control settings applicable to hosts that use [NDMP access mode](#) and specify NDMP defaults. For example, you can configure backup environment variables, specify a user name for authentication, or specify a password used to authenticate Oracle Secure Backup to each NDMP server.

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.

- Operations policies

These policies control various backup and restore operations. For example, you can set the amount of time that an RMAN [backup job](#) waits in the Oracle Secure Backup [scheduler](#) queue for the required resources to become available.

- Scheduler policies

These policies control the behavior of the Oracle Secure Backup scheduler. For example, you can specify a frequency at which the scheduler attempts to dispatch backup jobs.

- Security policies

These policies control aspects of administrative domain security. For example, you can enable [SSL](#) encryption for backup data in transit or set the host identity [certificate](#) key size. *Oracle Secure Backup Installation and Configuration Guide* explains how to change the default security policies.

- Staging policies

These policies control aspects of stagescan jobs.

- Vaulting policies

These policies control media management, which includes the rotation of tapes from one location to another as part of a data protection strategy.

 **See Also:**

Oracle Secure Backup Reference for more information about Oracle Secure Backup policies

About Jobs and Requests

In Oracle Secure Backup, a backup or restore request is distinct from a job. A request is a locally-stored specification of a backup or restore operation that is not yet eligible to run. A job is a request that has been forwarded to the Oracle Secure Backup scheduler and is eligible to be run.

Scheduler policies determine how the scheduler handles backup and restore jobs. You should familiarize yourself with these settings because they determine the frequency with which the scheduler dispatches jobs.

 **Note:**

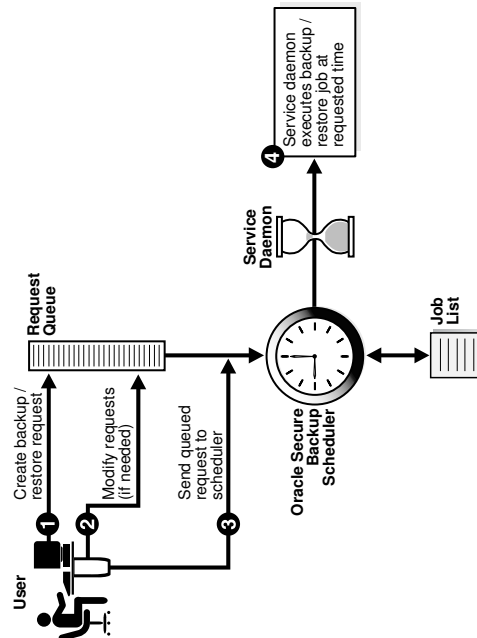
This section describes file-system backup and restore jobs. To learn about database backup and restore jobs, see "[How RMAN Accesses Oracle Secure Backup](#)".

 **See Also:**

- [About Defaults and Policies](#) for a description of scheduler policies.

[Figure 1-2](#) shows the process by which an Oracle Secure Backup user can create an [on-demand backup](#) or restore job.

Figure 1-2 Backup and Restore Requests and Jobs



The steps in the process illustrated in [Figure 1-2](#) are as follows:

1. A user creates a file-system backup or restore request. For example, the user submits a request for a backup of the `/home` directory of client host `brhost2`.

Oracle Secure Backup maintains a queue of backup and restore requests in the user's Oracle Secure Backup Web tool or `obtool` session. The user can review or modify this queue. When the user terminates the session, requests that are not yet sent to the scheduler are lost.
2. If necessary, the user modifies the requests in the queue. For example, the user can delete a job request.
3. The user sends the backup request to the scheduler (`obscheduled`) running on the administrative server.

When a user sends a file-system backup or restore request to the Oracle Secure Backup scheduler, the request becomes a job. Oracle Secure Backup assigns each job a name that is unique among all jobs in the administrative domain.
4. At the scheduled time, the service daemon runs the job.

About Job Creation

This section provides a more detailed explanation of how on-demand and scheduled file-system backup and restore jobs are created. The following events cause Oracle Secure Backup to create jobs:

- Oracle Secure Backup inspects each [trigger](#) defined in each backup schedule every five minutes by default. For each trigger that fires that day, Oracle Secure Backup creates one job for each [dataset](#) listed in the schedule.

 **Note:**

You can change the frequency with which the scheduler inspects triggers by specifying a different value for the scheduler `applybackupsfrequency` policy.

 **See Also:**

- ["Configuring Triggers"](#)
- *Oracle Secure Backup Reference* for information on scheduler defaults and policies

In job descriptions, Oracle Secure Backup identifies this as a dataset job. It assigns the scheduled dataset job a numeric job identifier such as 15.

- Each time you create an on-demand request and then click **Go** or use the `backup --go` command in `obtool` to send your request to the scheduler, Oracle Secure Backup creates a dataset job. It assigns the job an identifier prefixed by the user who runs the command, for example, `admin/15`.
- At the scheduled start time for a dataset job, Oracle Secure Backup reads the dataset and then creates one subordinate job for each host it includes.

In job descriptions, Oracle Secure Backup calls this a backup job. 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. For example, `15.1` could be a subordinate job for scheduled job 15.

- Each time you explicitly request that Oracle Secure Backup restore data and then click **Go** or use the `restore --go` command in `obtool` to send your request to the scheduler, Oracle Secure Backup creates a restore job for each [backup image instance](#) that must be read to initiate the restore operation. Oracle Secure Backup assigns each job an identifier such as `admin/15`.

If Oracle Secure Backup creates multiple jobs to satisfy one restore request, then it marks each job except the first as dependent on the success of the previous job. The effect of this notation is that, given the failure of a job on which a later job is dependent, that later job is also marked as failed.

After the earliest time to run a job has arrived, the next criterion used by the scheduler to determine which job to run next is the user-assigned schedule priority. The scheduler dispatches jobs in order of their priority to all available resources and then waits for resources to become available and continues to dispatch the jobs. The job with the lowest numeric schedule priority corresponds with the highest actual job priority and will be dispatched first.

 **See Also:**

["Performing On-Demand File-System Backups"](#) and ["Configuring Backup Schedules"](#)

About Job Logs

Oracle Secure Backup keeps a log for each job. This log describes high level events such as the creation, dispatch, and completion times of the job. You can view the log through both the Oracle Secure Backup Web tool and `obtool`.



See Also:

["Displaying Job Properties"](#)

About Job Transcripts

Oracle Secure Backup maintains a running transcript for each job. The transcript of a job describes the details of its 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 using the transcript.



See Also:

["Displaying Job Transcripts"](#)

About Job Summaries

A [job summary](#) is a text file report produced by Oracle Secure Backup that describes the status of selected file-system backup and restore jobs. Each report contains four sections, distinguished by job status:

- Jobs eligible to be performed now (but not yet started)
- Jobs running now
- Jobs completed successfully
- Jobs canceled, superseded, or failed

You can create a [job summary schedule](#), which enables Oracle Secure Backup to generate multiple summary reports, each covering different time periods or activities. When you create a job summary schedule, you can choose the following options:

- A unique name for the job summary
- The dates on which Oracle Secure Backup produces the job summary
- Users to whom the job summary is e-mailed
- The beginning of the time period spanned by the job summary
The end time is always the summary generation time.
- The contents of the job summary



See Also:

["Configuring Job Summary Schedules"](#)

About Users and Classes

Oracle Secure Backup provides user-level access control through users and classes. Information about users and classes is stored on the administrative server. An Oracle Secure Backup user is an entity who has the same identify across the administrative domain. You can use classes to grant the privileges that the user requires to perform backup, recovery, or administrative operations. A class is a named collection of rights that can be granted to Oracle Secure Backup users.

Oracle Secure Backup contains a set of predefined classes. When you install Oracle Secure Backup, the `admin` user is automatically created and is assigned the predefined `admin` class. You can create additional Oracle Secure Backup users and assign the required classes or operating system privileges to users. You can also define your own class and assign rights to this class.



See Also:

[Managing Users and Classes](#)

About Oracle Secure Backup Daemons

Oracle Secure Backup [daemons](#) are background processes that perform Oracle Secure Backup operations. Some daemons run continually, whereas others run only to perform specific work and then exit when they have finished.



Note:

On the Windows operating system, only the [service daemon](#) is a Windows service. The other Oracle Secure Backup daemons are not Windows services.

This section contains these topics:

- [Types of Daemons](#)
- [Daemon Interaction in a File-System Backup](#)

Types of Daemons

An Oracle Secure Backup administrative domain uses a variety of daemons to perform backup, restore, and configuration tasks. The daemon programs are located in the `etc` subdirectory of the Oracle Secure Backup home on Linux or UNIX, and in the `bin` directory on Windows. This section describes the Oracle Secure Backup daemons.

[Table 1-1](#) lists the Oracle Secure Backup daemons and shows on which hosts they run.

Table 1-1 Oracle Secure Backup Daemons by Host Type

Daemon	Administrative Server	Media Server	Client
Service	yes	yes	yes
Schedule	yes	no	no
Index	yes	no	no
Apache Web Server	yes	no	no
NDMP	yes	yes	yes
Pool Manager	yes	no	no
Robot	no	yes	no
Proxy	no	no	yes

This section contains these topics:

- [Service Daemon](#)
- [Schedule Daemon](#)
- [Index Daemon](#)
- [Apache Web Server Daemon](#)
- [NDMP Daemon](#)
- [Robot Daemon](#)
- [Pool Manager Daemon](#)
- [Proxy Daemon](#)

Service Daemon

The `observed` [service daemon](#) provides a wide variety of services. It runs continually on the administrative server, [media server](#), and [client](#).

On the administrative server, `observed` runs jobs at the request of the schedule daemon, cleans up log files and transcripts, and provides access to Oracle Secure Backup configuration data to other hosts in the domain. `observed` also serves as the [Certification Authority \(CA\)](#), accepting [certificate](#) signing requests from hosts within the administrative domain and sending signed certificates back to the requesting host. `observed` starts the schedule daemon and the [Apache Web server](#) during initialization.

When running on a media server or client, `observed` handles membership in a administrative domain, allows for remote administration of the host, and handles certificate operations. The [identity certificate](#) of the requesting host is used to verify that it is permitted to invoke the operation.

On all hosts, the service daemon is usually started as part of system startup. On UNIX and Linux, startup is usually performed through entries in `/etc/init.d`, whereas on Windows systems the service is started by the Service Control Manager.

Schedule Daemon

The `obscheduled` daemon is the Oracle Secure Backup [scheduler](#). The schedule daemon runs continually on the administrative server.

The schedule daemon manages each [scheduled backup](#), retains a list of every available [backup container](#) in the domain, and assigns backups to tape devices as they become available. The daemon receives job creation requests from obtool users and from the SBT interface in response to RMAN commands.

Scheduler policies control how a [backup request](#) is scheduled.

Index Daemon

The `obixd` daemon manages the backup catalog for each client. The index daemon runs intermittently on the administrative server.

The index daemon is started at the conclusion of any backup to import the index data generated by `obtar` into the backup catalog. In addition, `obixd` is started when the catalog must be accessed for restore or browsing operations.

Apache Web Server Daemon

The `obhttpd` daemon provides the Web tool for Oracle Secure Backup. This daemon runs continually on the administrative server.

The Web server daemon is signaled to start by the `observiced` daemon, which itself is normally started as part of system startup.

NDMP Daemon

The `obndmpd` daemon implements the [NDMP tape service](#) and provides data communication between the media server and client. This daemon runs on both the client and media server. It passes control of the data connection to a sub-process so it can remain free to respond to control messages sent by `obtar`.

Two instances of `obndmpd` run during an active backup or restore operation. If the same host is acting as both the media server and the client, then three instances of `obndmpd` are running: one acting as controller, one acting as the [data service](#), and one acting as the mover.

Robot Daemon

The `obrobotd` daemon manipulates tapes in a tape library. This daemon runs intermittently on a media server.

When an Oracle Secure Backup component such as `obtar` must interact with a tape library, it asks `observiced` on the media server to start an instance of `obrobotd`. The robot daemon then fields all requests for inventory manipulations, the movement of media in the tape library, and so on. Each invocation of `obrobotd` manages a single tape library. `obrobotd` exits when all users of a tape library have closed their connections.

Pool Manager Daemon

The `obpoolmgr` daemon manages the contents of [disk pools](#). It runs continuously on the administrative server.

The `obpoolmgr` daemon deletes expired [backup image instances](#), monitors disk pool space usage, and interacts with `obtar` when the disk pool runs out of space during a backup operation. Backup image instances are not deleted at the time they expire. They are deleted when the free space in the disk pool falls to below the threshold specified for the disk pool.

Proxy Daemon

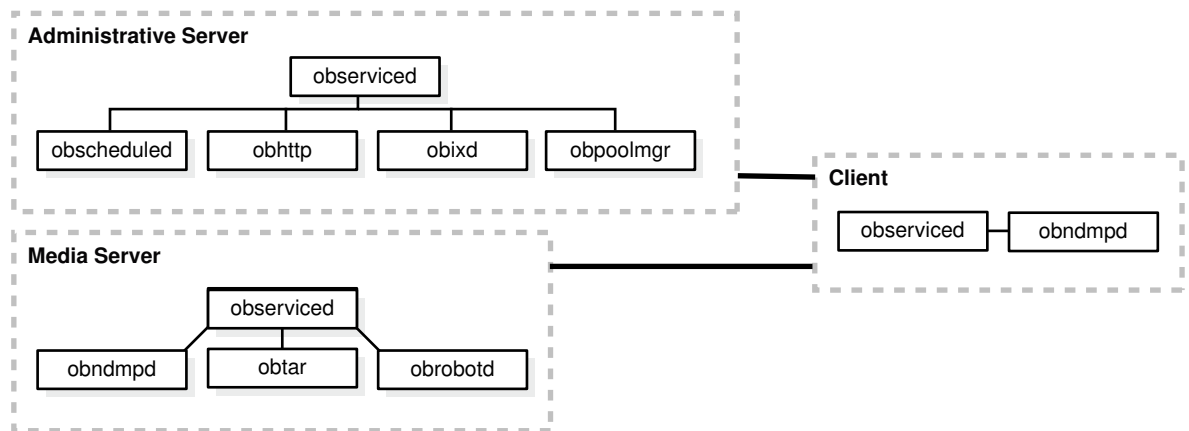
The `obproxyd` daemon verifies user access for SBT backup and restore operations. The proxy daemon runs on the host that contains the SBT library accessed during the operations. The invocation of the proxy daemon is platform-specific.

The proxy daemon uses the operating system user identity of the process invoking the SBT library and the local host name to determine the Oracle Secure Backup account to use for the backup operation. If a [preauthorization](#) exists for this operating system user and host, then the associated [Oracle Secure Backup user](#) is permitted to perform RMAN backups and the login to Oracle Secure Backup is permitted.

Daemon Interaction in a File-System Backup

The following figure provides a simplified graphical illustration of the relationships among the daemons on an administrative server, media server, and client.

Figure 1-3 Daemons in an Administrative Domain



The media server in the figure shows an `obtar` instance, but `obtar` is not itself a daemon. It is the underlying Oracle Secure Backup engine that manipulates the data, tape services, and [disk pools](#) during a backup or restore operation. When you issue commands in `obtool` or the Oracle Secure Backup Web tool, Oracle Secure Backup translates them internally to `obtar` commands.

Imagine that `observed` daemons run on all hosts, the `observed` daemon on the administrative server has invoked the `obscheduled` and `obhttpd` daemons, and a client file-system backup job has been created and scheduled to run. The Oracle Secure Backup daemons interact with `obtar` as follows:

1. On the administrative server, `obscheduled` sends a request to `observed` to run the backup job.
2. `observed` on the administrative server sends a request to `obrobotd` on the media server to mount each volume required for the backup job.
3. `observed` on the administrative server sends a request to `observed` on the media server to invoke `obtar`.

4. `obtar` on the media server establishes a data connection between the `obndmpd` daemon on the client and the `obndmpd` daemon on the media server. Backup data is transmitted over the data connection and written to a backup container.
`obtar` usually runs on the media server. If the media server is not running Oracle Secure Backup software, then `obtar` runs on the administrative server. An example of a media server not running Oracle Secure Backup is an NDMP-based [filer](#).
5. `obtar` sends catalog information to `obixd` on the administrative server and then terminates.
6. On the administrative server, `observiced` sends a job status update to `obscheduled`.


Overview of Backup Images and Backup Image Instances

A [backup image](#) is a set of data that comprises the product of one backup operation. A [backup image instance](#) contains the actual backup data.

When a backup operation is started, Oracle Secure Backup creates the following:


- backup image

A backup image stores basic information about the backup that is not specific to the [backup container](#) in which the backup data is stored.

 **See Also:**
"[Backup Images](#)"

- backup image instance

A backup image instance contains the backup data and certain additional information about the backup. Oracle Secure Backup creates one backup image instance based on the parameters specified during the backup operation. For example, if you specified that the backup must be created using the tape drive `my_drv`, a backup image instance is created using the volume in this tape drive.

 **See Also:**
"[Backup Image Instances](#)"

You can create additional backup image instances, on different [backup containers](#), if required.

Backup Images

A [backup image](#) is a set of metadata that describes a backup. It contains information about the backup such as the backup name, type of backup, creation date, size, backup level, and backup UUID. Each backup operation creates exactly one backup image. Oracle Secure Backup assigns a backup UUID to each backup image. The backup image UUID is unique across the administrative domain.

 **See Also:**

Oracle Secure Backup Reference for information about the format used for backup image names

When you perform a backup operation, you can specify a name for the backup image. 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. If you do not specify a name, then Oracle Secure Backup generates a name comprised of the host name, timestamp, and a system-generated sequence number.

Backup images can contain the following types of data:

- File-system data from a host in the Oracle Secure Backup domain
- RMAN-generated backup piece containing part of an Oracle Database backup
- Data generated by a backup operation from an NDMP data service

Backup Image Instances

Oracle Secure Backup can write backup data to multiple [backup containers](#). A [backup image instance](#) is a complete representation of a [backup image](#) that is stored in a particular [backup container](#). Backup image instances contain the actual data that is backed up. There can be multiple backup image instances for a particular backup image, with each instance being stored in a different backup container.

For example, when you perform a file-system backup, Oracle Secure Backup creates a backup image and a backup image instance. Assume that this backup image instance is created on a tape drive `drive1`. Subsequently, you can create other instances of this backup image on a tape drive `drive2` and a disk pool `my_disk`. The backup data contained in all the backup image instances is the same. However, because they are stored on different media, some properties such as the media family and encryption type may be different.

Oracle Secure Backup assigns a UUID to each backup image instance. This UUID is unique across the administrative domain. Each backup image instance is also assigned a name that is unique across the administrative domain. Oracle Secure Backup generates the name of the backup image instance based on the name of its associated backup image. For example, for a backup image called `daily_db_bk`, the first backup image instance created is called `daily_db_bk.1`, the next instance created is called `daily_db_bk.2` and so on.

 **See Also:**

Oracle Secure Backup Reference for information about the format that can be used for backup image names

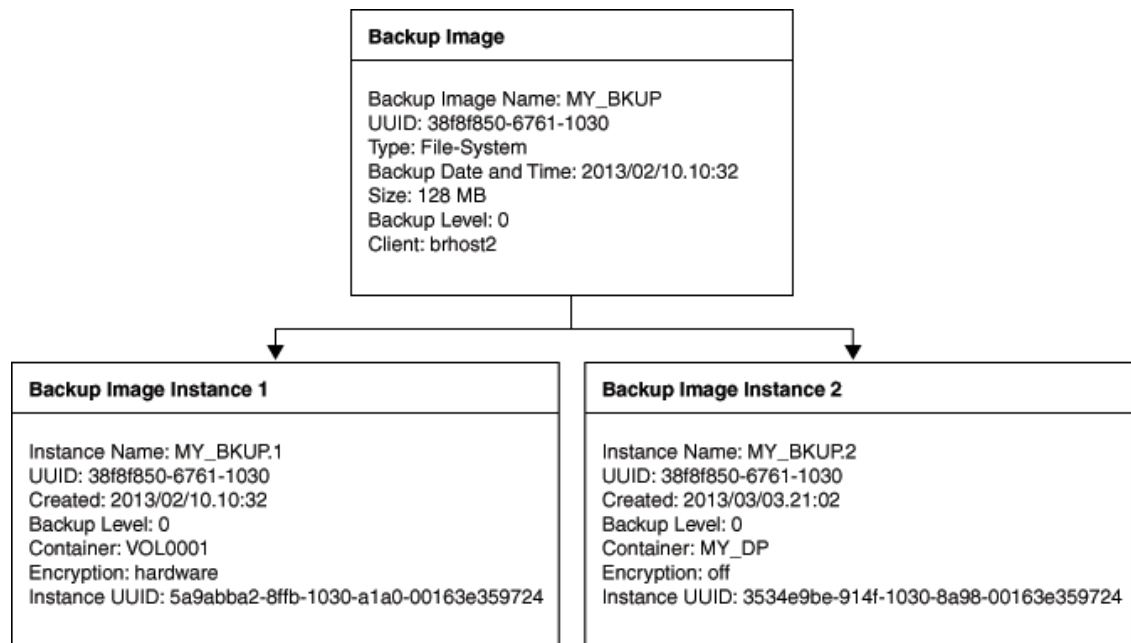
While storing backups on tape, each backup image instance is followed by [backup catalog data](#). During an [import catalog](#) operation, the backup catalog data provides the information which rebuilds that backup image instance, within the [Oracle Secure Backup catalog file](#), on

the current Oracle Secure Backup domain. By default, this function catalogs information about all the backup image instances stored within a volume set.

Relationship Between Backup Images and Backup Image Instances

Figure 1-4 illustrates the relationship between [backup images](#) and [backup image instances](#). When a backup operation completes, Oracle Secure Backup creates the backup image `MY_BKUP` and the backup image instance `MY_BKUP.1`. This instance is created in the tape volume `VOL0001`. Subsequently, another backup image instance is created on the disk pool `MY_DP`. The name of the backup image is `MY_BKUP.2`. Each backup image instance has its own unique UUID.

Figure 1-4 Backup Images and Backup Image Instances



Backup Image Instances and Catalog Data

When [backup image instances](#) are written to a [backup container](#), Oracle Secure Backup stores the catalog data for this backup along with the backup image instance. This catalog data enables you to quickly update the catalog when a backup container is imported into another administrative domain. Storing the catalog data along with the backup image instance also helps in disaster recovery scenarios. If the Oracle Secure Backup catalog information has been damaged and no backup copy of the catalog is available, this information can be used to recreate the catalog.

Overview of Oracle Secure Backup Media Concepts

Oracle Secure Backup stores the backups created as part of your data protection strategy on the specified storage media. This section provides an overview of the storage media and describes how backups are stored on different storage media.

This section contains the following topics:

- [About Backup Containers](#)
- [About Backup Sections](#)
- [About Volumes](#)
- [About Volume Sets](#)
- [About Disk Pools](#)
- [About Backup Image Instances and Tape Volumes](#)
- [About Data Blocks and Blocking Factors](#)
- [About Media Families](#)
- [About Cloud Storage Devices](#)

About Backup Containers

A backup container is the physical media on which [backup image instances](#) are stored. When you perform a backup operation, you can specify the backup container in which the backup should be stored. You can also copy or move backup image instances from one backup container to another.

Oracle Secure Backup supports the following types of backup containers:

- Disk pools

A disk pool is a file-system directory that is a repository for backup image instances. The contents of the file-system directory are managed by Oracle Secure Backup.



See Also:

["About Disk Pools"](#)

- Tape volumes

A tape volume is a physical piece of media such as the LTO5 tape cartridge. Tape volumes are physical cartridges that have been assigned a volume ID by Oracle Secure Backup. This volume ID is referenced by the catalog for performing restores. These volumes can reside in tape drives, libraries, vaulted or stored elsewhere at the system administrator's discretion.



See Also:

["About Volumes"](#)

- Cloud storage devices

Cloud storage devices store data in:

- Oracle Cloud Infrastructure Object Storage Classic
- Oracle Cloud Infrastructure Archive Storage Classic
- Oracle Cloud Infrastructure Standard Object Storage
- Oracle Cloud Infrastructure Archive Object Storage
- Oracle Cloud Infrastructure Infrequent Access Object Storage

Oracle Secure Backup creates a new container in the Oracle Cloud for each cloud storage device configured. All data backed up to a cloud storage device is stored in its associated container in the cloud.

 **See Also:**

- ["About Cloud Storage Devices"](#)
- The obtool commands "mkdev" and "lsdev" for more information about Cloud storage class options

Default Backup Container for Backup and Restore Operations

By default, Oracle Secure Backup stores backup image instances on tape. Backup image instances will be stored on disk pool if any of the following conditions are met:

- No tape devices are configured in the Oracle Secure Backup domain
- The backup job (on-demand or scheduled) has the disk pool configured as a device restriction

Oracle Secure Backup does not use cloud storage devices as targets for any job by default. It backs up data to a cloud storage device only if the cloud storage device is specified as a restriction in a job command.

While restoring data, Oracle Secure Backup first attempts to restore data from any available, online disk pool. If the required data is not available on disk pool, then Oracle Secure Backup restores it from tape. If the data is not available on tape, then it is restored from cloud storage.

About Backup Sections

A [backup image instance](#) can consist of one or more [backup sections](#). A backup section is a portion of a backup image instance that is stored contiguously in a [backup container](#). Each backup section is identified by a unique backup section ID that is generated by Oracle Secure Backup when the backup section is created.

When a backup image instance spans multiple tape volumes, the number of backup sections is the same as the number of tape volumes on which the backup image instance resides.

When a backup image is written to a disk pool, the entire backup image instance consists of exactly one backup section.

 **See Also:**

["Backup Image Instances and Backup Sections"](#)

About Volumes

A volume is a physical piece of media such as a tape. Oracle Secure Backup identifies each volume with a unique [volume ID](#). Oracle Secure Backup obtains the volume ID in a way described in ["Volumes in a Media Family"](#).

In addition to volume IDs, volumes can have tags. A [volume tag](#) is an alphanumeric string, up to 31 characters in length, that is typically obtained from a UPC [barcode](#) label affixed to the tape cartridge. Most libraries are equipped with barcode readers. This enables Oracle Secure Backup to determine the identity of a tape without having to load it and read the [volume label](#). Oracle Secure Backup correlates volume tags with volume IDs and remembers what [backup image instances](#) they contain for use during backup and restore operations.

Backup Image Instances and Volume Labels

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. The first block of a [backup image instance](#) is referred to as a [backup image label](#). It contains the file number, section number, and owner of the backup image instance.

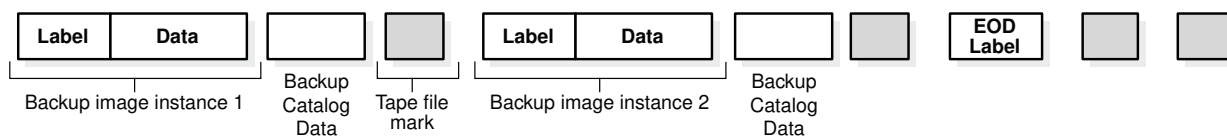
When a label is displayed, volume-related information is displayed with the header `Volume label` and backup image instance-related information is displayed with the header `Backup Image label`. These are actually different parts of a single label.

For volumes generated by the Oracle Secure Backup scheduling system, you might see entries such as media family and volume expiration.

Oracle Secure Backup numbers each backup image instance on a labeled volume set with a backup image file number, starting from 1.

When Oracle Secure Backup writes multiple backup image instances on a volume, it places a tape file mark after each backup image instance. After the last image, Oracle Secure Backup writes a tape file mark, then an end-of data (EOD) label, and then two more tape file marks. [Figure 1-5](#) illustrates the format of a volume that contains two backup image instances. This figure shows the position of the labels and tape file marks.

Figure 1-5 Two Backup Image Instances on a Volume



Backup image instances, volume labels, and the special `End of Data/End of Volume` labels share a common format and include both volume and backup image data. The volume label serves a dual role, being both the label for the volume and the label of the first backup image instance on the volume. Similarly, a backup image label contains information about the following backup image instance and a copy of the volume information from the volume label. Thus, Oracle Secure Backup can obtain volume information without having to rewind the tape to read the volume label.

Assume that the volume shown in [Figure 1-5](#) is the first volume in the set. The volume label for the first backup image instance could look like the one in [Example 1-2](#).

The volume label for the second backup image instance could look like the one in [Example 1-3](#).

After Oracle Secure Backup creates a backup image instance, it positions the volume just before the EOD label. The EOD label contains a copy of the data in the preceding backup image label, except that the image file number is incremented by one. Oracle Secure Backup

uses the EOD label to provide a volume ID, backup image file number, and sequence number for the next backup image instance without rewinding the volume.

After Oracle Secure Backup reads a backup image instance, it positions the volume after the tape file mark following the backup image instance that it just read and before the volume label of the next backup image instance.

Example 1-2 Backup Image Instance 1

```
Volume label:
Volume ID:      VOL000014
Owner:         jane
Host:          chicago
File number:   1
Section:       1
Sequence number: 1
...
```

Example 1-3 Backup Image Instance 2

```
Volume label:
Volume ID:      VOL000014
Owner:         jane
Host:          chicago
File number:   2
Section:       1
Sequence number: 1
...
```

About Volume Sets

Oracle Secure Backup enables a single backup image instance to span multiple volumes. A volume set is a group of one or more tape volumes in which the first volume is continued onto the second, the second is continued onto the third, and so on.

Each volume in a volume set has a [volume sequence number](#) that is greater than the sequence number of the previous volume. Consequently, you can back up or restore large amounts of data in a single session. Oracle Secure Backup always attempts to continue onto the next number in sequence with the current volume but in some cases this isn't possible. In this scenario, we will write to the next available volume ID in the same media family that has not been yet written to. Oracle Secure Backup will not allow any tape other than the first tape in the volume set to append to an existing Oracle Secure Backup volume, subsequent tapes will always write to a new volume using the next available volume ID in the sequence. For instance, if the first tape in a volume set was VOL00005, but volumes VOL00006 and VOL00007 have already been written to with other backups, then the second tape in VOL00005's volume set will be VOL00008.

When Oracle Secure Backup reads and writes multiple volumes, it keeps track of the proper order of volumes within the volume set with the following data:

- **EOV labels**

If a [backup image instance](#) extends beyond the end of one volume and continues onto a subsequent volume, then Oracle Secure Backup ends the first volume with a special EOV label. This label contains the volume ID of the next volume in the set. In a volume set, every volume except the last ends with an EOV label. The last ends with an EOD label.
- **Sequence numbers**

A sequence number, which is recorded in the volume label, indicates the order of volumes in a volume set. The first volume in a set has sequence number 1.

- Section numbers

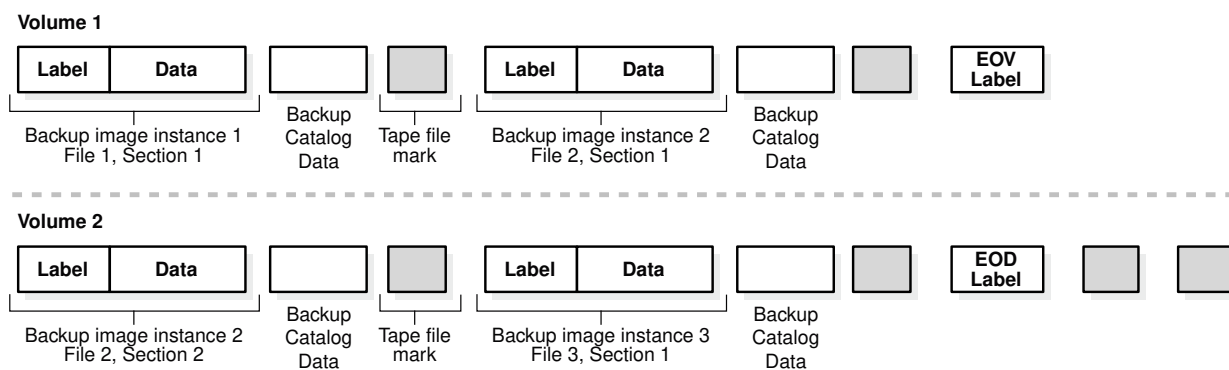
A section number, which is recorded in the volume label, indicates the order of the parts of a backup image instance that spans multiple volumes.

 **Note:**

The section number is always 1 unless the backup image instance spans volumes

Figure 1-6 illustrates a volume set that contains three backup image instances. Backup image instance 2 spans two volumes.

Figure 1-6 A Single Backup Image Instance on Multiple Volumes



A partial volume label for the first backup image instance could look like the one shown in [Example 1-4](#).

The partial volume label for the first section of the second backup image instance could look like the one shown in [Example 1-5](#).

The partial volume label for the second section of the second backup image instance could look like the one shown in [Example 1-6](#).

The partial volume label for the second section of the second backup image instance could look like the one shown in [Example 1-7](#).

Example 1-4 Backup Image Instance 1, Section 1

```
Volume label:
Volume ID:      VOL000014
Owner:         jane
Host:          chicago
File number:   1
Section:       1
Sequence number: 1
```

Example 1-5 Backup Image Instance 2, Section 1

```
Volume label:
Volume ID:      VOL000014
Owner:         jane
Host:          chicago
File number:   2
```

```
Section:          1
Sequence number: 1
```

Example 1-6 Backup Image Instance 2, Section 2

```
Volume label:
Volume ID:      VOL000015
Owner:         jane
Host:          chicago
File number:    2
Section:       2
Sequence number: 2
```

Example 1-7 Backup Image Instance 3, Section 1

```
Volume label:
Volume ID:      VOL000015
Owner:         jane
Host:          chicago
File number:    3
Section:       1
Sequence number: 2
```

About Disk Pools

A disk pool is a file-system directory that acts as a repository for [backup image instances](#). Each disk pool is associated with a file-system directory path and the contents of this directory are managed by Oracle Secure Backup. Disk pools can store file-system backups, RMAN backups of Oracle Databases, and backups created by NDMP filers. Disk pools can be accessed concurrently by multiple backup and restore operations thus providing improved performance for backup and restore jobs.

Each disk pool is represented as a device in Oracle Secure Backup. A disk pool can belong to only one Oracle Secure Backup administrative domain. It cannot be shared between multiple Oracle Secure Backup administrative domains.

Backup image instances remain in the disk pool until they expire, are explicitly deleted, or moved to tape. Oracle Secure Backup deletes expired backup image instances only when the disk pool space threshold is exceeded and not immediately after they expire.

Storage Capacity on Disk Pools

When you create a disk pool, it is recommended that you set a capacity value. A capacity value represents the amount of space that can be occupied by the backup image instances stored on this disk pool. When the specified capacity is reached, Oracle Secure Backup does not schedule any jobs for this disk pool until the space consumption drops below the capacity.

If a disk pool does not have a capacity set (unlimited capacity), then the current space utilization is used as the capacity value. The free-space-goal percentage is applied to that value and a purge is automatically performed to that utilization level.

For example, if the current disk pool utilization is 100 GB and the free space goal is 20%, then 20 GB of the space used by expired backup images (assuming such was available) is purged.



See Also:

["Monitoring Disk Pool Space Utilization"](#)

Space Utilization in Disk Pools

For each disk pool, you can specify a threshold value for space utilization. This threshold is referred to as the free space goal. It is expressed as a percentage and represents the amount of free space that Oracle Secure Backup attempts to maintain in the disk pool. When the space consumed by a disk pool exceeds the specified threshold, Oracle Secure Backup deletes expired backup image instances.



See Also:

["Monitoring Disk Pool Space Utilization"](#)

Disk Pool Orphans

If a backup to a disk pool fails, then the existing data related to this backup on the disk pool is not added to its disk pool catalog. Oracle Secure Backup does not detect the presence of these backup files on the disk pool. Such files are named orphans. Oracle Secure Backup runs a daily automatic cleanup process to delete files that do not have corresponding entries in the catalog. In some cases, this may cause loss of important data. Hence, it is highly recommended that you catalog your disk pool immediately after importing it into a new domain to avoid the automatic deletion of disk pool orphans during its cleanup. You can disable the daily cleanup process by changing policy settings.



See Also:

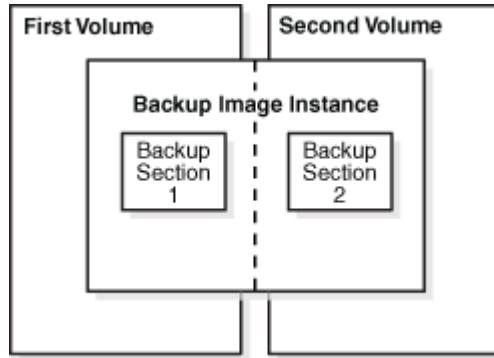
- ["Managing Disk Pools"](#) for more information on performing disk pool tasks
- ["Importing and Cataloging Backups"](#) for more information on cataloging disk pool data
- *Oracle Secure Backup Reference* for more information on the `deletediskorphans` policy.

About Backup Image Instances and Tape Volumes

To understand Oracle Secure Backup, you must understand the relationship between the physical backup files and the media on which those files are stored. [Figure 1-7](#) provides a graphical illustration of how backup files are related to volumes. The concepts are as follows:

- A **data block** is the amount of data written to media in each write operation.
- A **volume** is a unit of media, such as an LTO5 tape cartridge.
- A **backup section** is the part of a backup image instance that fits on one physical volume.
- A **backup image** is the product of a backup operation and stores metadata about the backup.
- A **backup image instance** is the product of a backup operations and stores the actual data backed up.

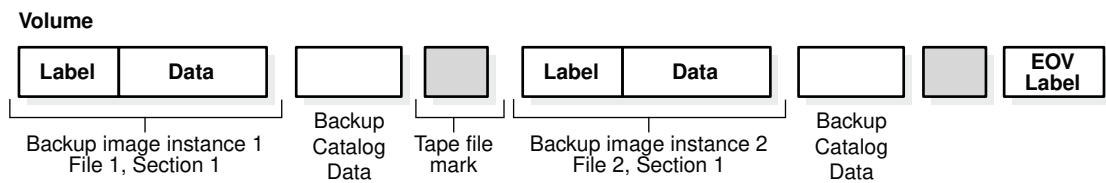
Figure 1-7 Backup Image Instances, Backup Sections, and Volumes



Backup Image Instances and Backup Sections

When you run a backup operation in Oracle Secure Backup, you create a [backup image instance](#). As shown in [Figure 1-8](#), a backup image instance is a file that consists of at least one [backup section](#).

Figure 1-8 Backup Image Instances and Backup Sections



A backup image instance is uniquely identified in the Oracle Secure Backup catalog by its backup UUID. Similarly, a backup section is uniquely identified in the catalog by its backup section OID.

[Example 1-8](#) shows output from the `lsbi` command for a backup with the backup UUID of `brhost2-20130329-123722.1`.

[Example 1-9](#) shows output from the `lsbi` command for the backup sections belonging to the backup image instance shown in [Example 1-8](#).

See Also:

Oracle Secure Backup Reference for complete syntax and semantics for the `lsbu` and `lssection` commands.

Example 1-8 Backup Image Instance

```
ob> lsbi brhost2-20130329-123722.1
      Instance Name                               Created
Container(s)brhost2-20130329-123722.1          2013/03/29.05:37 VOL000001
```

Example 1-9 Backup Section

```
ob> lsbi --sections brhost2-20130329-123722.1
      Instance Name          Created          Container(s)
brhost2-20130329-123722.1    2013/03/29.05:37
spantape-000001,
spantape-000002              BSOID File Sect  Size    103    1    1  100.1 MB
104      1    2    24.4 MB
```

About Validating Backups by Computing Checksums

Oracle Secure Backup ensures integrity of backups by detecting data corruption at any point during the lifecycle of the backup. This includes database backups, file-system backups, and backups from NDMP filers.

Data corruption can occur due to hardware failures, human errors or malicious attacks, network or latency issues, storage issues, or application corruption (as part of read or write processing). While creating a backup image instance (as part of a backup, staging, or copy instance operation), Oracle Secure Backup computes and stores a checksum. To verify the integrity of a backup image instance, the media server recomputes the checksum, reads the checksum that was stored when this backup image instance was created, and then compares the recomputed checksum with the stored checksum. If the stored checksum and the recomputed checksums match, the backup image instance is valid and has no data corruption.

The process of verifying backups is referred to as backup validation. Backup validation can also be used to validate backup image instances before performing vaulting or staging. You can perform backup validation immediately after a backup is created or through an automated script that runs a `validate` job at specified intervals. Each validation request creates a separate `validatechecksum` job. Note that backup validation does not restore backups or copy them to another location.

During an upgrade of Oracle Secure Backup administrative domain, the device policies for all storage devices are set to `SYSTEMDEFAULT`. Unless you modify this setting explicitly after the upgrade, by default, checksum computation is performed for all backups created on tape devices and disk pools after the upgrade.

Levels for Configuring Checksum Computation of Backups

Checksum computation can be configured in one of the following ways:

- To configure checksum computation for all storage devices of a particular type, set the device policy for that type of device.
- To configure checksum computation for a specific device, enable checksum computation for that device.

When you configure checksum validation both at the device type level and for a specific storage device, the device type level setting takes precedence over the individual device policy setting.

Operations for Which Checksum Computation Can be Performed

Checksum computation is applicable for the following types of jobs:

- backup
- copyinstance
- staging

All these operations result in copying an entire backup image instance to different storage containers. Checksums are recomputed and stored for each new backup instance that is

created. The checksums on the source device and that of the new backup instance must match.

For copy instance jobs, even if the source backup does not have a checksum stored, the copied backup image instance can compute and store a checksum.

Limitations of Checksum Computation

- Checksum computation cannot be performed for existing backups.
For example, you created a backup image instance using Oracle Secure Backup 12.2. The administrative domain was subsequently upgraded to Oracle Secure Backup 18.1. Backups that were created using Oracle Secure Backup 12.2 cannot be validated because checksums were not computed at the time the backup image instance was created.
- Restarted backups and backups to NDMP filers cannot be validated.
- Only one backup image instance can be validated at a time.
- Checksum validation is not supported when the copying backup image instances from an NDMP filer to another NDMP filer.
- Checksum validation is not supported when duplicating volumes.
- Hardware-encrypted transient backup image instances are not supported when performing checksum computation as part of the `validatechecksum` job.



See Also:

Oracle Secure Backup Reference for information about performing backup validation

About Data Blocks and Blocking Factors

In a typical format, a tape drive writes data to a tape in blocks. The tape drive writes each block in a single operation, leaving gaps between the blocks. The tape runs continuously during the write operation.

The *block size* of a block of data is just the size of the block in bytes as it was written to tape. All blocks read or written during a given backup or restore operation have the same block size. The *blocking factor* of a block of data expresses the number of 512-byte records that are contained in that block. So, for example, the Oracle Secure Backup default blocking factor (128) results in a tape block size of 128*512 bytes or 64KB.

The *maximum blocking factor* is an upper limit on the blocking factor that Oracle Secure Backup uses. This limit comes into play particularly during restores, when Oracle Secure Backup must pick an initial block size to use without knowing the actual block size on the tape. The maximum blocking factor limits this initial block size to a value that is acceptable to both the tape device and the underlying operating system.

When Oracle Secure Backup starts a backup, it decides what block size to use based on several factors. Listed in order of precedence, these factors are:

- Blocking factor specified using the `obtar -b` option
This option can also be specified as part of the `operations/backupoptions` policy. If this option is specified, then it overrides all other factors.

 **See Also:**

Oracle Secure Backup Reference for more information about the `obtar -b` option and the `operations/backupoptions` policy

- Configuration of the tape drive to be used

You can specify what blocking factor, maximum blocking factor, or both that Oracle Secure Backup should use for a particular tape drive when you configure that drive. You might want to do this if you have tape drives with very different block size limits.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for more information about configuring a tape drive

- Domain-wide blocking factors, maximum blocking factors, or both that the `media/blockingfactor` and `media/maxblockingfactor` policies set.

 **See Also:**

Oracle Secure Backup Reference for more information about the `media/blockingfactor` and `media/maxblockingfactor` policies

- The default blocking factor (128) and maximum blocking factor (128), resulting in a block size of 64 KB

When a blocking factor has been nominated by one or another of these factors, it must pass the following tests:

- The block size must be less than or equal to the maximum block size (blocking factor) in effect from applying whatever policies or tape drive configuration attributes are in force.
- The block size must be supported by the tape drive and attach point in question.

Sometimes a tape drive, device driver, or kernel operating system has a limitation that supersedes all other considerations.

When Oracle Secure Backup begins a restore operation, it does not know what block size was used to write a given tape. Because issuing a read for a too-small block would result in an error condition and a required tape reposition, Oracle Secure Backup always starts a restore operation by reading the largest possible block size. This is either the current setting of the `media/maxblockingfactor` policy or the tape drive configuration attribute. The maximum blocking factor, therefore, must always be greater than or equal to the largest block size you ever want to restore.

After the first read from the backup image instance, Oracle Secure Backup compares the amount of data requested to the actual size of the block and adjusts the size of subsequent reads to match what is on the tape.

About Media Families

A media family is a named classification of volume sets. This classification ensures that [backup containers](#) created at different times share characteristics. In this way, you can map a media family to a typical backup operation. Media families define the retention methodology, [write window](#), and retention time as appropriate.

You can associate a media family with a [disk pool](#). However, the only attribute that is applicable to disk pools is the retention time. It is possible to use the same media family for backups to tape and disk pool. When the backup is stored on a disk pool, only the retention time specified in the media family is used.

Media Family Attributes

A media family is an attribute defining multiple characteristics that is assigned to a volume at creation time. The media family contains information including whether or not a volume is time or content managed, when or if it ever expires, rotation and duplication policies, and what the volume ID name will look like.

The media family attributes associated with a tape will be whatever attributes the media family had defined when the first volume in a particular volume set was written. Later changes made to the media family settings will not be applied to existing tapes, only to tapes that are written or recycled using this family in the future.

Every volume in a media family shares the following attributes:

- Volume identification sequence

Oracle Secure Backup writes a unique identifier on each tape volume whenever one of these occurs:

- Oracle Secure Backup writes to the tape for the first time.
- Oracle Secure Backup overwrites the tape from the beginning.

The volume ID consists of a fixed portion, usually the name of a media family, followed by a sequence number assigned and updated by Oracle Secure Backup. For example, if the media family is `full_backup`, then a volume ID might be `full_backup-000029`. By default the sequence number of the first volume in the media family is 1. The sequence number is incremented by 1 for each successive volume in the media family. However, if a media family is deleted and another is created using the same name, then the volume sequence number is reset to 1.

- Volume expiration policy

An [expiration policy](#) defines when volumes in a media family are eligible to be overwritten and recycled. A media family can have either of the following mutually exclusive volume expiration policy types:

- Content-managed

Determines volume expiration by using RMAN retention parameters that are associated with the Oracle Database. Content-managed media families can only store Oracle Database backups.



See Also:

["Content-Managed Expiration Policies"](#)

– Time-managed

Determines volume expiration by leveraging a user-defined retention that is associated with the media family. Time-managed media families can store both Oracle Database and file-system backups.



See Also:

["Time-Managed Expiration Policies"](#)

For file system backups, if no media family is designated, then the `null` media family is used as the default which appears with the volume id `VOL`. For RMAN backups, if no media family is designated, the `RMAN-DEFAULT` media family is used as the default.

The media family associated with a volume is assigned to the tape during the first Oracle Secure Backup write to that tape. Volumes can be unexpired and have unused space remaining on them and not be selected for the next backup operation. Only backups from the same media family can append to a tape. Volumes that are full or closed will obviously not be written to, unless they have expired. When Oracle Secure Backup initiates a backup, it looks for the most recent volume with space available belonging to the specified media family. If none such volume is available, the first new or recyclable volume located in the library storage elements will be used for the backup.

When a time-managed volume set expires, Oracle Secure Backup automatically considers each volume in the set eligible to be overwritten and recycled. Content-managed volume sets expire independently of other members of a volume set; they become eligible for recycling as soon as all pieces on a volume expire.

- Write window

The write window is the period of time for which a time -managed volume set remains open for updates. Updates are other backups that can append an existing tape of the same media family that still has an open write window. 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.

If a backup is writing to a tape when the write window closes, then the backup completes but no further backups are written to the volume. 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 manually unlabeled.

- Rotation policy

A [rotation policy](#) defines the physical management of backup media throughout the media life cycle. This policy determines the sequence and timing during which a volume moves from its initial, [active location](#) to a storage location and back to an active location to be reused.

 **See Also:**

[Vaulting](#) for more information about rotation policies

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.

 **See Also:**

- "[Configuring Media Families](#)" to learn how to create media families
- *Oracle Secure Backup Reference* for a description of the media family commands

Volumes in a Media Family

When you create a media family, you specify how to generate volume IDs that become part of the volume label.

When Oracle Secure Backup labels a tape volume, it assigns it a volume ID based upon the contents of a [volume sequence file](#). This file resides on the administrative server. Its location is defined by the media family of the volume. The volume sequence file is usually located in the `admin/state/general` subdirectory of the Oracle Secure Backup home.

When you define a media family, you direct Oracle Secure Backup how to assign a volume ID. You can direct Oracle Secure Backup in the following ways:

- Media family default volume sequence file

In most cases, you should use this file. Volume sequence files for each media family are located in the `admin/state/family/family_name` directory. For example, if you define a media family with the name `new_data`, then files are located in the `admin/state/family/new_data` directory.

Oracle Secure Backup constructs each volume ID by starting with the media family name, appending a dash, then appending a 6-digit sequence number, the first of which is `000001`. For example, if you define a media family called `new_data`, then Oracle Secure Backup creates a volume sequence file on the administrative server called `.vid.new_data`. The first volume ID in this file is `new_data000001`. Each time Oracle Secure Backup assigns an ID to a volume, it increments by one. That is, the next volume ID that Oracle Secure Backup assigns is `new_data000002` and so on.

- User-specified volume sequence file

Oracle Secure Backup creates a default volume sequence file during installation. It resides in the `admin/state/general` subdirectory on the administrative server. The first volume ID in this file is `VOL000001`. Each time Oracle Secure Backup assigns an ID to a volume, it increments it by one. That is, the next volume ID that Oracle Secure Backup assigns is `VOL000002`, and so on.

If you specify your own volume sequence file, then Oracle Secure Backup ignores the default volume sequence file and instead uses your file for obtaining volume IDs. You can enter a full path name to specify where this file should be created later. Oracle Secure Backup does not create this file automatically. You must do so manually. You can use a text editor to customize the volume ID prefix.

Each volume ID file can contain a single volume ID. The maximum length of the volume ID is 31 characters. You can use the first few characters to help classify your volumes. For example, you could create volume IDs that begin with:

- The prefix `8mm` to identify volumes created by one tape device and `DAT` to identify volumes created by a different tape device
- The prefix `INCR` or `FULL` to identify volumes used for a [full backup](#) or an [incremental backup](#)
- The initials of the [operator](#) who performs the backup, for example, `la`.

If you do not include any digits in the sequence number you create, then Oracle Secure Backup appends a 1 to the sequence number and increments that number by 1 each time the sequence number is used.

- User-specified volume ID

You can use the `--vidunique` option on the `mkmf` command to specify an explicit volume ID. For example, you can create your own volume ID if you previously created a tape that is partially unreadable. You can perform the backup again and use the `--vidunique` option, specifying a volume ID that keeps your volume IDs in sequence.

You can also use the `--vid` option on the `restore` command to ensure that the volume being read is the correct one.



See Also:

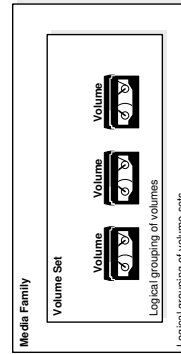
Oracle Secure Backup Reference for complete syntax and semantics for the `mkmf` and `restore` commands

Volume Sets and Media Families

[Figure 1-9](#) provides a graphical illustration of how a [volume set](#) is related to a media family. The concepts are as follows:

- A volume set is a logical grouping of one or more physical volumes spanned by a [backup image instance](#).
- A media family is a logical classification of volumes that share common attributes. For example, volumes in a media family share a common naming pattern and policies used to write and keep data.

Figure 1-9 Volumes, Volume Sets, and Media Families

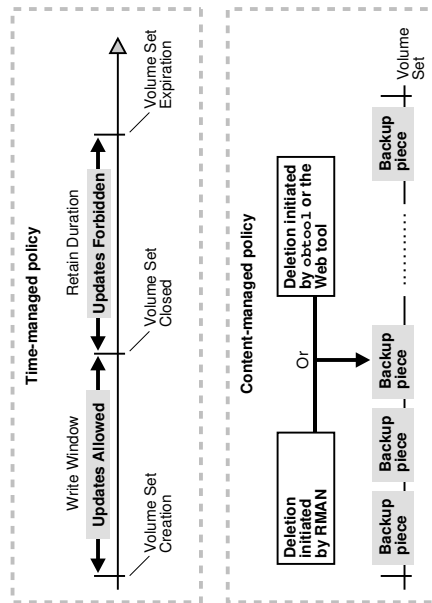


When you back up files with Oracle Secure Backup, you generate a volume set that has some common characteristics defined by the corresponding media family associated with your backup.

Volume Expiration Policies

When you create a media family, you specify a volume expiration policy that determines when volumes in a media family are eligible to be overwritten and recycled. As shown in [Figure 1-10](#), volumes in a media family use either a [content-managed expiration policy](#) or [time-managed expiration policy](#).

Figure 1-10 Volume Expiration Policies



Content-Managed Expiration Policies

You can make an RMAN backup, but not a [file-system backup](#), to a volume that uses a content-managed expiration policy. The expiration of a content-managed volume is determined based on the attribute associated with the backup pieces stored on the volume. When each [backup piece](#) on the volume has been marked as deleted, the volume is eligible to be recycled.

A volume in a content-managed volume set can expire even though the other volumes in the set are not yet expired.

Since content-managed volumes adhere to user-defined RMAN retention settings, RMAN instructs Oracle Secure Backup when to mark a backup piece as deleted. The actual backup piece is not deleted from the volume, only the value of the attribute in the Oracle Secure Backup catalog is updated.

When you install Oracle Secure Backup, the software includes a default content-managed media family named `RMAN-DEFAULT`. You cannot delete or rename this media family, although you can modify certain attributes of it through the Oracle Secure Backup Web tool or the `chmf` command in `obtool`.

As shown in [Figure 1-10](#), you can delete backup pieces through the RMAN or Oracle Secure Backup interfaces. Deleting backup pieces with Oracle Secure Backup tools leaves the metadata in the RMAN repository inconsistent with the contents of your tapes. If RMAN backups are deleted from tape at the Oracle Secure Backup level, or if RMAN backups on tape are unavailable or lost for other reasons, then you should immediately use the RMAN `CROSSCHECK` command to update the RMAN repository.

See Also:

- *Oracle Secure Backup Reference* to learn about the `chmf` command

Time-Managed Expiration Policies

Volumes in a time-managed media family expire when they reach their volume expiration time. At this point Oracle Secure Backup automatically considers each volume in the volume set eligible to be overwritten.

As shown in [Figure 1-10](#), Oracle Secure Backup computes the volume expiration time by adding the following:

- Volume creation time for the first volume in the set
This is the time at which Oracle Secure Backup wrote backup image file number 1 to the first volume in the volume set.
- Write window period
This is the user-specified period during which volumes in a media family can be written to. All volumes in a volume set share the same write window.
- Retention period
This is the user-specified period during which volumes in a media family are not eligible to be overwritten. All volumes in a volume set share the same retention period.

If no write window is configured, then the retention period begins with the first tape write. If a write window is configured, then the retention period begins when the write window closes for the volume set.

The retention period setting prevents you from overwriting any volume in this media family until the specified amount of time has passed. If one volume becomes full, and if Oracle Secure Backup continues the backup onto subsequent volumes, then it assigns each volume the same retention period.

For example, if you set the write window for a media family to 7 days and the retention period to 14 days, then the data on all volumes in the volume set is retained for 14 days from the close of the write window. If 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, then all 21 volumes in the set expire on January 22 at noon.

You can make both a file-system backup and an RMAN backup to a time-managed volume. Thus, a volume with a time-managed expiration policy can contain a mixture of file-system backups and RMAN backup pieces. If you make an RMAN backup to a time-managed volume, then the time-managed expiration policy overrides any retention settings set in RMAN.

 **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.

About Cloud Storage Devices

Oracle Secure Backup cloud storage devices are used to backup and restore data to and from Oracle Cloud Infrastructure Object Storage Classic and from Oracle Cloud Infrastructure Object Storage. A cloud storage device operates on a cloud storage container in the Oracle Cloud user's identity domain. The cloud storage container acts as a repository for backup image instances.

Each cloud storage device is associated with only one cloud container. The storage class options for a cloud container are:

- Standard storage class (`object`) for both Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure
- Archive storage class (`archive`) for both Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure
- Infrequent access storage class (`infrequentaccess`) for Oracle Cloud Infrastructure

 **See Also:**

- *Oracle Secure Backup Installation and Configuration Guide* for information about configuring cloud storage devices
- [Oracle Cloud Infrastructure Object Storage Classic](#) for more information about the Oracle Cloud Infrastructure Object Storage Classic
- The `obtool` commands "mkdev" and "lsdev" for more information about Cloud storage class options

The cloud storage device is an Oracle Secure Backup device resource. Backup jobs must be explicitly configured to use cloud storage devices. The cloud storage device can store file-system backups or RMAN backups of Oracle databases. Cloud storage devices can be accessed concurrently by multiple backup and restore jobs. The number of concurrent jobs is defined by the device's `concurrentjob` setting. Each of the backup or restore job creates

parallel data connections to Oracle Cloud storage. The number of parallel connections is controlled by device's `streamsperjob` setting.

A cloud storage device and its associated container can belong to only one Oracle Secure Backup administrative domain. It cannot be shared between multiple Oracle Secure Backup administrative domains.

Oracle Secure Backup stores each backup image instance by splitting it into multiple segments and storing each segment as a single object in the container. The segment size defines the size of the object and is specified by the device's `segmentsize` parameter.

Backup image instances remain in the cloud container until they expire, are explicitly deleted, or are migrated to a cloud archive container. Oracle Secure Backup deletes expired backup image instances only when the device's free space threshold is exceeded; not immediately after they expire.

 **See Also:**

- [Managing Cloud Storage Devices](#)

Oracle Secure Backup ensures that backup data is encrypted on the client before it is written to the cloud. If the backup job does not require encryption, then Oracle Secure Backup's client-side software encryption is automatically forced on and the encryption policies set up in the client are applied to the backup data written to the cloud storage device.

You can stage backup data to a disk pool and then move it to a cloud storage device using automated staging. The backup data in the disk pool must be encrypted in order to copy it to the cloud storage device. However, a cloud storage device cannot be used as the source device for automated staging.

You can move a backup image instance from a standard storage class (`object`) container to an infrequent access storage class container or an archive storage class container with a manual copy job. Both containers must be located in the same identity domain. The copy between the standard object storage container and the infrequent access storage container or the archive storage container does not download the data to the client.

Oracle Secure Backup Using Multipart Upload

Oracle Secure Backup can perform secure backup and restore operations using multipart upload for efficient backup jobs.

The backup and restore jobs are run on the media server. Oracle Secure Backup uploads data in segmented chunks to a cloud storage device. In bucket, each segment is written as a single object. The segment size can be anywhere between 10MB and 1 GB. A huge backup generates a high number of objects in the bucket. Managing a large number of objects becomes harder as the number of backups grows. Some actions, such as delete instance, storage reclaim, cloud copy, and cataloging backups taking a lengthy time, may have performance issues.

With multipart uploads, backup segments are uploaded in parallel and once the entire backup is uploaded, segments are concatenated to form a single object (segment), lowering the number of objects in the bucket. This helps to improve the performance of above-mentioned operations.

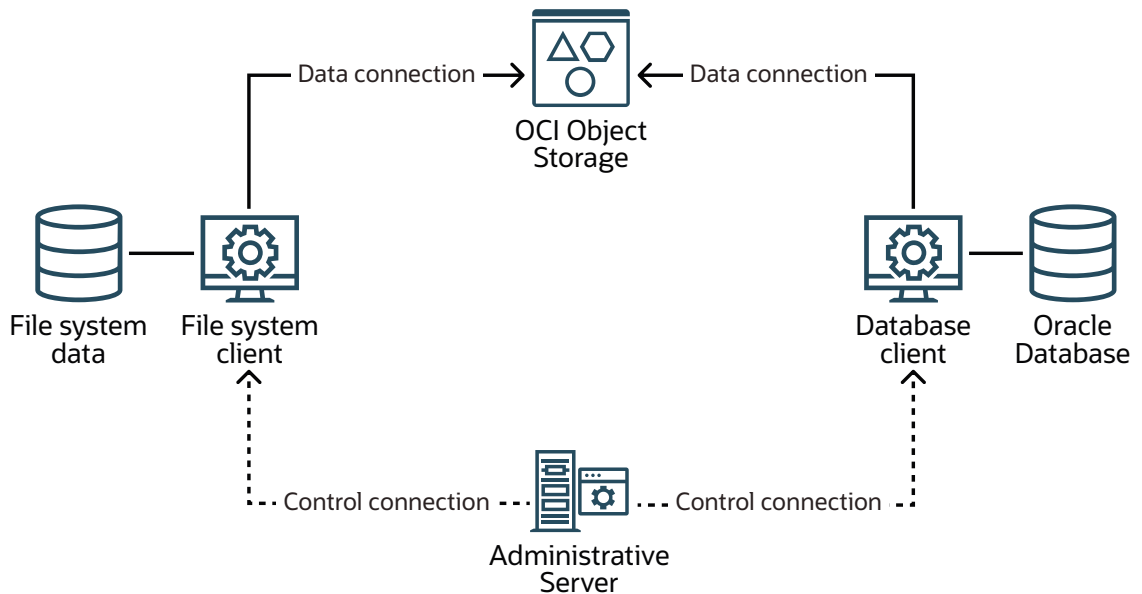
 **See Also:**

- [Cloud Policies for Multipart Uploads](#) in *Oracle Cloud Infrastructure Documentation*.
- `segmentsize` from `mkdev` and `chdev` in *Oracle Secure Backup Reference*.

About Client Direct to Cloud

Oracle Secure Backup provides options for uploading backups to the Oracle Cloud Infrastructure object storage.

Figure 1-11 Client Direct to Cloud Feature



Generally, during a backup operation, clients send backup data to Oracle Secure Backup media server, which buffers it in memory and later uploads it to the cloud object storage. These steps require additional resources at the media server. Lack of sufficient resources and too many concurrent backup jobs may result in poor backup throughput.

To improve the throughput of backup jobs, you can use the Client Direct to Cloud feature. With this feature, a client host can upload backup data directly to the Oracle Cloud Infrastructure object storage without the intervention of media servers. If the administrative server has sufficient resources, such as CPU, memory, and storage, then this option eliminates the use of additional media servers for uploading backups.

 **Note:**

You must enable the Client Direct to Cloud feature at both the client host and the cloud storage device. If enabled at only one place, that is, the client or the cloud storage device, then this feature remains in disabled state.

Key Benefits

- Helps upload backups directly to cloud storage, thus improving backup throughput.
- Removes the requirement for additional memory or CPU at media servers.
- This configuration is more scalable because the clients upload backups directly to cloud storage.

See Also:

- [Enabling Client Direct to Cloud](#) for how to enable this feature

About Backups in Immutable Buckets

Oracle Secure Backup supports the immutable buckets feature provided by Oracle Cloud Infrastructure. This feature enables Oracle Secure Backup to store backups in Oracle Cloud Infrastructure object storage and archive storage but prevents any modification or deletion of data.

Oracle Cloud Infrastructure provides different types of retention rules to safeguard the data in immutable buckets for a specified duration. When you configure retention rule for a bucket, it applies to all the objects within the bucket.

Retention Rules

For your backup data, Oracle Secure Backup helps you create and manage the following retention rules of Oracle Cloud Infrastructure:

- **Compliance rule:** These rules define the duration how long a particular bucket stores an object. During this period, you can access and read the data multiple times but cannot modify or delete them. If an object has multiple compliance rules, then the object storage considers the rule with the longest time period. The retention rule also depends on the last modification time stamp of the object.

For example, an object storage bucket has three objects, A, B, and C that are either uploaded or last modified 3 months, 6 months, and 1 year ago respectively.

- If you create a compliance rule on the bucket for 9 months duration, then the objects A and B becomes immutable immediately but object C can be modified or deleted.
- If you change the retention duration on the bucket to 2 years, then all three objects become immutable. The object C becomes mutable after another year, object B becomes mutable after 1 year and 6 months, and object A becomes mutable after 1 year and 9 months.

Oracle Cloud Infrastructure provides an option to apply locks to these time-based retention rules. When a retention rule is locked, you can increase the retention time but cannot decrease it or delete the rule. To delete the rule, all objects in the object storage bucket must be mutable and the bucket must be deleted.

Note:

You can delete an object storage bucket only if it is empty.

- **Legal hold:** These rules indicate any regulatory obligation to retain a backup. A legal hold has no time period associated with it.

If a backup data in an immutable bucket has a compliance rule and you apply legal hold to it, then the legal hold takes precedence. As a result, the data remains in the object storage beyond the time period specified in the compliance rule. The compliance rule comes into effect only after the legal hold on that bucket is removed. You cannot apply locks on a legal hold.

Using Oracle Secure Backup, you can create one time-based compliance rule and one legal hold rule for a bucket in Oracle Cloud Infrastructure object storage.

 **Note:**

To manage rules from Oracle Secure Backup, ensure that you create them using Oracle Secure Backup. You cannot use Oracle Secure Backup to modify or delete rules that were created using other sources, such as the Oracle Cloud Infrastructure console.

 **See Also:**

- [Using Immutable Buckets of Oracle Cloud Infrastructure](#)

2

Managing Users and Classes

An [Oracle Secure Backup user](#) is an administrative domain-wide identity, associated with a username. A [class](#) is a named collection of [rights](#) assigned to this user.

 **Note:**

Do not confuse this sense of the term class with [defaults and policies](#) classes, which are a convenience for grouping defaults and policies related to one functional area of Oracle Secure Backup.

This chapter describes Oracle Secure Backup users and classes and explains how to configure them in your [administrative domain](#).

This chapter contains these sections:

- [Overview of Oracle Secure Backup Users](#)
- [Overview of Oracle Secure Backup Classes and Rights](#)
- [Managing Users](#)
- [Managing Classes](#)
- [Managing Defaults and Policies](#)

 **Note:**

Before you set up an administrative domain, ensure you have logged into Oracle Secure Backup.

Overview of Oracle Secure Backup Users

Oracle Secure Backup stores information pertaining to Oracle Secure Backup users and rights on the administrative server, enabling Oracle Secure Backup to maintain a consistent Oracle Secure Backup user identity across the administrative domain.

Each user of an Oracle Secure Backup administrative domain has an account and an encrypted password stored on the administrative server. An operating system user can enter his or her Oracle Secure Backup username and password in the Oracle Secure Backup [Web tool](#) or [obtool](#). The client program sends the password over an encrypted [SSL](#) connection to the administrative server for [host authentication](#).

 **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 user be prompted for the password.

About Operating System Accounts

The namespace for Oracle Secure Backup users is distinct from the namespaces of existing UNIX, Linux, and Windows users. Thus, if you log in to a host in the administrative domain as operating system user `johndoe`, and if an Oracle Secure Backup user in the administrative domain is named `johndoe`, then these accounts are separately managed even though the name is the same. For convenience, you might want to create an Oracle Secure Backup user with the same name and password as an operating system user.

When you create an Oracle Secure Backup user, you can associate it with Linux, UNIX and Windows accounts. You can use one of these accounts for a backup operation that does not run with `root` privileges, also known as an [unprivileged backup](#) operation. In contrast, [privileged backup](#) and restore operations run on a [client](#) with `root` permissions on Linux and UNIX or `Local System` permissions on Windows.

Assume you create the Oracle Secure Backup user `jdoe` and associate it with UNIX account `x_usr` and Windows account `w_usr`. When `jdoe` uses the `backup --unprivileged` command to back up a client in the administrative domain, the job runs under the operating system accounts associated with `jdoe`. Thus, `jdoe` can only back up files on a UNIX client accessible to `x_usr` and files on a Windows client accessible to `w_usr`.

If you have the `modify administrative domain's configuration` right, then you can configure the [preauthorization](#) attribute of an Oracle Secure Backup user. You can preauthorize operating system users to make RMAN backups or log in to Oracle Secure Backup command-line utilities. For example, you can preauthorize the `x_usr` UNIX user to log in to `obtool` as Oracle Secure Backup user `jdoe`.

 **See Also:**

Oracle Secure Backup Reference for more information about the `modify administrative domain's configuration` right

 **Note:**

On Windows, Oracle Secure Backup stores the Windows name, password, and [domain](#) for each account. This data is communicated to the required client host over an encrypted SSL channel.

About NDMP Hosts

When setting up an Oracle Secure Backup user account, you can configure user access to an [NDMP](#) host, which is a device such as a [filer](#) that does not run NDMP natively. Passwords for

NDMP hosts are associated with the host instead of the user. You can configure the host to use the default NDMP password, a user-defined text password, or a null password. You can also configure a password authentication method such as text or MD5-encrypted.



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 user be prompted for the password.

About User Configuration

When you ran `installob` on the administrative server, Oracle Secure Backup created the `admin` user by default. Unless you chose to create the `oracle` user for use in backing up and recovering Oracle Databases, no other Oracle Secure Backup users exist in the administrative domain.

After installation, you can create more Oracle Secure Backup users or manage the attributes of individual Oracle Secure Backup users. The following user attributes are particularly important:

- Preauthorizations

You can preauthorize an operating system user to log in to the user-invoked Oracle Secure Backup command-line utilities. You must preauthorize an operating system user to make Oracle Database SBT backups through RMAN.

A preauthorization for an operating system user is associated with a specific Oracle Secure Backup user. For example, you can enable the Linux user `johndoe` to log in to `obtool` as the Oracle Secure Backup user named `backup_admin`. You could also preauthorize `johndoe` to run RMAN backups under the `backup_admin` identity.

- Operating system accounts for unprivileged backups

An unprivileged backup is a file-system backup of a client that does not run on the operating system as `root` on UNIX and Linux or as a member of the Administrators group on Windows. You must specify which operating system accounts are used for unprivileged backups.



See Also:

- ["Managing Users"](#) for more information about creating and managing users
- ["Assigning Preauthorized Access"](#) for more information about configuring preauthorization
- ["Configuring a User in an Administrative Domain"](#) for steps on setting up and managing user in an administrative domain

About Oracle Secure Backup Password Policies

Every time you log on to Oracle Secure Backup, you must enter a valid user name and user password. Oracle Secure Backup enables you to manage your user passwords and their lifetime by choosing appropriate security settings. You can configure the global password

settings, that apply to all users, while setting the global security policies. You also have the choice to specify user-specific settings while creating an [Oracle Secure Backup user](#). When password settings are not specified for a particular user, the global security password policies are automatically applied. When password settings are specified while creating a user, the user-specific settings override the global password settings.

You can configure and modify the following settings to manipulate the lifetime of your password:

Password Lifetime

Password lifetime is the length of time, measured in number of days, for which an Oracle Secure Backup user password is valid. Once the stated lifetime of a password expires, you are asked to change the password.

However, if [password grace time](#) has been set, you are allowed to log on using the current password for a limited number of days, after it's validity has expired.

You can also disable the [password lifetime](#), in which case the password will never expire. The Oracle Secure Backup Web tool enables you to set the password lifetime for an Oracle Secure Backup user.

Password Grace Time

Password grace time is the length of time, measured in number of days, for which an [Oracle Secure Backup user](#) can continue to log on to Oracle Secure Backup, after the validity of the current password has expired. The user receives a warning message while logging in, during the period for which the grace time has been set, indicating that the password will expire after the grace time ends. If you do not change your password by the time the set grace time ends, you are forced to change your password when you attempt to log on. You can choose to disable the [password grace time](#) in which case no grace time will be provided for that user.

Assume that you create an [Oracle Secure Backup user](#) `scott` and set the [password lifetime](#) to 60 days and the password grace time to 6 days. During the first Oracle Secure Backup login after the user password has expired, you will receive a message saying the current password has expired and you are recommended to change your password. You will not be forced to change the password immediately, but if you do not change the password, you will continue to receive the same message for the next six days as that is your password grace time. If the password is not changed even after the grace time expires, you will be presented with a password change screen during the next login. Once you change the password, you will be redirected to the user interface.

Password Reuse Time

Password reuse time is the duration, in number of days, that must elapse before you may reuse a previously-used Oracle Secure Backup password. You can choose to disable the [password reuse time](#), in which case the password can never be reused.

Forcing a Password Change

You can force an [Oracle Secure Backup user](#) to change their current password, if required. The user must implement the forced password change, regardless of the password settings that were set during the user configuration.

 **Note:**

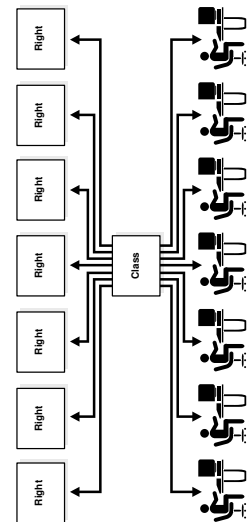
To modify Oracle Secure Backup users, you must be a member of a class that has this right enabled. See "[Overview of Oracle Secure Backup Classes and Rights](#)" for details.

Overview of Oracle Secure Backup Classes and Rights

An Oracle Secure Backup class defines a set of rights granted to an Oracle Secure Backup user. A class is similar to a Linux or UNIX group, but it defines a finer granularity of access rights tailored to the needs of Oracle Secure Backup.

As shown in [Figure 2-1](#), you can assign multiple Oracle Secure Backup users to a class. Each Oracle Secure Backup user can be a member of only one class.

Figure 2-1 Classes and Rights



The following classes are key to understanding Oracle Secure Backup user rights:

- `admin`
This class is used for overall management of an administrative domain. The `admin` class has all the rights needed to modify administrative domain configurations and perform backup and restore operations.
- `operator`
This class is used for standard day-to-day operations. The `operator` class lacks configuration rights but has all the rights needed for backup and restore operations. It also allows the Oracle Secure Backup user to query the state of any primary or secondary storage device and to control the state of these devices.
- `oracle`
This class is similar to the `operator` class. The `oracle` class has all rights necessary to modify Oracle Database configuration settings and to perform Oracle Database backups. Class members are usually Oracle Secure Backup users that are mapped to operating system accounts of Oracle Database installations.
- `user`
This class gives Oracle Secure Backup users permission to interact in a limited way with their domains. This class is reserved for Oracle Secure Backup users who must browse their own data within the Oracle Secure Backup [catalog](#) and perform user-based restore operations.

- `reader`

This class enables Oracle Secure Backup users only to modify the given name and password for their user account and to browse their own catalog. Users in the `reader` class must know the exact restore path that they own, because they are not even able to see a listing of what hosts belong to the Oracle Secure Backup administrative domain.

When creating a user in the `reader` class, you must map the user to a valid operating system user and group.

- `monitor`

This class enables Oracle Secure Backup users only to access Oracle Database backups, access file-system backups, display the administrative domain configuration, list all jobs, and display information about devices. Users in this class cannot perform backup or restore operations, modify the administrative domain, or receive email notifications.

An Oracle Secure Backup user assigned to the `monitor` class is necessary as the `OSB_username` parameter in Oracle Secure Backup target registration within Oracle Enterprise Manager.

See Also:

- ["Managing Classes"](#) for a detailed description of the rights available to each class
- [Oracle Secure Backup Reference](#) for more information about classes and rights

Managing Users

Oracle Secure Backup users are managed in their own namespace, distinct from operating system users. This section describes how to create and manage an Oracle Secure Backup user with the Web tool.

This section contains these topics:

- [Displaying the Oracle Secure Backup Web Tool Home Page](#)
- [Displaying the Users Page](#)
- [Adding a User](#)
- [Editing or Displaying User Properties](#)
- [Changing a User Password](#)
- [Assigning Windows Account Information](#)
- [Assigning Preauthorized Access](#)
- [Renaming a User](#)
- [Removing a User](#)

See Also:

- ["About Operating System Accounts"](#)

Displaying the Oracle Secure Backup Web Tool Home Page

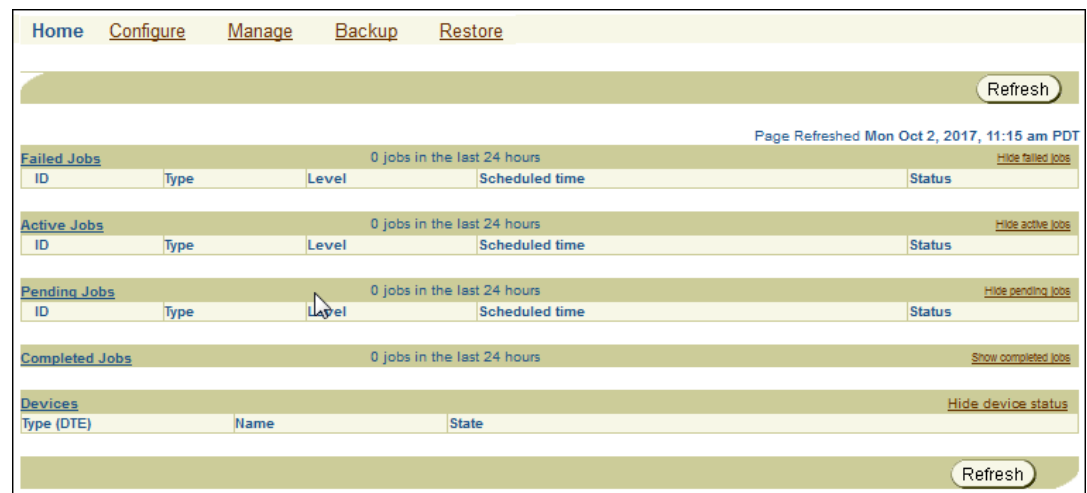
Accessing the Oracle Secure Backup web tool home page is the first step in performing all Oracle Secure Backup backup and restore operations.

To access the Oracle Secure Backup web tool home page:

1. Enter the URL of your Oracle Secure Backup web tool for your host in your web browser. The URL for the interface should have its format as *https://hostname:portnumber*.
2. Add the security certificate for this URL and confirm the security exception on the **Security Alert** page to proceed.
3. Enter your administrative credentials on the Oracle Secure Backup Login page. Enter your username and your administrative user password in the **User Name** and **Password** fields, respectively.

The Oracle Secure Backup: Home Page appears as shown in the following figure.

Figure 2-2 Oracle Secure Backup Home Page

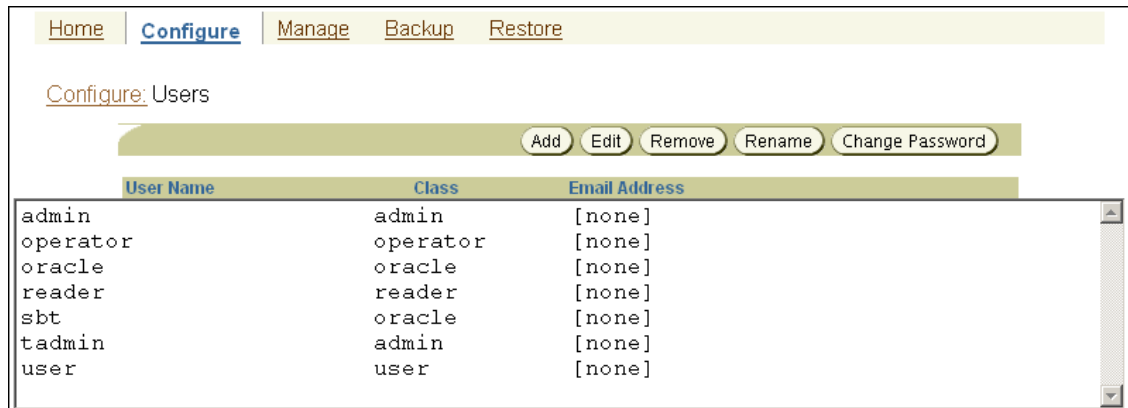


Displaying the Users Page

To display the Users page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)". The Oracle Secure Backup: Home Page appears
2. Click **Configure**.
3. On the Configure page, click **Users** to display the Users page, which is shown in [Figure 2-3](#). This page lists all users authorized by Oracle Secure Backup along with their class names and email addresses. You can perform all user configuration tasks in this page or in pages to which it provides links.

Figure 2-3 Users Page



User Name	Class	Email Address
admin	admin	[none]
operator	operator	[none]
oracle	oracle	[none]
reader	reader	[none]
sbt	oracle	[none]
tadmin	admin	[none]
user	user	[none]

**See Also:**

Oracle Secure Backup Reference to learn about the user commands in `obtool`

Adding a User

You can use the Web tool 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.

To add one or more users:

1. Follow the steps in "[Displaying the Users Page](#)".

The Configure: Users page appears.

2. Click **Add**.

The Configure: Users > New Users page appears.

3. Enter a user name in the **User** field.

The name you enter must start with an alphanumeric character. It can contain only letters, numerals, dashes, underscores, or periods. The maximum character length that you can enter is 31 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. Practically, it is helpful to choose Oracle Secure Backup user names that are identical to operating system user names.

4. Enter a password in the **Password** field.

This password is used to log in to Oracle Secure Backup. The maximum character length that you can enter is 16 characters.

 **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.

5. Select a class in the **User class** list.

A class defines a set of [rights](#).

 **See Also:**

["Overview of Oracle Secure Backup Classes and Rights"](#)

6. Enter a name for the Oracle Secure Backup user in the **Given name** box.

This step is optional. The given name is for information purposes only.

7. Enter a UNIX name for this account in the **UNIX name** field.

This name forms the identity of any non-privileged jobs run by the Oracle Secure Backup user on UNIX systems. If you do not want this Oracle Secure Backup user to run Oracle Secure Backup jobs on UNIX systems, then leave this field blank.

8. Enter a UNIX group name for this account in the **UNIX group** field.

This name forms the identity of any non-privileged jobs run by the Oracle Secure Backup user on UNIX systems. If you do not want this Oracle Secure Backup user to run Oracle Secure Backup jobs on UNIX systems, then leave this field blank.

9. Select **yes** in the **NDMP server user** list to request that NDMP servers in the Oracle Secure Backup administrative domain accept a login from this Oracle Secure Backup user by using the supplied user name and password.

This option is not required for normal Oracle Secure Backup operation and is typically set to **no**.

10. Enter the email address for the Oracle Secure Backup user in the **Email Address** field.

When Oracle Secure Backup communicates with this user, for example to deliver a [job summary](#) or notify the user of a pending input request, it sends email to this address.

11. Enter the duration of the password grace time in the **Password grace time** field. You can select the system default which is 3 days.

12. Enter the duration of the password lifetime in the **Password lifetime field**. You can select the system default which is 180 days.

13. Enter the duration of the password reuse time in the **Password reuse time** field. You can select the system default which is 1 year.

 **See Also:**

["About Oracle Secure Backup Password Policies"](#) for detailed description of the available password settings

14. Click **Apply**, **OK**, or **Cancel**.
15. If the Oracle Secure Backup user you configured must initiate backup and restore operations on Windows clients, then see "[Assigning Windows Account Information](#)".

Editing or Displaying User Properties

This section explains how to modify properties for an existing user account.

Note:

To modify Oracle Secure Backup users, you must be a member of a [class](#) that has this right enabled. See "[Overview of Oracle Secure Backup Classes and Rights](#)" for details.

To edit Oracle Secure Backup user properties:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. Select an Oracle Secure Backup user whose properties you want to modify from the **User Name** list.
3. Click **Edit**.
The Configure: Users > *user_name* page appears.
4. Edit the required user properties.

See Also:

"[Adding a User](#)" for information on setting user properties

You cannot change the name of an Oracle Secure Backup user on this page. To rename an Oracle Secure Backup user, see "[Renaming a User](#)".

5. Click **Apply** to apply the changes and remain on the Configure: Users > *user_name* page.
6. Click **OK** to apply the changes and return to the Configure: Users page.
7. Click **Cancel** to return to the Configure: Users page without making any changes.
8. If the Oracle Secure Backup user you configured must initiate backup and restore operations on Windows clients, then see "[Assigning Windows Account Information](#)".

Changing a User Password

This section explains how to modify the password for an existing user account.

 **Note:**

To modify Oracle Secure Backup users, you must be a member of a class that has this right enabled. See "[Overview of Oracle Secure Backup Classes and Rights](#)" for details.

To change an Oracle Secure Backup user password:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. From the **Users** page, select an Oracle Secure Backup user from the **User name** list.
3. Click **Change Password**.
The Configure: Users > *user_name* page appears.
4. Enter a password.
5. Confirm the password.
6. Click **OK** or **Cancel**.

 **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.

Configuring a User in an Administrative Domain

It is recommended that you follow these steps to set up and manage Oracle Secure Backup users in your administrative domain:

1. Add Oracle Secure Backup users by following the steps in "[Adding a User](#)", if necessary.
2. Change the `admin` password if necessary.

You set the original password when you installed Oracle Secure Backup on the administrative server. "[Changing a User Password](#)" describes this task.

 **See Also:**

"[About Oracle Secure Backup Password Policies](#)" for more information about the available password settings

3. Review the attributes of each Oracle Secure Backup user.
"[Editing or Displaying User Properties](#)" describes this task.
4. Configure preauthorization and account settings for unprivileged backups if necessary.

"Assigning Windows Account Information", and "Assigning Preauthorized Access" describe this task.

Assigning Windows Account Information

This section explains how to configure Windows account information for a user who must initiate backups and restore operations on Windows systems. You can associate an Oracle Secure Backup user with multiple Windows **domain** accounts or use a single account that applies to all Windows domains.

To assign Windows account information to an Oracle Secure Backup user:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. Select an Oracle Secure Backup user in the **User Name** list.
3. Click **Edit**.
The Configure: Users > *user_name* page appears.
4. Click **Windows Domains**.
The Configure: Users > *user_name* > Windows Domains page appears.
5. Enter a Windows domain name in the **Domain name** field.
Enter an asterisk (*) in this field to associate this Oracle Secure Backup user with all Windows domains.
6. Enter the account information for a Windows user in the **Username** and **Password** fields.
7. Click **Add** to add the Windows account information.
The page displays a success message, and account information appears in the **Domain:Username** list.

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.

Removing a Windows Account

You can use the Web tool to remove Windows account information from an Oracle Secure Backup user account.

To remove a Windows account:

1. From the Windows Domain page, select a Windows account in the **Domain: Username** list.
2. Click **Remove**.
The Configure: Users > *user_name* > Windows Domains page displays a message informing you that the Windows account was successfully removed.

Assigning Preauthorized Access

This section explains how to give access to Oracle Secure Backup services and data to a specified operating system user. You can preauthorize Oracle Database SBT backups through RMAN or preauthorize login to the user-invoked Oracle Secure Backup command-line utilities.

Oracle Secure Backup preauthorizes access only for a specified operating system user on a 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 user and Oracle Secure Backup user identities.

You can create a preauthorization only if you have the `modify administrative domain's configuration` right. Typically, only an Oracle Secure Backup user in the `admin` class has this right.



See Also:

Oracle Secure Backup Reference for more information about the `modify administrative domain's configuration` right

To assign preauthorized access:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. Select an Oracle Secure Backup user in the **User Name** list.
3. Click **Edit**.
The Configure: Users > *user_name* page appears.
4. Click **Preauthorized Access**.
The Configure: Users > *user_name* > Preauthorized Access page appears.
5. In the **Hosts** list, select either **all hosts** or the name of the host to which the operating system user is granted preauthorized access.
6. In the **OS username** field, enter the operating system user account with which the Oracle Secure Backup user should access services and data. Enter an asterisk (*) or leave blank to select all operating system users.
7. In the **Windows domain name** field, enter the Windows domain to which the operating system user belongs. The Windows domain is only applicable to preauthorized logins from a Windows host. Enter an asterisk (*) or leave blank to select all domains.
If you enter a Windows account name in the **OS username** field, then you must enter an asterisk, leave the box blank, or enter a specific domain.
8. In the **Attributes** list, select **cmdline**, **rman**, or both.
You can select both attributes by clicking one of them and then shift-clicking the other.
The **cmdline** attribute preauthorizes login through the user-invoked Oracle Secure Backup command-line utilities such as `obtool`. The **rman** attribute preauthorizes Oracle Database SBT backups through RMAN.
9. Click **Add**.

The page displays a success message, and the preauthorized Oracle Secure Backup user appears in the list.

 **See Also:**

"[Creating a Preauthorized Oracle Secure Backup User](#)" for more details about RMAN preauthorization

Removing Preauthorized Access

You can remove a preauthorization only if you have the `modify administrative domain's configuration` right. Typically, only an Oracle Secure Backup user in the `admin` class has this right.

To remove preauthorized access:

1. From the Configure: Users > `user_name` > Preauthorized Access page, select the preauthorized access entry you want to remove in the main text pane.
2. Click **Remove**.

The preauthorized access entry is no longer displayed in the main text pane.

Renaming a User

You must have the `modify administrative domain's configuration` right to rename an Oracle Secure Backup user.

To rename an Oracle Secure Backup user:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. Select the Oracle Secure Backup user whose name you want to change from the **User Name** list.
3. Click **Rename**.

A different page appears.

4. Enter the name in the **Rename `user_name` to** field and click **Yes**.

The Configure: Users page displays a success message, and the Oracle Secure Backup user has a different name in the **User Name** list

Removing a User

You must have the `modify administrative domain's configuration` right to remove an Oracle Secure Backup user.

To remove an Oracle Secure Backup user:

1. Follow the steps in "[Displaying the Users Page](#)".
The Configure: Users page appears.
2. Select the Oracle Secure Backup user you want to remove from the **User Name** list.

3. Click **Remove**.

A confirmation page appears.

4. Click **Yes** to remove the Oracle Secure Backup user.

You are returned to the Configure: Users page. A message appears telling you the Oracle Secure Backup user was successfully removed.

Managing Classes

A class defines a set of rights that are granted to a user. A class can include multiple Oracle Secure Backup users, but each Oracle Secure Backup user is a member of one and only one class. In most cases, the default classes are sufficient.

This section contains these topics:

- [Displaying the Classes Page](#)
- [Adding a Class](#)
- [Editing or Displaying Class Properties](#)
- [Removing a Class](#)
- [Renaming a Class](#)



See Also:

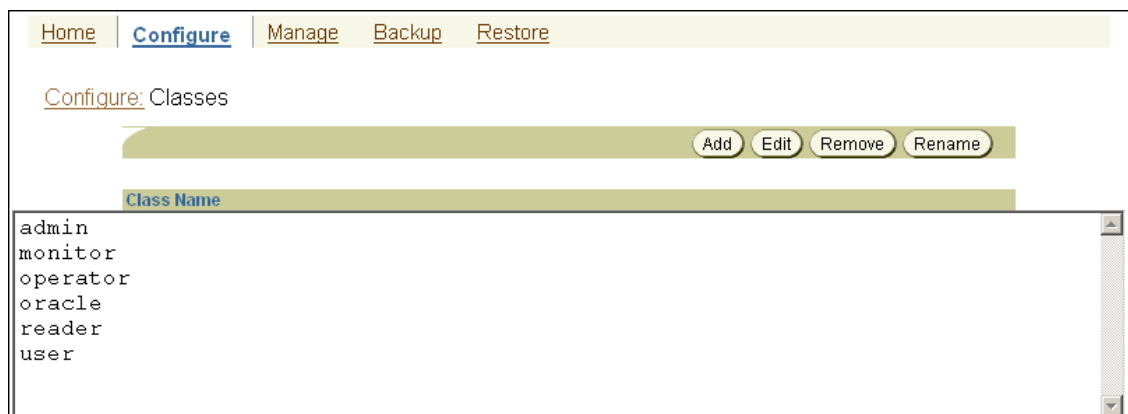
["Overview of Oracle Secure Backup Classes and Rights"](#)

Displaying the Classes Page

To display the Oracle Secure Backup: Classes Page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Configure**.
3. In the Advanced section of the Configure page, click **Classes** to display the Configure: Classes page, as shown in [Figure 2-4](#). You can use this page to manage existing classes or configure additional classes.

Figure 2-4 Classes Page



**See Also:**

Oracle Secure Backup Reference to learn about the class commands in `obtool`

Adding a Class

Oracle Secure Backup creates default classes when the administrative domain is first initialized. You can use these classes or create your own.

To add a class:

1. Follow the steps in "[Displaying the Classes Page](#)"

The Configure: Classes page appears.

2. Click **Add**.

The Configure: Classes > New Classes page appears. This page lists class rights options.

3. Enter a name for the class in the **Class** field.

The name you enter must start with an alphanumeric character. It can contain only letters, numerals, dashes, underscores, or periods. The maximum character length is 127 characters.

The class name must be unique among all Oracle Secure Backup class names. It is unrelated to any other name used in your computing environment or the Oracle Secure Backup administrative domain.

4. Select the rights to grant to this class.

**See Also:**

Oracle Secure Backup Reference for a detailed explanation of these rights

5. Click **Apply** or **OK**.

The Configure: Classes page displays a success message, and your additional class appears in the list of classes.

Editing or Displaying Class Properties

To modify existing classes, you must have the `modify administrative domain's configuration` right. When you change the class that an Oracle Secure Backup user belongs to or modify the rights of such a class, changes do not take effect until the user exits from the Oracle Secure Backup component currently in use.

**See Also:**

Oracle Secure Backup Reference for more information about the `modify administrative domain's configuration` right

To edit a class:

1. Follow the steps in "[Displaying the Classes Page](#)"
The Configure: Classes page appears.
2. Select the name of the class to edit in the **Class Name** list.
3. Click **Edit**.
The Configure: Classes > *class_name* page appears with details for the class you selected.
4. Make the required changes.
You cannot rename a class from this page. To rename a class, see "[Renaming a Class](#)".
5. Click **Apply** to apply your changes and remain on the Configure: Classes > *class_name* page.
6. Click OK to apply your changes and return to the Configure: Classes page.
7. Click Cancel to return to the Configure: Classes page without making any changes.

Removing a Class

You cannot remove a class to which a user currently belongs. Instead, you must reassign or delete all existing members of a class before the class can be removed.

To remove a class:

1. Follow the steps in "[Displaying the Classes Page](#)"
The Configure: Classes page appears.
2. Select the class to be removed in the **Class Name** list.
3. Click **Remove**.
A confirmation page appears.
4. Click **Yes**.
The Configure: Classes page displays a success message, and the class is gone from the Class Name list.

Renaming a Class

You must have the `modify administrative domain's configuration` right to rename a class.

To rename a class:

1. Follow the steps in "[Displaying the Classes Page](#)"
The Configure: Classes page appears.
2. Select the class to rename in the **Class Name** list.
3. Click **Rename**.
A different page appears.
4. Enter the name for the class in the **Rename *class_name* to** field and click **Yes**.
The Configure: Classes page displays a success message, and the class appears with its different name in the Class Name list.

Managing Defaults and Policies

Defaults and policies control how Oracle Secure Backup operates within an administrative domain. Defaults and policies are divided into classes, depending upon what area of functionality they control. Each policy has a default setting, which you can modify based on your business or backup requirement.



See Also:

"[About Defaults and Policies](#)" for more information about the classification of policy classes

This section contains these topics:

- [Viewing Configured Defaults and Policies Values](#)
- [Setting a Policy](#)
- [Resetting a Policy](#)

Viewing Configured Defaults and Policies Values

To view the Oracle Secure Backup: Defaults and Policies Page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Configure**.
3. In the Advanced section of the Configure page, click **Defaults and Policies** to display the page shown in [Figure 2-5](#). This page lists the policy classes.

Figure 2-5 Defaults and Policies Page

Policy	Description
Backup compression	policies for backup compression operations
Backup encryption	policies for backup encryption operations
Cloud	cloud related policies
Copy instance	copy instance policies
Daemons	daemon and service control policies
Devices	device management policies
Duplication	duplication-related policies
Index	index catalog generation and management policies
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	backup scheduler policies
Security	security-related policies
Staging	staging-related policies
Testing	controls for test and debug tools
Vaulting	policies for media life cycle management operations

See Also:

Oracle Secure Backup Reference to learn about the policy commands in the `obtool` command-line interface and the descriptions of the defaults and policies

Setting a Policy

Before changing a policy setting, refer to the "Defaults and Policies" chapter in *Oracle Secure Backup Reference*. This chapter contains extensive descriptions of the policies and describes valid settings. You should not ordinarily be required to change the default settings.

To change a policy setting:

1. Follow the steps in "[Viewing Configured Defaults and Policies Values](#)".
2. In the Policy column on the Defaults and Policies page, click the name of the policy class to be edited. For example, click **scheduler**.

The `policy_name` page appears. [Figure 2-6](#) shows the Scheduler page.

Figure 2-6 Unmodified Scheduler Page

Name	Current Value	Reset to Default Value
Apply backups frequency	5 minutes	
Cache all jobs	yes	
Default start time	00 hours 00 minutes	
Max data retries	6	
Poll frequency	30 minutes	
Recycle jobs threshold	90000	
Retain backup metrics	no	

3. Change the settings of one or more policies.
4. Do one of these:
 - Click **Apply** to remain on this page.
 - Click **OK** to save the changes and return to the Defaults and Policies page.

When you change a policy setting from its default, the Web tool displays the default value for the policy in the Reset to Default Value column.

Resetting a Policy

You can use the Web tool to reset the value of one or more Oracle Secure Backup policies to the default value.

To reset a policy:

1. Follow the steps in "[Viewing Configured Defaults and Policies Values](#)".
2. In the Policy column on the Defaults and Policies page, click the name of the policy class that contains the policy to be reset.
3. Select the **Reset to Default Value** column for the policy that you are resetting.
4. Click **Apply** or **OK**.

3

Managing Backup and Media Settings

This chapter explains how to configure backup and media settings for an [administrative domain](#).

This chapter contains these sections:

- [Overview of Backup and Media Settings Configuration](#)
- [Configuring Media Families](#)
- [Configuring Database Backup Storage Selectors](#)
- [Configuring Job Summary Schedules](#)

Overview of Backup and Media Settings Configuration

To begin managing your file-system and Oracle Database backups, install Oracle Secure Backup on your host (expect NDMP servers and NAS filers) and then configure your administrative domain. After the administrative domain is configured, the storage devices are available to store backups.

See Also:

Oracle Secure Backup Installation and Configuration Guide for information about configuring the administrative domain

You can perform additional configuration that enables you to manage your storage media. Configuring media families enables you to assign common characteristics to a set of tape volumes or [disk pools](#). A media family is a named classification of volume sets that share certain common attributes. Use media families to logically group volumes or volume sets. They ensure that volumes created at different times share common characteristics.

Oracle Secure Backup provides policy-based media management for Oracle Database backups through the use of [database backup storage selector](#). A database backup storage selector specifies the parts of the database that need to be backed up, the media family that must be used for this backup, and the devices that can be used to store the backed up data.

Oracle Secure Backup automatically uses the storage selections defined within a database backup storage selector while backing up an Oracle Database. You can override the storage selections for one-time backup operations by defining alternate media management parameters in the RMAN backup script.

Configuring Media Families

A [media family](#) is a logical classification of volumes that share common attributes. Volumes in a media family share a common naming pattern and policies used to write and keep backup data.

A media family has either of the following types of volume [expiration policy](#) types: content-managed (default) or time-managed. Content-managed volumes expire only when every [backup piece](#) recorded on a [volume](#) has been marked as deleted. Time-managed volumes expire when they pass the duration expressed by the sum of the [write window time](#) (if specified), [retention period](#), and [volume creation time](#).

The only default media family is `RMAN-DEFAULT`, which is a content-managed media family used only for RMAN backups. You cannot delete or rename this media family, although you can modify certain of its attributes.

**See Also:**

["Editing or Displaying Media Family Attributes"](#)

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

It is useful to create media families for the following backup types:

- Full backups
- Incremental backups
- Off-site backups

This media family contains volumes with no expiration time. These volumes, which are stored off-site, are intended for disaster recovery or long-term storage.

- Scratch backups

This media family is intended for test backups or backup and restore work that occurs outside your usual [backup schedule](#).

This section contains these topics:

- [Displaying Defined Media Families](#)
- [Adding a Media Family](#)
- [Editing or Displaying Media Family Attributes](#)
- [Removing a Media Family](#)

**Note:**

You can also manage media families with the Oracle Secure Backup [Web tool](#).

**See Also:**

["About Media Families"](#)

Displaying Defined Media Families

You can use Oracle Secure Backup Web tool to display every defined media family. You must have the `display administrative domain's configuration` right to view the families.

To display defined media families:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup web tool home page, click **Configure**.

The Configure page appears.

3. In the Basic section, click **Media Families**.

The Oracle Secure Backup Configure: Media Families page appears.

4. The Media Families page displays a list of all currently defined media families. It also specifies the write window and volume expiration details for each media family.

You also have the Edit, Remove, and Add options for each entry. These are described in the following sections.

See Also:

Oracle Secure Backup Reference to learn about the media family commands in `obtool`

Adding a Media Family

Use the Oracle Secure Backup web tool to create a media family. A media family ensures that volumes created at different times have similar characteristics.

To add a media family:

1. Follow the steps in "[Displaying Defined Media Families](#)".

The Oracle Secure Backup Configure: Media Families page appears.

2. Click **Add**.

The Add Media Family page appears.

3. In **Media Family Name**, enter a name for your 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.

4. For **Volume ID Used**, select one of the following:

- **System Default**
Select this option to specify the default volume ID used.
- **Unique to this Media Family**
Select this option to set a unique volume ID for this media family.
- **Same as for Media Family**

Select this option to set the same volume ID as an already existing media family

- **From File**

Select this option to specify the volume sequence file for this media family.

 **See:**

Oracle Secure Backup Reference for more information about volume ID options

5. For **Volume Expiration**, select one of the following options:

- **Time Managed: Keep Volume Sets**

By specifying this option, you indicate that this media family is time-managed and not content-managed. If you select this option, then you must also specify a value in the adjacent field and select a time unit from the adjacent list.

The retention period of the media family 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 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.

- **Content Managed**

Volumes that use this option 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 a [backup piece](#) through [Recovery Manager \(RMAN\)](#) or through the `mpiece` command in `obtool`. A volume in a content-managed volume set can expire even though other volumes in the same set are not expired.

6. In **Write Window**, enter an amount of time.

You can choose Seconds, Minutes, Hours, Days, Weeks, Months, Years, or Forever in the list to the right of the Write Window field.

A write window is the period for which a volume set remains open for updates, usually by another [backup image](#). Every volume in the family is 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. It closes when the specified period elapses. When the write window closes, Oracle Secure Backup disallows further updates to the volume set until one of these 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 the next backup operation until the write window closes.

7. In **Appendable**, select one of the following:

- **Yes**

The media family allows additional [backup image instances](#) to be appended to the volumes.

- **No**

The media family does not allow additional backup image instances to be appended to the volumes.

The Media Families page appears with a success message and an entry for your additional media family.

8. In **Rotation Policy**, select a policy from the list of defined rotation policies to manage the life cycle of volumes in the media family.
9. In **Volume Duplication Policy**, select a policy from the list of defined duplication policies to manage the creation of duplicate volumes.

 **Note:**

The **Rotation Policy** and **Volume Duplication Policy** options show information only if you have set up a vaulting environment. See [Vaulting](#) to learn more about vaulting.

10. In **ACSL Scratch ID**, enter the ID of the volume if it is located in the ACSLS library.
11. In **Comment**, enter a description of the media family (optional) and click **OK**.

The Media Families page appears with a success message and an entry for your additional media family.

Editing or Displaying Media Family Attributes

Use the Oracle Secure Backup web tool to edit any attributes of a user-defined media family so long as you have the `modify administrative domain's configuration` right. You can also edit any attributes of the `RMAN-DEFAULT` media family except for `write window` or `keep volume set`.

To display or edit attributes for an existing media family:

1. Follow the steps in "[Displaying Defined Media Families](#)".

The Oracle Secure Backup Configure: Media Families page appears.

2. Select the media family you want to display or edit and click **Edit**.

The Media Family page appears with fields and options set to the existing values for the selected media family.

3. Make the required changes, click **Apply**, and then **OK**.

The Media Families page appears with a success message and the values for your edited media family.

Renaming a Media Family

You can use the Oracle Secure Backup Web tool to rename a media family. You must have the `modify administrative domain's configuration` right to rename a media family.

To rename a media family:

1. Follow the steps in "[Displaying Defined Media Families](#)".

The Oracle Secure Backup Configure: Media Families page appears.

2. Select the media family you want to rename and click **Rename**.

A confirmation screen appears.

3. Enter the new name for the media family and click **Yes**.

The Media Families page appears with a success message and the renamed media family.

Removing a Media Family

Use the Oracle Secure Backup Web tool to delete a media family from the domain. Note that removing a media family does not affect the metadata in the backup container that was originally written using that media family.

To remove a media family:

1. Follow the steps in "[Displaying Defined Media Families](#)".

The Oracle Secure Backup Configure: Media Families page appears.

2. Select the media family you want to remove and click **Remove**.

A Confirmation page appears.

3. Click **Yes**.

The Media Families page appears with a success message and no entry for the deleted media family.

Configuring Database Backup Storage Selectors

A [database backup storage selector](#) associates an RMAN backup with Oracle Secure Backup storage media. For example, you can specify that RMAN backups of archived redo logs from the `orcl` database should use the `orcl_log` media family.

You can use the Oracle Secure Backup Web tool to create a storage selector. To create a storage selector with `obtool`, use the `mkssel` command.

One [database backup storage selector](#) may apply to multiple Oracle Databases. Also, multiple database backup storage selectors can be associated with one Oracle Database. For example, you can create two database backup storage selectors for a database when you use RMAN duplexing and each copy can be written to a different media family.

The database backup storage selector contains the following information:

- Database name or Database ID of the database to be backed up

If this is omitted, the selector is applicable to all databases.

- Host name

If this is omitted, the selector is applicable to all hosts.

- Content to be backed up
- Media family name
- Devices to which operations are restricted

If no device restrictions are configured, Oracle Secure Backup uses any available device.

- Wait time (duration) for available tape resources
- Number of backup copies to create (when RMAN duplexing is enabled)
- Encryption settings

This section contains these topics:

- [Displaying Defined Database Backup Storage Selectors](#)
- [Adding a Database Backup Storage Selector](#)
- [Editing a Database Backup Storage Selector](#)
- [Removing a Database Backup Storage Selector](#)



Note:

You can also manage database backup storage selectors with the Oracle Secure Backup Web tool.

Displaying Defined Database Backup Storage Selectors

You must have the `display administrative domain's configuration` right to display storage selectors.

To display defined database storage selectors:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool home page, click **Configure**.

The Configure page appears.

3. In the Basic section, click **Database Backup Storage Selectors**.

The Configure:Database Backup Storage Selectors page appears.

Adding a Database Backup Storage Selector

You can use the web tool 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).

To configure a database backup storage selector:

1. Perform the steps in "[Displaying Defined Database Backup Storage Selectors](#)".

- The Configure: Database Backup Storage Selectors page appears.
- On the Database Backup Storage Selectors Page, click **Add**.
The New Database Backup Storage Selector page appears as shown in [Figure 3-1](#).

Figure 3-1 New Database Backup Storage Selector Page

The screenshot shows a web-based configuration form for a Database Backup Storage Selector. The form is titled "Name" and has a value of "store_sel". Below this are several sections:

- Backup Image Name:** An empty text input field.
- Content:** A dropdown menu with options: "all", "full", "incr", "archive log", and "auto backups".
- Database(s):** A text input field with a note: "Use * for all database names".
- Database ID(s):** A text input field with a note: "Use * for all database ids".
- Host:** A dropdown menu with the value "brhost1".
- Media family:** A dropdown menu with the value "OSB-CATALOG-MF".
- Restrictions:** An empty text area.
- Copy number:** A dropdown menu with the value "*".
- Resource wait time:** A dropdown menu with the value "forever".
- Encryption:** Radio buttons for "on", "off" (selected), "forced off", and "software encryption".
- Priority:** Radio buttons for "default" (selected) and an empty text input field.

At the top right and bottom right of the form are buttons for "Apply", "OK", and "Cancel".

- In the **Name**, enter a name for backup storage selector.
Database Backup Storage Selector names are case-sensitive and must begin with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They can contain a maximum of 31 characters.
- Under **Content**, select one of the following backup types:
 - All**
 - Full**
 - Incremental**
 - Archive log**
 - Auto backups**

5. For **Database**, you can specify the name of the database that needs to be backed up.
6. For **Database ID**, you can specify the ID of the database that needs to be backed up.
7. For **Host**, select a host from the list of hosts.
8. In **Media Family**, select a media family.
9. For **Restrictions**, select one or more restrictions on this volume. If no device is selected, then Oracle Secure Backup uses tape device polling to find any available tape device for use in backup and restore operations.
10. In **Copy Number**, select a copy number.
If you leave the Copy Number list at the default (*), then this storage selector applies to all backups.
11. In **Resource Wait Time**, enter a value and select a unit from the adjacent list. The default is `Forever`.
The resource wait time specifies how long to wait for the availability of resources required by backups. If resources do not become available within this time, then the backup fails.
12. In **Encryption**, select one of the following options to indicate the type of encryption.
 - **on**: The backup data is encrypted, unless it is already encrypted by RMAN.
 - **off**: The backup data is not encrypted unless either the host or global policy is set to required. This is the default setting.
 - **forced off**: The backup data is not encrypted, overriding any host-specific encryption settings. This setting does not affect RMAN, which can still encrypt the backup data.
 - **software encryption**: Uses software encryption to encrypt data instead of hardware encryption.
13. In **Priority**, either select the Default option or enter a positive numeric value. The lower the value, the greater the importance assigned to the job by the scheduler. The scheduler gives preference to dispatching more important jobs over those having lesser importance. The default priority is 100.
14. Click **Apply** and **OK**.

The Backup Storage Selectors page appears with a success message. The additional database backup storage selector appears in the list.

Editing a Database Backup Storage Selector

You must have the modify administrative domain's configuration right to modify a storage selector.

To edit parameters for an existing database backup storage selector:

1. Perform the steps in "[Displaying Defined Database Backup Storage Selectors](#)".
The Configure: Database Backup Storage Selectors page appears.
2. Select a Database Backup Storage Selector from the list of configured storage selectors and click **Edit**.
The Edit Backup Storage Selector page appears.
3. Make the required changes to the selected backup storage selector, click **Apply** and then click **OK**.

The Backup Storage Selectors page displays a success message and the changes you made to the selected backup storage selector.

Renaming a Database Backup Storage Selector:

You can use the Oracle Secure Backup Web tool to rename a backup storage selector. You must have the `modify administrative domain's configuration` right to rename a backup storage selector.

To rename a database backup storage selector:

1. Perform the steps in "[Displaying Defined Database Backup Storage Selectors](#)".

The Oracle Secure Backup Configure: Database Backup Storage Selector

2. Select the backup storage selector you want to rename and click **Rename**.

A confirmation screen appears.

3. Enter a new name for the storage selector and click **Yes**.

The Database Backup Storage Selector page appears with a success message and the renamed backup storage selector.

Removing a Database Backup Storage Selector

You must have the `modify administrative domain's configuration` right to remove a storage selector.

To remove a database backup storage selector:

1. Perform the steps in "[Displaying Defined Database Backup Storage Selectors](#)".

The Configure: Database Backup Storage Selector page appears.

2. Select the backup storage selector from the list configured storage selectors to remove and click **Remove**.

A confirmation page appears.

3. Click **Yes**.

The Backup Storage Selectors page displays a success message, and the selected backup storage selector does not appear in the list.

Configuring Job Summary Schedules

A [job summary](#) is a report that describes the status of selected file-system backup or restore jobs, database backup or restore jobs, media movement jobs or duplication jobs. You can configure a [job summary schedule](#) that indicates when the reports should be generated and who should receive them.

It is recommended that you create at least one job summary schedule so that you receive an automated email describing the status of each [backup job](#) that you have scheduled.

This section contains these topics:

- [Displaying the Defined Job Summaries Page](#)
- [Creating a Job Summary Schedule](#)
- [Editing a Job Summary Schedule](#)

- [Removing a Job Summary Schedule](#)
- [Renaming a Job Summary Schedule](#)



See Also:

["About Job Summaries"](#)

Displaying the Defined Job Summaries Page

You must have the `display administrative domain's configuration right to list job summaries`.

To display the list of currently defined job summaries with the Web tool:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Advanced section, click **Job Summaries**.
The Configure: Job Summaries page appears as shown in [Figure 3-2](#).

Figure 3-2 Configure Job Summaries Page

Summary Name	Produce On	Covers Preceding
OSB-CATALOG-SUM	daily at 06:00	24 hours

4. The Configure: Job Summaries page lists all currently defined job summaries by name. It also shows when each job summary runs and what period it covers.



See Also:

Oracle Secure Backup Reference to learn about the job summary commands in `obtool`

Creating a Job Summary Schedule

You can use the Web tool 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.

To create a job summary schedule:

1. Perform the steps in "Displaying the Defined Job Summaries Page".
The Configure: Job Summaries page appears.
2. Click **Add**.
The Configure: Job Summaries > New Job Summaries page appears as shown in Figure 3-3.

Figure 3-3 New Job Summaries Page

3. Enter a name for the job summary in the **Summary** field.
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.
4. Select one of these options:

- **Select daily**
This option produces a daily job summary, seven days a week.
 - **Select weekdays**
This option produces a daily job summary, Monday through Friday.
 - **Select weekend**
This option produces a job summary only on Saturday and Sunday.
 - Select one or more days of the week
5. Select a time to produce the job summary from the **hours** and **minutes** lists.
 6. Enter an email address in the **Mail to** field.

This option 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.
 7. Select one of these schedule options:
 - **Cover preceding**
This option specifies a time frame for the report. Enter a value in the adjacent field and select a unit from the list. If you are producing daily reports, for example, then you might enter 24 in this field and select hours in the list.
 - **Since**
This option specifies a starting point for the time period that the report covers. Select a day of the week from the adjacent list and a time in the **hours** and **minutes** lists.
 8. Select report options. You can enable or disable each of the following options independently of other report options:
 - **Backup jobs**
This option specifies whether file-system backup jobs should be included in the report.
 - **Oracle backup jobs**
This option specifies whether RMAN backup jobs should be included in the report.
 - **Scheduled jobs**
This option 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.
 - **Subordinate jobs**
This option specifies whether the report should include subordinate jobs.
 - **Volume duplication jobs**
This option specifies whether volume duplication jobs should be included in the report.
 - **Restore jobs**
This option specifies whether file-system restore jobs should be included in the report.
 - **Oracle restore jobs**
This option specifies whether RMAN backup jobs should be included in the report.
 - **User jobs**
This option specifies whether the report should include user-initiated jobs. If this option is set to `no`, then the summary only shows scheduled jobs.

- **Superseded jobs**
This option specifies whether the report should include all jobs that have identical criteria.
 - **Catalog backup jobs**
This option specifies whether the report should include information about [catalog](#) backups. 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. This option is intended to help monitor the status of catalog backups independently of other backup jobs.
9. Click **OK**.
- The Configure: Job Summaries page displays a success message, and your job summary appears in the list.

Editing a Job Summary Schedule

You can use the Web tool to change an existing backup schedule, volume duplication scan, or vaulting scan schedule. You must have the `modify administrative domain's configuration` right to edit a job summary schedule.

To edit a job summary schedule:

1. Perform the steps in "[Displaying the Defined Job Summaries Page](#)".
The Configure: Job Summaries page appears.
2. Select the job summary you want to edit and click **Edit**.
The Configure: Job Summaries > `summary_name` page appears, with fields and options set to their current values.
3. Make whatever changes you want and click **OK**.
The Configure: Job Summaries page displays a success message. If you edited the start time or coverage period, then the changed values appear in the table.

Removing a Job Summary Schedule

You can use the Web tool to remove a backup schedule. You must have the `modify administrative domain's configuration` right to remove a job summary schedule.

To remove a job summary schedule:

1. Perform the steps in "[Displaying the Defined Job Summaries Page](#)".
The Configure: Job Summaries page appears.
2. Select the job summary you want to remove and click **Remove**.
A confirmation page appears.
3. Click **Yes**.
The Configure: Job Summaries page displays a success message, and your job summary is gone from the table.

Renaming a Job Summary Schedule

You must have the `modify administrative domain's configuration` right to rename a job summary schedule.

To rename a job summary schedule:

1. Perform the steps in "[Displaying the Defined Job Summaries Page](#)".

The Configure: Job Summaries page appears.

2. Select the job summary you want to rename and click **Rename**.

3. Enter a name for the summary in the **Rename summary_name to** field and click **Yes**.

The Configure: Job Summaries page displays a success message, and your job summary appears with its changed name in the table.

Part II

Performing Backup and Restore Operations

This part describes backup and recovery operations for databases and file-system data using Oracle Secure Backup.

This part contains these chapters:

- [Using Recovery Manager with Oracle Secure Backup](#)
- [Backing Up File-System Data](#)
- [Restoring File-System Data](#)

4

Using Recovery Manager with Oracle Secure Backup

This chapter explains how to use [Recovery Manager \(RMAN\)](#) with Oracle Secure Backup. It assumes that you are familiar with RMAN concepts and operations.

This chapter contains these sections:

- [About Recovery Manager and Oracle Secure Backup](#)
- [Configuring Oracle Secure Backup for Use with RMAN](#)
- [Performing Backups with RMAN and Oracle Secure Backup](#)
- [Performing Recovery with RMAN and Oracle Secure Backup](#)
- [RMAN Backup Metadata in Oracle Secure Backup](#)
- [Using RMAN and Oracle Secure Backup in an Oracle RAC Environment](#)



See Also:

Oracle Database Backup and Recovery User's Guide for more information about RMAN

About Recovery Manager and Oracle Secure Backup

Oracle Secure Backup serves as a media management layer for RMAN through the [SBT interface](#). Oracle Secure Backup and third-party backup utilities integrate with RMAN through the SBT interface.



Note:

Information about the Oracle Database and Oracle Enterprise Manager releases with which you can use Oracle Secure Backup is available at the following URL:

<http://www.oracle.com/technetwork/database/database-technologies/secure-backup/learnmore/index.html>

While Oracle Secure Backup supports previous database versions, key functionality has been added beginning with Oracle Database 10g release 2 (10.2). The following integration enhancements are exclusive to Oracle Secure Backup and are not available with other media management products:

- Oracle Database 10g release 2 (10.2)

- Oracle Enterprise Manager provides a unified interface for RMAN and Oracle Secure Backup. In addition, managing tape devices, disk pools, and media servers using Oracle Enterprise Manager is exclusive to Oracle Secure Backup.
- The Oracle Secure Backup SBT library is the only interface that supports RMAN encrypted backups directly to tape. If you attempt an encrypted RMAN backup using another SBT library, then you encounter the following error message:

```
ORA-19916: encrypted backups to tertiary storage require Oracle Secure Backup
```

- Unused block compression directly to tape is available only with Oracle Secure Backup.

If you are backing up to disk or directly to tape using Oracle Secure Backup, then this enables the unused-block optimization. If the backup is directly to tape using a third-party media management product, then this does not have any effect because unused-block optimization directly to tape is available only with Oracle Secure Backup.

- Oracle Database 11g
 - Optimized SBT buffer allocation uses a shared buffer for SBT and tape. This eliminates the copy process from SBT to the tape buffer, which reduces CPU overhead.
 - Enhanced backup of undo tablespace eliminates backup of committed undo, reducing tape consumption and improving performance.

This section contains these topics:

- [RMAN Environment](#)
- [Database Backups](#)
- [Database Restore and Recovery](#)
- [Interfaces for Managing Database Backup and Recovery](#)
- [RMAN and the Oracle Secure Backup Administrative Domain](#)
- [How RMAN Accesses Oracle Secure Backup](#)

RMAN Environment

RMAN is a utility that enables you to back up Oracle Database files. The RMAN environment includes the following basic components:

- RMAN client

The [RMAN client](#) program, which is installed automatically with Oracle Database software, initiates database backup and recovery. The RMAN client can back up and recover any Oracle Database files accessible locally or through Oracle Net so long as it meets compatibility requirements.
- RMAN target database

The [RMAN target database](#) is the database that RMAN backs up or restores. The RMAN metadata used for managing backup and recovery is stored in the control file of the target database and optionally in an [RMAN recovery catalog](#).
- RMAN recovery catalog

The RMAN recovery catalog is an optional database schema that serves as a secondary repository of RMAN metadata. You can create a centralized recovery catalog in a database to store the metadata for multiple target databases.



See Also:

Oracle Database Backup and Recovery User's Guide for more information about RMAN

Database Backups

Oracle Secure Backup supplies an SBT interface that RMAN can use to back up database files to tape. Within the Oracle Secure Backup administrative domain, an SBT backup is initiated through the RMAN command line or Oracle Enterprise Manager, while a [file-system backup](#) is initiated through the Oracle Secure Backup [Web tool](#) or [obtool](#) commands.

Types of Backups

RMAN performs the following types of backups:

Full backups

By default, RMAN performs full backups. A full backup of a data includes every allocated block in the file being backed up.

Incremental Backups

Incremental backups capture block-level changes to a database made after a previous incremental backup. Incremental backups are generally smaller and faster to make than full database backups. An incremental backup at level 0 is identical in content to a full backup.

Cumulative Incremental Backups

These backups include all blocks changed since the most recent level 0 backup.

Differential Incremental Backups

These backups include only blocks changed since the most recent incremental backup. Incremental backups are differential by default.



See Also:

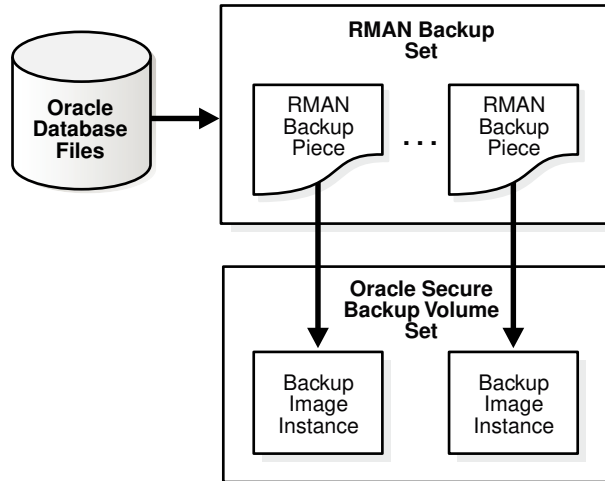
Oracle Database Backup and Recovery User's Guide for more detailed backup concepts

RMAN Backup Sets and Oracle Secure Backup Images

The backup of Oracle Database files performed with RMAN results in a backup set. A backup set is a logical grouping of physical files, each known as a [backup piece](#). For more information about RMAN backup sets and backup pieces, see *Oracle Database Backup and Recovery User's Guide*.

When you use Oracle Secure Backup to store database backups on tape, each backup piece is treated as one Oracle Secure Backup backup image instance. [Figure 4-1](#) illustrates the relationship between pieces and instances. A single backup image instance can span multiple tapes. Oracle Secure Backup can write database backup images (RMAN backup pieces) and file-system backup image instances on the same [volume](#).

Figure 4-1 Backup Sets and Backup Images




 **See Also:**
"About Volume Sets"

About RMAN Storage Parameters

Defining storage parameters for RMAN backups within Oracle Secure Backup can be accomplished by:

- Defining parameters in an RMAN script specific to Oracle Secure Backup
- Defining Oracle Secure Backup database backup storage selectors

It is recommended that you define one or more database backup storage selectors to automate the tape or disk pool storage selection. Use RMAN storage parameter settings only to override the database backup storage selectors in non-recurring backups that require different media selection than included in the backup storage selector.

 **See Also:**
"Database Backup Storage Selectors" for more information about storage selectors

Database Backup Storage Selectors

Oracle Secure Backup uses information encapsulated in a [database backup storage selector](#) to interact with RMAN when performing a backup operation. Oracle Secure Backup uses storage selectors to represent backup attributes that identify Oracle Database files.

A database backup storage selector must specify the following

- The database name or [DBID](#) that uniquely identifies the database
- The name of the database host

- The name of the [media family](#) to use for the RMAN backups
- The content or type of the backup, for example, whether it is a [full backup](#) or an [incremental backup](#) (optional)
- The copy number of duplexed backups (optional)
- Restrictions on which [tape device](#) the backup can use (optional)

When backing up Oracle Database files, RMAN passes the database name, content type, and copy number to Oracle Secure Backup. Using this information, Oracle Secure Backup determines the corresponding database backup storage selector. This storage selector specifies for Oracle Secure Backup what tape devices or disk pools, if any, to restrict this backup to and which media family (if any) to use.

You can create multiple database backup storage selectors. For example, you can create one database storage selector for data file backups of all databases in the administrative domain, and another selector for archived log backups of all databases in the administrative domain. You can specify one [tape library](#) destination for the data file backups and a different tape library destination for the archived log backups.

When an RMAN backup job is initiated through its SBT interface, Oracle Secure Backup examines the database backup storage selectors to determine whether a backup storage selector matches the attributes of the backup job. A match occurs when every attribute of a backup storage selector matches the corresponding attribute of the backup job. If multiple storage selectors match the job, then Oracle Secure Backup chooses the selector whose attributes are most specific. For example, a backup storage selector with the database name set to `db_1` matches before a backup storage selector with the database name set to `all (*)`.

Oracle Secure Backup maintains storage selectors in the `admin/sse1` subdirectory of the [Oracle Secure Backup home](#) on the administrative server.

 **Note:**

Database storage selectors must be unique. With the exception of a wildcard (*), a more general setting matches a more specific setting. For example, if you create a storage selector with `--dbname set to db_1` and `db_2`, then you cannot create another selector that has `--dbname set to db_1` only and has all other attributes identical to those in the first selector. If you create a storage selector that has `--dbname set to set to all (*)`, however, then you can create another selector that has `--dbname set to db_1` and has all other attributes identical to those used for the first selector.

 **See Also:**

- ["Creating a Database Backup Storage Selector in Enterprise Manager"](#)
- ["Setting Media Management Parameters in RMAN"](#) explains how media management parameters specified on RMAN channels can override settings in a backup storage selector.
- *Oracle Secure Backup Reference* to learn about database backup storage selector commands

Duplexing Backups

You might want to duplex backup operations, each on a separate volume set, keeping one set on-site for convenient access, and storing a second set off-site for disaster recovery. For ease of management, each duplexed backup operation can be defined by its own database storage selectors and written to its own separate Oracle Secure Backup media family.

See Also:

- ["Configuring Media Families"](#)
- ["Database Backup Storage Selectors"](#)

Database backup storage selectors are user-defined Oracle Secure Backup media policies for Oracle Database backups. They define which media family, tape device, and resource wait time should be applied by content and copy number of the backup. One database storage selector can apply to all database backups within the administrative domain or multiple storage selectors can be defined for each database.

In the following example, two database storage selectors named `ssel_1` and `ssel_2` are created. They both back up all content of all databases on `host_name`. But `ssel_1` uses media family `mf_1`, while `ssel_2` uses media family `mf_2`:

```
ob> mkssel --dbid * --host host_name --content * --family mf_1 -- copynum 1 ssel_1
ob> mkssel --dbid * --host host_name --content * --family mf_2 -- copynum 2 ssel_2
```

See Also:

Oracle Secure Backup Reference for complete `mkssel` syntax and semantics

If you use RMAN duplexed backups and `PARALLELISM`, then the number of available tape drives must accommodate both copies simultaneously. If channel configuration is set to `PARALLELISM` of 2 for the duplexed backups in the preceding example, then four tape drives are needed for backup operations (two backup copies multiplied by `PARALLELISM` of 2).

Note:

If a tape drive is not available for one copy, then the other copy cannot proceed. In addition, if a backup stream fails for one copy, then it fails for the other copy as well.

Restore operations require only two tape drives in this situation, because restore operations are not duplexed.

RMAN and Oracle Secure Backup Encryption

Oracle Database backup encryption can be performed in one of two ways using Oracle Secure Backup:

- Use RMAN backup encryption, which encrypts data within the database.
This option is available with Oracle Database 10g release 2 (10.2) forward. Please refer to Oracle Database licensing documentation for any restrictions.
- Use Oracle Secure Backup encryption, which encrypts data after RMAN has passed the data through the SBT to Oracle Secure Backup.
This option is available with Oracle9i forward. While encryption occurs outside the database, the data is encrypted on the server before transport over the network or written to a locally attached tape device.

 **Note:**

Oracle Secure Backup encryption is available for both RMAN and file-system backup operations.

 **See Also:**

[Managing Backup Encryption](#) for more information about Oracle Secure Backup encryption and an example on encrypting a database backup

RMAN Backup and Restore Policies

To control the length of queue time before the onset of a backup job, modify the following policy settings:

- Operations policy `rmanresourcewaittime`
This policy is set to `forever` by default. Any configuration in a backup storage selector or RMAN parameter overrides this policy.
- Specifying the `--waittime` option in an `mkssel` or `chssel` command in `obtool`
- RMAN parameter `OB_RESOURCE_WAIT_TIME`

For RMAN restore operations, the start time depends on the setting of the `rmanrestrestartdelay` policy in the operations policy class.

 **See Also:**

- *Oracle Secure Backup Reference* for more information about the `mkssel` and `chssel` commands
- "[Setting Media Management Parameters in RMAN](#)"
- *Oracle Secure Backup Reference* for information on defaults and policies

Database Restore and Recovery

A restore operation that you initiate through RMAN is called an Oracle Database restore operation. RMAN first performs a full backup to restore data files, and only then moves on to performing incremental backups. The RMAN restore operation retrieves data files from backups for a recovery operation in case of loss or damage of these files.

See Also:

- ["Database Backup Storage Selectors"](#)
- ["Performing Recovery with RMAN and Oracle Secure Backup"](#)

Interfaces for Managing Database Backup and Recovery

When performing RMAN backup and restore operations with the Oracle Secure Backup SBT interface, you can use the following interfaces:

- [RMAN Command-Line Client](#)
- [Oracle Enterprise Manager Cloud Control](#)

RMAN Command-Line Client

The `rman` executable is located in the `ORACLE_HOME/bin` directory of a database installation. The RMAN client can run from any Oracle home, regardless of whether the computer containing this home is a member of the Oracle Secure Backup administrative domain. The target database host must be a member of the Oracle Secure Backup administrative domain. The target database uses the Oracle Secure Backup SBT on the target host to communicate with the Oracle Secure Backup administrative domain.

Oracle Enterprise Manager Cloud Control

You can manage multiple databases with Oracle Enterprise Manager Cloud Control, which is the graphical user interface for database administration. The Cloud Control console can run on any database host in the administrative domain.

You can manage SBT backups of all databases in the Oracle Secure Backup administrative domain through Cloud Control. You can create a centralized RMAN recovery catalog in the same database that contains the Cloud Control repository.

When you use Cloud Control, you can use Oracle Secure Backup on a host that runs an Oracle Database 10g release 1 (10.1) or earlier database if the repository for Enterprise Manager is in an Oracle Database 10g release 2 (10.2) database.

RMAN and the Oracle Secure Backup Administrative Domain

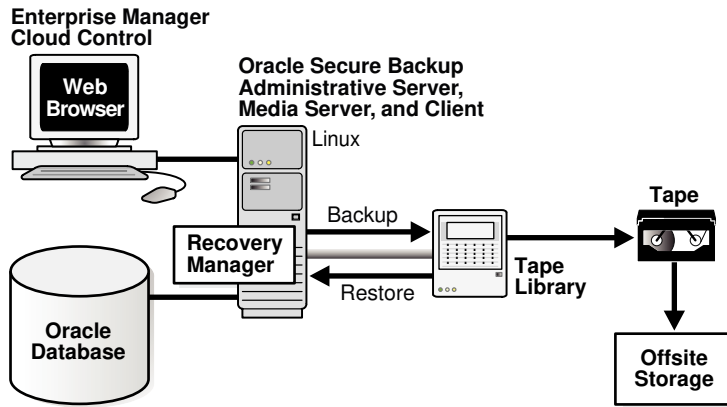
This section describes RMAN operations in the following situations:

- [Single-Host Administrative Domain](#)
- [Multiple-Host Administrative Domain with Database Backups](#)

Single-Host Administrative Domain

In a single-host administrative domain, one host plays the role of administrative server, [media server](#), and [client](#). An Oracle database is installed on this host. [Figure 4-2](#) illustrates a typical single-host scenario.

Figure 4-2 Single-Host Administrative Domain with Database Backups



 **Note:**

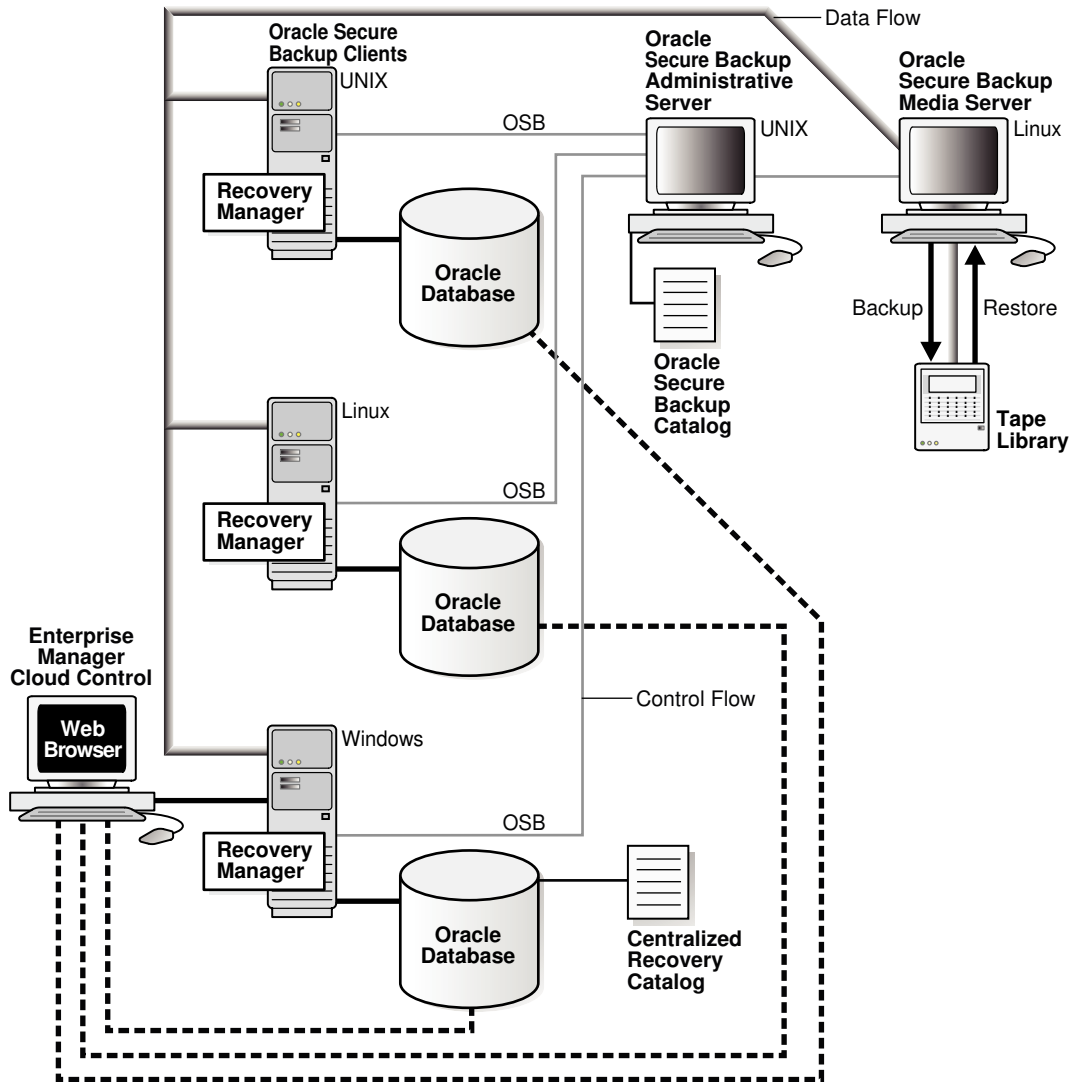
This chapter is written from the perspective of the administrator of a single-host administrative domain that is configured like the one in [Figure 4-2](#).

Multiple-Host Administrative Domain with Database Backups

In a multiple-host administrative domain, the administrative server, media server, and client hosts might all be separate, or each database server might also be a media server. The latter arrangement has the advantage of minimizing network-based backup operations. A single administrative domain can include only one administrative server but can include multiple media servers and clients.

[Figure 4-3](#) illustrates a typical multiple-host domain in which each client host runs an Oracle database. In this example, the administrative server and media server do not run databases. The Windows database includes a centralized recovery catalog to store metadata for backups of all databases in the administrative domain.

Figure 4-3 Multiple-Host Administrative Domain

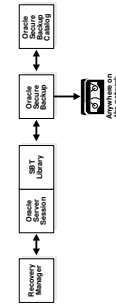


You can use Cloud Control on a client to initiate SBT operations involving all databases in the administrative domain.

How RMAN Accesses Oracle Secure Backup

Regardless of the administrative domain configuration and the front-end interface that you use to manage backup and recovery, the process by which RMAN communicates with the Oracle Secure Backup SBT library is the same. Figure 4-4 displays the basic components of RMAN backup and restore operations that use the Oracle Secure Backup SBT.

Figure 4-4 RMAN and the Oracle Secure Backup SBT Interface



The basic process for RMAN backup and restore operations with Oracle Secure Backup is as follows:

1. An [Oracle Secure Backup user](#) starts the RMAN client, either through the command line or the Oracle Enterprise Manager console.
2. The Oracle Secure Backup user allocates an SBT channel and runs an RMAN `BACKUP` or `RESTORE` command.

When the channel is allocated, a server session starts on the Oracle database.

3. The server session on the database host makes the backup or restore job request through the Oracle Secure Backup SBT library.
4. Oracle Secure Backup creates the backup or restore job and assigns it a unique identifier such as `sbt/15`.

 **See Also:**

Oracle Secure Backup Reference for a description of job identifiers

5. For an RMAN backup operation, Oracle Secure Backup immediately tries to reserve and start the appropriate resources. If the resources are unavailable, then Oracle Secure Backup queues the job while it waits for the resources to become available.

 **See Also:**

"[RMAN Backup and Restore Policies](#)" for information on settings related to RMAN backup and restore operations

6. RMAN creates or restores the backup pieces.
7. For backups, Oracle Secure Backup stores metadata about RMAN backup pieces in the Oracle Secure Backup catalog.

The Oracle Secure Backup catalog is stored and managed completely separately from the RMAN recovery catalog. Oracle Secure Backup stores each backup piece and corresponding metadata about the piece.

Oracle Secure Backup Support for Non-Uniform Memory Access (NUMA)

Starting with Oracle Secure Backup 10.4.0.1, Oracle Secure Backup supports NUMA architecture. In a NUMA system, the processors are grouped into smaller systems called nodes or regions. Each node has its own processors and a common memory. All processors within a node share the common memory. Access to this local memory area is faster thus resulting in improved scalability and performance.

During a database backup or restore operation, the Oracle shadow process manages the interaction between Oracle Secure Backup and the Oracle Database. The shadow process loads the SBT library and starts the Oracle Secure Backup data service (`obndmpd` process), which performs the network I/O required for the operation, on the client. The Oracle shadow process and the Oracle Secure Backup data service use a common memory area to exchange data.

On NUMA machines, Oracle Secure Backup ensures that the Oracle shadow process and the Oracle Secure Backup data service run on the same node and therefore access the same common memory. This results in improved performance when the Oracle shadow process and the Oracle Secure Backup data service are not on the same node.

Configuring Oracle Secure Backup for Use with RMAN

To configure Oracle Secure Backup for use with RMAN, perform the following steps in Oracle Secure Backup:

1. Configure RMAN access to the Oracle Secure Backup SBT.

 **See Also:**

["Configuring RMAN Access to the Oracle Secure Backup SBT Library"](#)

2. Create an Oracle Secure Backup user preauthorized for RMAN operations.

 **Note:**

This is a required step. An RMAN backup operation fails without it.

 **See Also:**

["Creating a Preauthorized Oracle Secure Backup User"](#)

3. It is recommended that you create media families for data files and archived redo logs. If you do not create your own media families, then by default RMAN uses the `RMAN-DEFAULT` media family.

 **See Also:**

["Creating Media Families for RMAN Backups"](#)

4. Optionally, configure database backup storage selectors or RMAN media management parameters. These settings give you more fine-grained control over storage selection for backups.

 **See Also:**

- ["Creating a Database Backup Storage Selector in Enterprise Manager"](#)
- ["Setting Media Management Parameters in RMAN"](#)

5. Optionally, disable NUMA-awareness by setting the `OB_IGNORE_NUMA` to 0.

The default value of this parameter is 1, thus making Oracle Secure Backup NUMA-aware. This ensures that, for a database backup or restore operation, the Oracle shadow process and the Oracle Secure Backup data service are located in the same NUMA region or node.

 **See Also:**

["Interfaces for Managing Database Backup and Recovery"](#)

Configuring RMAN Access to the Oracle Secure Backup SBT Library

You can use Enterprise Manager Cloud Control to configure RMAN access to Oracle Secure Backup. You need only specify the Oracle Secure Backup home directory. RMAN locates the SBT library automatically.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for information on registering an administrative server in Enterprise Manager

By default, RMAN looks in a platform-specific default location for the SBT library. On Linux and UNIX the default library filename is `/lib/libobk.so`, with the extension name varying according to platform: `.so`, `.sl`, `.a`, and so on. On Windows the default library location is `%WINDIR%\System32\orasbt.dll`.

When you install Oracle Secure Backup on Linux and UNIX, the installer automatically copies the SBT library to the `lib` subdirectory of the Oracle Secure Backup home and creates a symbolic link to the library in the `/lib` or `/usr/lib` directory.

By default, RMAN searches the standard path and loads the Oracle Secure Backup SBT library when an SBT channel is allocated.

 **Note:**

You can override the default SBT library location by specifying the library path in the `SBT_LIBRARY` media management parameter when allocating or configuring RMAN channels.

Creating a Preauthorized Oracle Secure Backup User

Oracle Secure Backup honors SBT requests only if the Oracle Secure Backup user making the request has been preauthorized for RMAN backup on that host. This preauthorized Oracle Secure Backup user must meet two sets of requirements:

- The preauthorized Oracle Secure Backup user must be mapped to operating system privileges to access the files to be backed up or restored. The preauthorized Oracle Secure Backup user can perform RMAN operations only on the host where it has access to files.
- The preauthorized Oracle Secure Backup user must also be assigned to an Oracle Secure Backup [class](#) possessing the following [rights](#):
 - `access Oracle backups (set to owner, class, or all)`
 - `perform Oracle backups and restores`

 **See Also:**

Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

Only one Oracle Secure Backup user can be preauthorized for RMAN backup and restore operations on a particular host. A database can have multiple RMAN users that can start backup or restore operations, but Oracle Secure Backup has only one preauthorized Oracle Secure Backup user for that database server.

You can also preauthorize an Oracle Secure Backup user for command-line (`obtool`) operations. This is useful if you use backup and restore scripts.

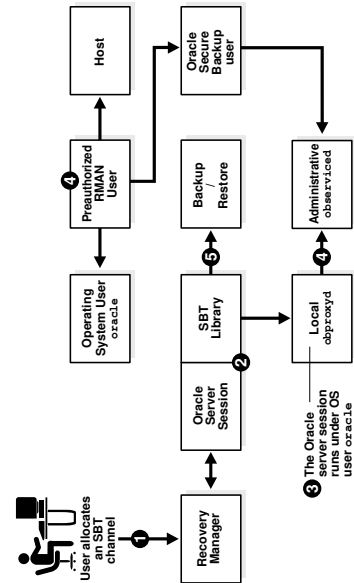
 **See Also:**

["Assigning Preauthorized Access"](#)

How Oracle Secure Backup Preauthorizes SBT Backups

The following figure illustrates the basic process by which an Oracle Secure Backup user preauthorized for RMAN operations on a particular host submits a backup or restore request to Oracle Secure Backup.

Figure 4-5 Preauthorization for Database Backup and Restore Operations



The process works as follows:

1. When you start RMAN and allocate an SBT channel, Oracle Database starts a server session.
2. The server session uses the SBT library to communicate with the `obproxyd` daemon running locally on its host.
3. The local `obproxyd` daemon determines which operating system user the server session runs under. Assume in this example that the operating system user is named `oracle` and runs on Linux host `brhost2`.
4. The local `obproxyd` daemon checks the operating system user information with the administrative server `observiced` daemon. If the operating system user on this host and operating system is preauthenticated as an Oracle Secure Backup user, then the login to Oracle Secure Backup is successful.

For example, assume that the `oracle` operating system user on host `brhost2` is preauthorized to run as Oracle Secure Backup user `obuser`. Assume also that `obuser` is a member of the `oracle` class, which is assigned the `perform Oracle backups and restores` right by default.

 **See Also:**

Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

5. The server session uses the Oracle Secure Backup user to back up or restore files.
The Oracle Secure Backup operations submitted through the SBT use the operating system user defined by the Oracle Secure Backup user to access the host. In this figure, the backup and restore operations run under the `oracle` operating system account on `brhost2`.

Configuring an RMAN Preauthorization

You can configure a preauthorized Oracle Secure Backup user with required rights to perform backups of Oracle Database files to tape with Oracle Secure Backup during installation of the Oracle Secure Backup software or after installation using either the Oracle Secure Backup Web tool or the `mkuser` command in `obtool`.

To create a preauthorized Oracle Secure Backup user during an Oracle Secure Backup installation on Linux or UNIX, you must set the `obparameters` parameter `create_preauthorized_oracle_user`.

See Also:

Oracle Secure Backup Installation and Configuration Guide for information on configuring `obparameters` for creating a preauthorized `oracle` user

To create a preauthorized Oracle Secure Backup user during an Oracle Secure Backup installation on Windows, you must enable the action for **Create "oracle" user** when selecting features for the administrative server.

See Also:

Oracle Secure Backup Installation and Configuration Guide for information on administrative server features

To configure a preauthorized Oracle Secure Backup user after installation, use the Web tool or the `mkuser` command in `obtool`. [Example 4-1](#) uses `mkuser` to create an Oracle Secure Backup user named `preauth_user` and assign this user to the `oracle` class. The example uses `--preauth` to map `preauth_user` to the Linux or UNIX user `oracle` on host `brhost2`. The mapping to an operating system user with access to the files to be backed up or restored is required.

See Also:

Oracle Secure Backup Reference to learn about the `mkuser` command

Example 4-1 Preauthorizing an Operating System User to Make RMAN Backups

```
mkuser preauth_user --class oracle --preauth brhost2:oracle+rman
```

Creating Media Families for RMAN Backups

It is recommended that you create dedicated media families for use in RMAN operations. If you do not create dedicated RMAN media families, then Oracle Secure Backup uses a default media family.

The default media family for use by RMAN is named `RMAN-DEFAULT`. You cannot delete or rename the `RMAN-DEFAULT` media family, although you can modify some of its attributes through the Oracle Secure Backup Web tool or `obtool`.

 **See Also:**

- ["Content-Managed Expiration Policies"](#)
- ["Editing or Displaying Media Family Attributes"](#)

It is useful to create different media families for archived redo log and data file backup sets. You can create media families with Enterprise Manager, the Oracle Secure Backup Web tool, or the `mkmf` command in `obtool`.

 **See Also:**

- ["Adding a Media Family"](#) for information on adding a media family
- *Oracle Secure Backup Reference* for complete syntax and semantics for the `obtool mkmf` command

When you create a media family, you specify a volume [expiration policy](#) that determines when a volume in that media family is eligible to be overwritten and recycled. Volumes in a media family use either a [content-managed expiration policy](#) or [time-managed expiration policy](#).

Content-managed volumes can only be used for RMAN operations. You can use time-managed volumes for both RMAN and file-system backup and restore operations. It is possible, therefore, that time-managed volumes could contain a mixture of file-system backups 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 a backup piece that was on that volume as available. In this case, you must use the `CROSSCHECK` command in RMAN to resolve the discrepancy.

Creating a Database Backup Storage Selector in Enterprise Manager

You can use Oracle Enterprise Manager Cloud Control to create a database backup storage selector. Cloud Control gives the selector a system-defined name. To specify the name for the storage selector, use the `mkssel` command in `obtool`.

Setting Media Management Parameters in RMAN

If you use Oracle Secure Backup database storage selectors, then you are not required to set media management parameters in RMAN. In some circumstances, however, you might want to override the database storage selectors by setting RMAN parameters.

See Also:

Oracle Secure Backup Reference to learn about the RMAN media management parameters and their relationship with database backup storage selectors

To set media management parameters in an RMAN database backup:

1. Follow Step 1 through Step 9 in "[Performing Backups with RMAN and Oracle Secure Backup](#)".

2. Click **Edit RMAN Script**.

The Schedule Customized Backup: Review: Edit RMAN Script page appears.

3. In the main window, modify the script to use media management parameters. For example, assume the backup script is as follows:

```
backup device type sbt database include current controlfile;  
backup device type sbt archivelog all not backed up;
```

To configure the backup to use the `my_mf` media family, you could modify the script as follows:

```
run  
{  
  allocate channel c1 device type sbt  
    parms 'ENV=(OB_MEDIA_FAMILY=my_mf)';  
  backup database include current controlfile;  
  backup archivelog all not backed up;  
}
```

4. Click **Submit Job**.

The Status page appears.

Performing Backups with RMAN and Oracle Secure Backup

After you have configured RMAN to use the Oracle Secure Backup SBT, the procedure for making RMAN backups is identical to the procedure described in *Oracle Database Backup and Recovery User's Guide*.

To backup a database file using RMAN and Oracle Secure Backup:

1. Start RMAN and connect to the target database by using the `CONNECT TARGET` command. The following example starts RMAN and connects to the target database as the user `sbu`, created with the `SYSBACKUP` privilege. You are prompted to enter your password.

```
rman%  
  
RMAN> CONNECT TARGET sbu AS SYSBACKUP
```

2. Use the `BACKUP` command to perform the required backup.

The parameters required for the Oracle Secure Backup Media Manager are set while configuring an SBT channel.

```
RMAN> run {
@ 2> allocate channel ch1 device type sbt PARS 'ENV=(OB_DEVICE=drv1)';
@ 3> allocate channel ch2 device type sbt PARS 'ENV=(OB_DEVICE=drv2)';
@ 4> backup datafile 1,3;
@ 5> }
@ .
@ using target database control file instead of recovery catalog
@ allocated channel: ch1
@ channel ch1: SID=156 device type=SBT_TAPE
@ channel ch1: Oracle Secure Backup
@ .
@ allocated channel: ch2
@ channel ch2: SID=189 device type=SBT_TAPE
@ channel ch2: Oracle Secure Backup
@ .
@ Starting backup at 17-MAR-15
@ channel ch1: starting full datafile backup set
@ channel ch1: specifying datafile(s) in backup set
@ input datafile file number=00001
@ name=/scratch/abc/app/abc/oradata1/orcl/system01.dbf
@ channel ch1: starting piece 1 at 17-MAR-15
@ channel ch2: starting full datafile backup set
@ channel ch2: specifying datafile(s) in backup set
@ input datafile file number=00003
@ name=/scratch/abc/app/abc/oradata1/orcl/undotbs01.dbf
@ channel ch2: starting piece 1 at 17-MAR-15
@ .
@ .
```

Performing Recovery with RMAN and Oracle Secure Backup

After you have configured RMAN to use the Oracle Secure Backup SBT, the procedure for restoring database files is identical to the procedure described in *Oracle Database Backup and Recovery User's Guide*.



See Also:

["Configuring RMAN Access to the Oracle Secure Backup SBT Library"](#)

To restore database files using RMAN and Oracle Secure Backup:

1. Start RMAN and connect to the target database by using the `CONNECT TARGET` command. The following example starts RMAN and connects to the target database as the user `sbu`, created with the `SYSBACKUP` privilege. You are prompted to enter your password.

```
rman%
RMAN> CONNECT TARGET sbu AS SYSBACKUP
```

2. Run the `RESTORE DATAFILE` command to restore the datafile backed up in the section ["Performing Backups with RMAN and Oracle Secure Backup"](#).

```
RMAN> RESTORE DATAFILE 3;
Starting restore at 20-SEP-13
```

```
allocated channel: ORA_SBT_TAPE_1
channel ORA_SBT_TAPE_1: SID=11 device type=SBT_TAPE
channel ORA_SBT_TAPE_1: Oracle Secure Backup
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=97 device type=DISK
channel ORA_SBT_TAPE_1: starting datafile backup set restore
channel ORA_SBT_TAPE_1: specifying datafile(s) to restore from backup set
channel ORA_SBT_TAPE_1: restoring datafile 00003 to /ade/osb_test/oracle/dbs/
t_undol.f
channel ORA_SBT_TAPE_1: reading from backup piece 06ok9trl_1_1
channel ORA_SBT_TAPE_1: piece handle=06ok9trl_1_1 tag=TAG20130920T040300
channel ORA_SBT_TAPE_1: restored backup piece 1
channel ORA_SBT_TAPE_1: restore complete, elapsed time: 00:00:25
Finished restore at 20-SEP-13
```

3. Run the RECOVER DATAFILE to complete the recovery operation.

```
RMAN> RECOVER DATAFILE 3;
Starting recover at 20-SEP-13
using channel ORA_SBT_TAPE_1
using channel ORA_DISK_1
starting media recovery
media recovery complete, elapsed time: 00:00:00
Redo Buffers 4984832 bytes
Finished recover at 20-SEP-13
```

RMAN Backup Metadata in Oracle Secure Backup

Oracle Secure Backup maintains backup metadata for all RMAN and file-system backup operations. This section explains how to access RMAN metadata within the Oracle Secure Backup catalog.

This section contains these topics:

- [About RMAN and Oracle Secure Backup Metadata](#)
- [Displaying RMAN Job Information in Oracle Secure Backup](#)
- [Displaying Backup Piece Information](#)

About RMAN and Oracle Secure Backup Metadata

Oracle Secure Backup maintains a [catalog](#) of metadata for Oracle Secure Backup jobs on the administrative server. You can use the Web tool to display catalog metadata about each backup piece, referred to as a backup image in the Oracle Secure Backup Web tool. You can also use the `lsjob`, `catxcr`, and `lspiece` commands in `obtool`.

 **See Also:**

Oracle Database Backup and Recovery User's Guide for more information about accessing RMAN metadata

Expiration of RMAN Backups on Tape

You can make RMAN backups on a volume that use a content-managed or time-managed expiration policy. If the RMAN backup is on a content-managed volume, then you should use the `DELETE OBSOLETE` command in RMAN to mark backup pieces as deleted in the RMAN repository. In response, Oracle Secure Backup updates its catalog to indicate that the backup pieces are deleted, so both the RMAN repository and Oracle Secure Backup catalog show the pieces as deleted.

 **Note:**

If you use content-managed volumes for RMAN backups, then the RMAN retention configuration determines when the tape expires. If you use a control file for the RMAN repository, then the record keep time must be at least equal to the period you want backups retained.

Oracle does not recommend using the `rmpiece` command in Oracle Secure Backup to delete backup pieces from tape, because the RMAN metadata then fails to reflect the tape contents. This discrepancy can also occur when RMAN backup pieces exist on volumes that are expired by a time-managed expiration policy, or when you forcibly **overwrite** a volume containing RMAN backup pieces. Use the `CROSSCHECK` command in RMAN to resolve discrepancies between the Oracle Secure Backup catalog and the RMAN repository.

 **See Also:**

Oracle Database Backup and Recovery User's Guide to learn about crosschecking backups and deleting RMAN backups

Displaying RMAN Job Information in Oracle Secure Backup

RMAN backups made with the Oracle Secure Backup SBT are subject to all Oracle Secure Backup job management commands.

 **See Also:**

[Managing Backup and Restore Jobs](#)

When you use RMAN to backup or restore a database, the job contains the name of the database. [Example 4-2](#) shows sample output for backup and restore jobs relating to a

database named `orcl`. The Job IDs in this example include `oracle` because the jobs were run by the `oracle` user.

Example 4-2 Database Backup and Restore Jobs

```
ob> lsjob --all
Job ID          Sched time  Contents                                     State
-----
oracle/1        none       database orcl (dbid=1091504057)             completed successfully at 2013/11/21.15:24
oracle/1.1      none       datafile backup                             completed successfully at 2013/11/21.15:28
oracle/2        none       database orcl (dbid=1091504057)             completed successfully at 2013/11/21.15:53
oracle/2.1      none       datafile backup                             completed successfully at 2013/11/21.15:54
oracle/3        none       database orcl (dbid=1091504057)             completed successfully at 2013/11/21.15:57
oracle/3.1      none       restore piece '06grqejs_1_1'               completed successfully at 2013/11/21.15:59
```

Displaying Job Transcripts

Job transcripts contain detailed information about Oracle Secure Backup jobs. [Example 4-3](#) shows part of the transcript for an archived log backup. This backup uses the `RMAN-DEFAULT` media family.



See Also:

- *Oracle Secure Backup Reference* for complete syntax and semantics for the `catxcr` command in `obtool`
- "[Displaying Job Transcripts](#)" for instructions on using the Oracle Secure Backup Web tool to display job transcripts

Example 4-3 Transcript of an Archived Log Backup Job

```
ob> catxcr --head 22 sbt/6.1
2008/06/28.13:01:04

2008/06/28.13:01:04
2008/06/28.13:01:04          Transcript for job sbt/6.1 running on brhost1
2008/06/28.13:01:04
Volume label:
  Volume tag:          ADE202
  Volume ID:           RMAN-DEFAULT-000002
  Volume sequence:    1
  Volume set owner:   root
  Volume set created: Tue Jun 28 13:01:30 2008
  Media family:       RMAN-DEFAULT
  Volume set expires: never; content manages reuse

Archive label:
  File number:        1
  File section:       1
  Owner:              root
  Client host:        brhost1
  Backup level:       0
  S/w compression:   no
  Archive created:    Tue Jun 28 13:01:30 2008
```

Displaying SBT Errors

If an error occurs during an SBT session, then Oracle Secure Backup attempts to send the error description to the administrative server to be saved in the job transcript. The database writes SBT errors to the `sbtio.log` trace file, unless the user has configured the file to be named otherwise. Typically, `sbtio.log` is located in the `rdbms/log` subdirectory of the Oracle home.

See Also:

Oracle Database Backup and Recovery User's Guide to learn how to troubleshoot RMAN backup and restore operations

Displaying Backup Piece Information

Oracle Secure Backup maintains information about RMAN backups at the backup piece level. This information can be browsed in the Oracle Secure Backup Web tool under backup image or by using `obtool` commands. While information regarding backup pieces is available with Oracle Secure Backup, backup sets are logical groupings that only RMAN has knowledge of.

An RMAN backup piece is represented in Oracle Secure Backup as a backup image. You can use the `lspiece` command in `obtool` to display information about backup pieces recorded in the Oracle Secure Backup catalog. [Example 4-4](#) shows sample output for `lspiece`.

Note:

Each piece name must be unique across all databases in the Oracle Secure Backup administrative domain. You can make piece names unique either by using the RMAN catalog option, so that the backup catalog for all databases in the domain is centralized, or by using RMAN format string to create unique piece names.

See Also:

- ["RMAN Backup Sets and Oracle Secure Backup Images"](#)
- ["Displaying Backup Sections"](#) for instructions on using the Oracle Secure Backup Web tool to display information about backup pieces
- *Oracle Database Backup and Recovery User's Guide* for detailed information on backup piece names
- *Oracle Secure Backup Reference* for complete syntax and semantics for the `lspiece` command

Example 4-4 Displaying Backup Pieces

```
ob> lspiece --long
Backup piece OID:      104
Database:             ob
Database ID:          1566254457
```

```
Content:                archivelog
Copy number:            0
Created:                2008/06/28.13:01
Host:                  brhost1
Piece name:             05go3tgd_1_1
Backup piece OID:      105
Database:               ob
Database ID:            1566254457
Content:                archivelog
Copy number:            0
Created:                2008/06/28.13:02
Host:                  brhost1
Piece name:             06go3ti5_1_1
```

Using RMAN and Oracle Secure Backup in an Oracle RAC Environment

You can use the Oracle Secure Backup SBT library with RMAN to back up a database in an Oracle Real Application Clusters (Oracle RAC) system.

This section contains these topics:

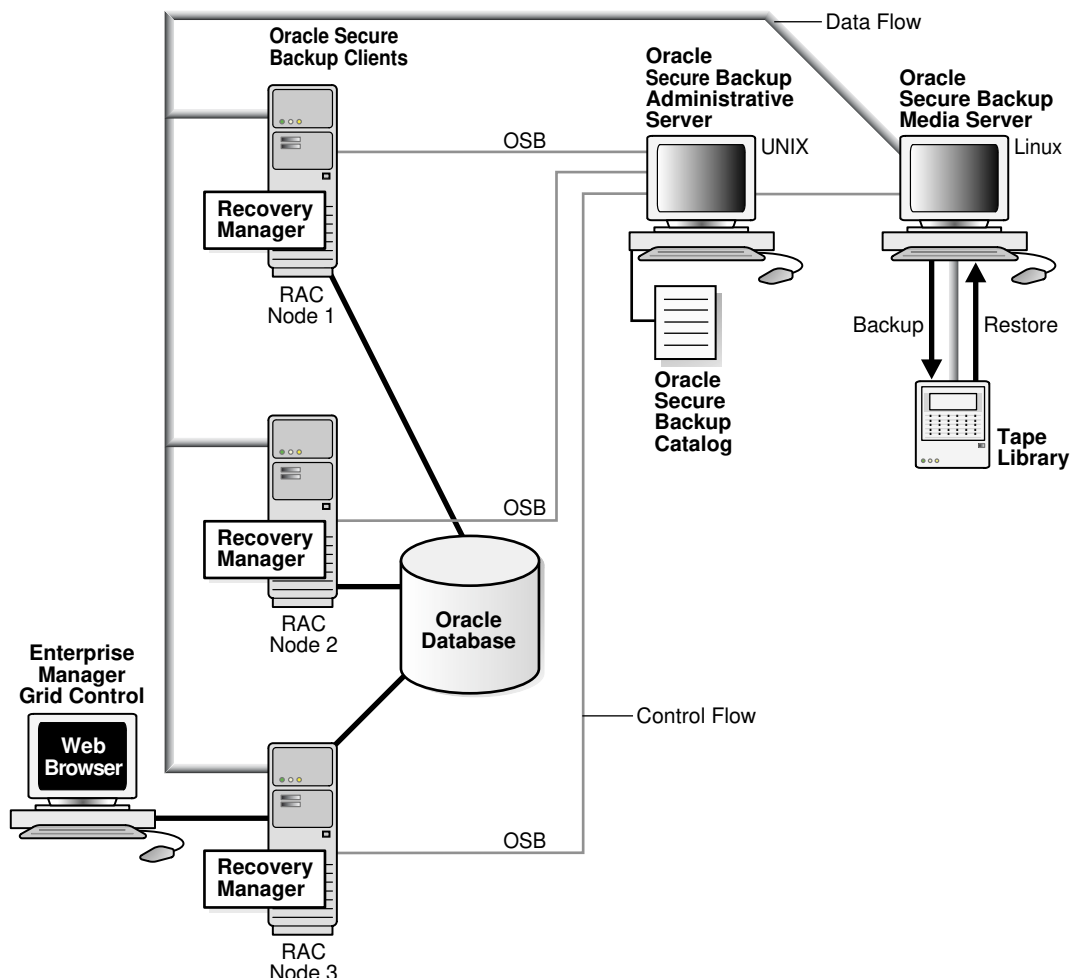
- [Installing Oracle Secure Backup in an Oracle RAC Environment](#)
- [Network Versus Local Backups](#)

Installing Oracle Secure Backup in an Oracle RAC Environment

It is recommended that you install Oracle Secure Backup on each node in the cluster, configuring the node as a client, media server, or both. By including all nodes in the administrative domain, local files on the node can be protected. Oracle Secure Backup handles file-system backup operations for an Oracle RAC client no differently from any other client host.

[Figure 4-6](#) shows a sample administrative domain that includes a three-node Oracle RAC system, with each node configured as an Oracle Secure Backup client. In Oracle RAC environments, RMAN can restore a backup piece to any node within a cluster that has the Oracle Secure Backup software installed, regardless of which node created the backup piece.

Figure 4-6 Using RMAN and Oracle Secure Backup in a Real Application Clusters Environment



Network Versus Local Backups

For performance reasons, it is important to configure the Oracle RAC environment differently for networked or local backups. RMAN backups can be dynamically allocated in the Oracle RAC environment based on the work load distribution. This technique works well if the Oracle RAC database is backed up over the network using Oracle Secure Backup because it does not matter to Oracle Secure Backup which of the nodes performs a client backup.

If a node in the Oracle RAC environment is a media server, then it is more efficient for this node to create backups on a locally accessed tape device. This technique avoids allocating network bandwidth for backups, as would happen if an Oracle RAC node configured as a client were to perform the backup.

You can configure RMAN backups to be performed from specific nodes. It is recommended that RMAN be configured persistently so it must be configured only once and affects all backup and restore operations from that database.

In the following example, there are three tape drives attached to hostA and another three tape drives attached to hostB. The configuration steps are as follows:

1. Connect to any node in the Oracle RAC environment to configure RMAN parameters.

2. Set parallelism.
3. Configure channel (3 channels) /connect / sid hostA.
4. Configure channel (3 channels) /connect / sid hostB.

In the preceding example, you are establishing that six total channels are necessary, three from each host. This configuration applies to every backup and restore operation unless you override this setting. You can start an RMAN operation by connecting to any node within the Oracle RAC environment. The operation is performed only on the two configured hosts.

 **Note:**

If you do not configure persistent settings, then you can accomplish the same goal in RMAN scripts by allocating channels by host.

5

Backing Up File-System Data

This chapter explains how to make backups of file-system data with Oracle Secure Backup. File-system data can be defined as the collection of files and file management structures on physical or logical storage. Oracle Secure Backup can back up all types of files on the file system to a backup container. For example, you can use Oracle Secure Backup to back up the root directory on a host or an Oracle Database home.

Unlike a [Recovery Manager \(RMAN\)](#) database backup made through the [SBT interface](#), a [file-system backup](#) is initiated by Oracle Secure Backup and can include any file on the file system.

You can set up a [backup schedule](#) so that file-system backups occur automatically at user-defined intervals. You can also perform [on-demand backups](#), which are one-time-only backups. You can create scheduled and on-demand file-system backups with either the Oracle Secure Backup [Web tool](#) or [obtool](#) (you cannot create or manage file-system backups with Oracle Enterprise Manager). This chapter provides instructions for using the Oracle Secure Backup Web tool.

This chapter contains these sections:

- [About File-System Backups](#)
- [Preparing to Perform File-System Backups](#)
- [Steps to Perform File-System Backups](#)
- [Performing Scheduled File-System Backups](#)
- [Performing On-Demand File-System Backups](#)
- [Backing Up Critical Data on the Administrative Server](#)

About File-System Backups

This section provides an overview of file-system backups using Oracle Secure Backup.

This section contains these topics:

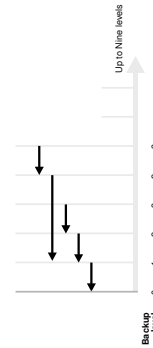
- [File-System Backup Types](#)
- [Backup Datasets](#)
- [Scheduled Backups](#)
- [On-Demand Backups](#)
- [Restartable Backups](#)

File-System Backup Types

A [full backup](#) backs up all specified files, regardless of when they were last backed up. An [incremental backup](#) backs up the subset of specified files that have changed since a previous full or incremental backup.

Oracle Secure Backup supports nine different incremental backup levels. In a [cumulative incremental backup](#), Oracle Secure Backup backs up only those files that have changed since the last backup at a numerically lower [backup level](#). For example, a level 3 cumulative backup copies only that data that has changed since the most recent backup that is level 2 or lower. [Figure 5-1](#) shows a series of cumulative backups.

Figure 5-1 Cumulative Incremental Backups



In a [differential incremental backup](#), Oracle Secure Backup backs up files modified since the most recent incremental backup at the same or lower level (0-9). This option is identical to a level 10 incremental backup. Oracle Secure Backup does not support the level 10 backup with some platforms, including [Network Attached Storage \(NAS\)](#) devices such as a Network Appliance [filer](#).

Oracle Secure Backup includes an [off-site backup](#) option that enables you to perform a [full backup](#) without affecting the full or incremental [backup schedule](#). This technique is useful when you want to create an archive for off-site storage without disturbing your schedule of incremental backups.



See Also:

["Choosing a Backup Schedule"](#)

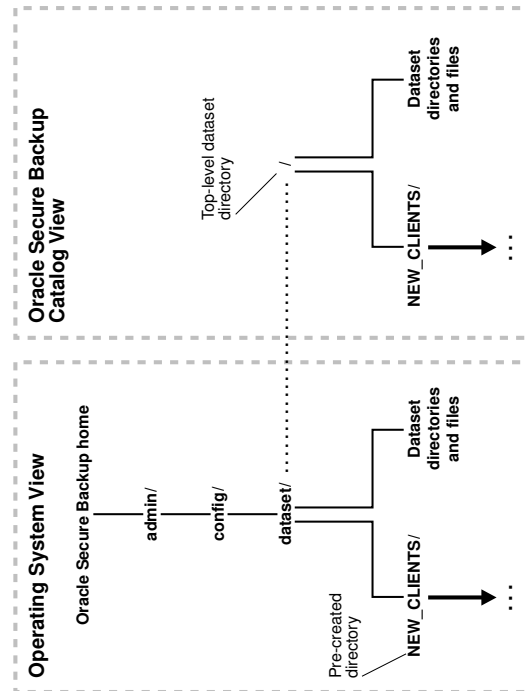
Backup Datasets

A [dataset file](#) defines the file-system data that Oracle Secure Backup includes in or excludes from a backup. Dataset files employ a lightweight language that gives you the flexibility to build and organize the definitions of the data to be backed up. You can find several sample dataset files in the samples subdirectory of the [Oracle Secure Backup home](#). You can use these as templates to design your own dataset files.

The sample dataset file shown in [Example 5-1](#) instructs Oracle Secure Backup to back up everything in directory `/usr1/home` on `brhost2`, except for the directories `/usr1/home/temp` and `/usr1/home/oldfiles`, and the entire contents of directory `/usr2/home`.

Dataset files are hierarchically organized into a directory structure. As shown in [Figure 5-2](#), you can view this structure from the perspective of the operating system or the Oracle Secure Backup [catalog](#).

Figure 5-2 Dataset Directories and Files



Dataset files and directories are stored in the `admin/config/dataset` subdirectory of the Oracle Secure Backup home. As shown on the left part of [Figure 5-2](#), the `NEW_CLIENTS` directory is automatically created in `admin/config/dataset` during installation. You can use this directory to store your dataset files.

You can run `obtool` or Oracle Secure Backup Web tool commands to create and manage dataset files and directories. You can create your own dataset directories and files and organize them into a tree-like structure.

See Also:

- ["Creating Dataset Files"](#)
- *Oracle Secure Backup Reference* for a description of the Oracle Secure Backup dataset language and information on the `obtool` dataset commands

Example 5-1 Sample Dataset File

```
exclude name *.backup
exclude name *~

include host brhost2 {
    include path /usr1/home {
        exclude path /usr1/home/temp
        exclude path /usr1/home/oldfiles
    }
    include path /usr2/home
}
```

Scheduled Backups

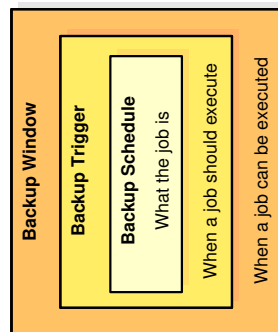
A [scheduled backup](#) is the basis of your backup strategy. Your first task after setting up the [administrative domain](#) should be choosing and configuring a backup schedule that makes sense for your environment.

In a scheduled backup, you instruct Oracle Secure Backup to make backups according to a backup schedule, which specifies each [dataset](#) for the backup. A [trigger](#) defined in the schedule specifies when the job should run. Jobs scheduled from different time zones are synchronized with one another.

For example, you can instruct Oracle Secure Backup to back up the `/home` directory on [client](#) host `brhost2` every Sunday.

As shown in [Figure 5-3](#), the processing of a scheduled [backup job](#) depends on whether a [backup window](#) exists in which the jobs can run. A backup window is a time range within which Oracle Secure Backup performs scheduled backup jobs.

Figure 5-3 Backup Windows and Scheduled Backups



A single backup window can apply to all days of the week or only to specific days or dates. The default backup window is daily 00:00-24:00. If the backup window is closed, or if no backup window is defined, then scheduled backups do not run. If a job is running when the backup window closes, then it continues to completion.

Scheduled backup jobs run with the privileges of the Oracle Secure Backup [scheduler](#): `root` on Linux and UNIX and `Local System` on Windows.



See Also:

["Configuring Backup Schedules"](#)

On-Demand Backups

In an on-demand backup, you instruct Oracle Secure Backup to perform a one-time-only backup of the specified data. For example, you might instruct Oracle Secure Backup to back up the Oracle home on client host `brhost2`. On-demand backups do not require an open backup window.

An on-demand backup job can run in privileged or unprivileged mode. A [privileged backup](#) runs under the `root` user identity on Linux and UNIX. On Windows systems, a privileged backup runs under the same account identity as the Oracle Secure Backup service on the Windows client. You must have the `perform backups as privileged user` right to make privileged backups.

An [unprivileged backup](#) runs under the Linux or UNIX user identity or Windows account identity configured in the [Oracle Secure Backup user](#) profile. Access to file-system data is constrained by the privileges of the Linux or UNIX user identity or Windows account identity.

 **See Also:**

- ["About Operating System Accounts"](#)
- *Oracle Secure Backup Reference* for more information about the `perform backups as privileged user` right

About Transferring Ownership of Backups

You can transfer ownership of backups that you create to another Oracle Secure Backup user.

Backups can be listed or restored only by the backup owner and the Oracle Secure Backup administrative user. Scheduled backups are owned by the Oracle Secure Backup administrative user. On-demand backups are owned by the Oracle Secure Backup user who created the backup job. Starting with Oracle Secure Backup version 12.1.0.3, you can transfer ownership of a backup to another Oracle Secure Backup user at the time of creating the backup. In this case, the backup job runs with the privileges and identity of the specified user.

Restartable Backups

If a file-system backup fails due to an unexpected event like a network failure, power outage, unexpected system shutdown, or tape media error, then Oracle Secure Backup must usually restart the backup from the beginning. Some types of backups are restartable from a mid-point, however, after such a failure occurs.

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 a server that uses [NDMP](#) version 3 or later.
- The `restartablebackups` policy in the `operations` class is enabled. This is the default setting.
- The backup has reached a point from which it can be restarted.

A checkpoint is a collection of state information that describes a midpoint in a backup and how to restart from it. Some information for each checkpoint resides on the Oracle Secure Backup administrative server, whereas the remainder resides on the client host.

 **Note:**

If you use the restartable backups feature, then ensure that the `/tmp` directory on the administrative server is on a partition that maintains sufficient free space.

At the beginning of each backup job, Oracle Secure Backup automatically determines whether the backup can be restarted from a midpoint. If it can be restarted, then Oracle Secure Backup periodically establishes a checkpoint that it can later use to restart the backup. After each additional checkpoint is recorded, the previous checkpoint is discarded.

When considering jobs to run, the Oracle Secure Backup scheduler takes note of restartable jobs that were interrupted before completing. If it finds a restartable job, then the scheduler restarts it and uses the same `volume` and tape drive in the same tape library in use when the interruption occurred.

 **See Also:**

["Managing Checkpoints"](#)

Preparing to Perform File-System Backups

This section directs you to plan your file-system backup by choosing the required backup strategy and backup schedule. This section includes the following topics:

- [Choosing a Backup Strategy](#)
- [Choosing a Backup Schedule](#)

Choosing a Backup Strategy

Because there is no single best method for managing backups that works for all sites, Oracle Secure Backup gives you flexibility in the way that you perform backups. You must consider several factors when determining the best method of performing backups at your site:

- How much data are you required to back up?

If you are required to back up a large amount of data, then you probably want to consider some combination of full backup and incremental backup operations. Incremental backups enable you to control how much data is backed up, thereby reducing the number of volumes you need for the backup image instance and the amount of time required to perform the backup. Make sure that each dataset file includes only the path names that you must include in the backup.

 **See Also:**

["File-System Backup Types"](#)

- How frequently does your management or users expect you to make a full backup?
- How frequently are you required to restore data?

You might be required to perform restore operations many times a day or only rarely. If you must restore data frequently, then you might want to perform full backups frequently to decrease the amount of time needed to restore. If you perform restore operations infrequently, however, then you might want to save time, media, and disk space by performing full backups less frequently.

- How much time do you want to spend performing backup and restore operations?

If your schedule includes frequent full backups, then you probably spend more time performing the backups and less time restoring data. If your schedule includes less frequent full backups, then you probably spend less time performing the backups and more time restoring data.

- How much disk space do you have available?

Oracle Secure Backup catalog files are stored in the Oracle Secure Backup home on the administrative server. If you need more disk space than is available on a single administrative server, then you might want to use multiple administrative domains.

See Also:

- ["About the Administrative Domain"](#)
- ["About the Oracle Secure Backup Catalog"](#)

Choosing a Backup Schedule

When you make a full backup, Oracle Secure Backup copies all data regardless of whether the data changed since the last backup. A full backup is equivalent to a level 0 incremental backup.

See Also:

["File-System Backup Types"](#)

When you make an incremental backup, Oracle Secure Backup backs up only the data that has changed since a previous backup. A cumulative incremental backup copies only data that has changed since an incremental backup at a lower level. For example, a level 3 incremental backup only copies data that has changed since a level 2 backup. A differential backup, which is equivalent to a level 10 incremental backup, copies data that has changed since an incremental backup at the same or lower level.

Incremental backups can help save time and media space, but they can also increase your use of media and the time required to restore data. If you were to perform only full backups, then you are required to restore only the contents of the most recent backup image instance to fully restore a given tree. If you use incremental backups, however, then you might be required to restore several backup image instances.

A typical strategy is to use cumulative backups. For example, you could create a level 0 backup and then repeat level 3 backups on successive days. The level number that you select is arbitrary; the key is that the number is between 1 and 9 and that it is the same value every night. The advantage to a cumulative strategy is that to restore a directory, only the level 0 backup and one level 3 backup from the date required would be necessary.

A differential backup backs up the files modified since the last backup at the same or lower level. The advantage to using a differential backup strategy is that less data is backed up every night so it is quicker and uses less storage space. The disadvantage is that more backups are required to restore a directory.

By analyzing how data is used and when you might be required to restore data, you can create a backup schedule that takes into account the trade-off between the cost to back up and the cost to restore. The following example demonstrates one way you might create a cumulative backup schedule.

Suppose that most changes to the `/data` file-system tree on client `c_host` occur during the week. Few changes, if any, occur on the weekend. In this situation, you might use the following schedule:

- Full backup (level 0) on Sunday night
- Level 1 incremental backups on Monday, Tuesday, Wednesday, and Thursday nights to capture changes made after the Sunday backup
- Level 2 incremental backup on Friday night to capture changes made after the Thursday backup

Given the preceding backup schedule, restoring `/data` on Monday would require only the volumes written during the full backup on Sunday. Restoring `/data` on Tuesday through Friday would require the volumes from the full backup made on Sunday and the most recent incremental backup. Restoring `/data` on Saturday or Sunday would require the volumes from the full backup made on Sunday, the incremental backup made on Thursday, and the incremental backup made on Friday.

Steps to Perform File-System Backups

This section lists the essential tasks to perform a file-system backups. It describes the necessary configurations for datasets, schedules, and triggers. This section contains the following topics:

- [Creating Dataset Files](#)
- [Configuring Backup Windows](#)
- [Configuring Backup Schedules](#)
- [Configuring Triggers](#)

Creating Dataset Files

This section describes how to create a dataset file, which describes the file-system data that Oracle Secure Backup should back up.

This section contains these topics:

- [Dataset File Examples](#)
- [Displaying the Datasets Page](#)
- [Adding a Dataset File](#)
- [Checking a Dataset File](#)
- [Editing a Dataset File](#)
- [Renaming a Dataset File](#)
- [Removing a Dataset File](#)

 **See Also:**

- ["Backup Datasets"](#)
- *Oracle Secure Backup Reference* for information on the dataset language syntax

Dataset File Examples

When configuring a dataset file, it might be helpful to study the dataset files in the samples subdirectory of the Oracle Secure Backup home directory. The sample dataset files use the *.ds extension.

Including Only One Host in Each Dataset File

A typical strategy is to create one dataset file for each host to back up. For example, assume that your administrative domain includes client hosts `brhost2`, `brhost3`, and `brhost4`. You could create the dataset files `brhost2.ds`, `brhost3.ds`, and `winhost1.ds` as shown in the following examples. Each of the examples excludes core dumps and editor backup files.

[Example 5-2](#) includes all files in the `/`, `/usr`, and `/home` file systems on host `brhost2` except for core dumps and editor backup files.

[Example 5-3](#) includes all files in the `/` and `/usr` file systems on host `brhost3` except for core dumps and editor backup files.

[Example 5-4](#) includes all files in the `C:\Documents and Settings` folder on host `winhost1` except for log files.

 **Note:**

Surround path names containing spaces with single or double quotes, for example, `"C:\Documents and Settings"`.

When you want Oracle Secure Backup to back up data, you specify the name of the dataset file that describes the contents of the backup. [Example 5-5](#) uses `obtool` to schedule three backups jobs on Saturday morning.

Alternatively, you could create a dataset directory and save the dataset files into this directory. You could then schedule a backup that specifies this dataset directory, which is equivalent to naming all of the dataset files contained within the directory tree. For example, if you create a dataset directory `brhost` that includes `brhost2.ds`, `brhost3.ds`, and `winhost1.ds`, then you could schedule a backup as follows:

```
ob> mksched --dataset brhost --day saturday --time 08:00 brhost.sch
```

Including Multiple Hosts in One Dataset File

If you have several hosts that use the same file-system structure, then you can create a single dataset file that specifies all of the hosts. The `brhosts.ds` dataset file in [Example 5-6](#) specifies the backup of the `/` and `/home` file systems on hosts `brhost2`, `brhost3`, and `brhost4`.

You could schedule a backup as follows:

```
ob> mksched --dataset brhosts.ds --day saturday --time 08:00 brhosts.sch
```

Unless an unusual event occurs, such as a tape device failure, disk failure, or a client host that is not available, Oracle Secure Backup attempts to back up the hosts in the order listed in the dataset file to the same [volume set](#) on the same [media server](#).

**See Also:**

Oracle Secure Backup Reference for dataset syntax and examples of datasets

Example 5-2 brhost2.ds

```
include host brhost2 {
  exclude name core
  exclude name *.bak
  exclude name *~

  include path /
  include path /usr
  include path /home
}
```

Example 5-3 brhost3.ds

```
include host brhost3 {
  exclude name core
  exclude name *.bak
  exclude name *~

  include path /
  include path /usr
}
```

Example 5-4 winhost1.ds

```
include host winhost1
include path "C:\Documents and Settings" {
  exclude name *.log
}
```

Example 5-5 Scheduling Three Backups

```
ob> mksched --dataset brhost2.ds --day saturday --time 08:00 brhost2.sch
ob> mksched --dataset brhost3.ds --day saturday --time 09:00 brhost3.sch
ob> mksched --dataset winhost1.ds --day saturday --time 10:00 winhost1.sch
```

Example 5-6 brhosts.ds

```
include host brhost2
include host brhost3
include host brhost4

include path /
include path /home
```

Displaying the Datasets Page

This section describes the steps needed to display the Oracle Secure Backup datasets page.

To display the datasets page

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click Backup.
3. On the Backup page, click **Datasets** to display the Datasets page.

This page lists every dataset file and dataset directory. Dataset directories appear in the Path list with a slash as the last character in the name. You can perform all dataset configuration tasks in this page or in pages to which it provides links.

See Also:

Oracle Secure Backup Reference to learn about the dataset commands in `obtool`

Adding a Dataset File

You can use the Web tool to list the contents of a dataset file. You must have the `display administrative domain's configuration right` to add a dataset.

To add a dataset file:

1. Follow the steps in "[Displaying the Datasets Page](#)".
The Backup: Datasets page appears.
2. Click **Add**.
The Backup: Datasets > New Datasets page appears.
3. Select **File** or **Directory** in the **Dataset type** list.
4. Enter a name for the dataset file in the **Name** field.
5. When you create a dataset file, the initial contents of the dataset are defined by a dataset template. Update the dataset statements displayed in the template file to define your backup data.

Like Windows and UNIX file systems, Oracle Secure Backup dataset files are organized in a naming tree. You can optionally create dataset directories to help you organize your dataset files. Dataset directories can be nested up to 10 levels deep.

When you want Oracle Secure Backup to back up data, you identify the name of the dataset file that defines the data. If you give the name of a dataset directory, then it is equivalent to naming all of the dataset files contained within the dataset directory tree.

See Also:

Oracle Secure Backup Reference for dataset syntax and examples of datasets

 **Note:**

Some NDMP data services provide for backup of directories and their contents only. You cannot explicitly back up individual files. You can restore both individual files and directory trees. This situation applies to Network Appliance's Data ONTAP.

6. Click **Save.**

The Backup: Datasets page displays a success message and your dataset file appears in the Datasets list.

 **See Also:**

"[Checking a Dataset File](#)" for details on errors

Checking a Dataset File

This section explains how to check a dataset file for errors. When you check a dataset file, you perform a syntactic check to ask the dataset parser if your use of the dataset language is correct. You can check a dataset file at any time during editing.

To check a dataset file for errors:

1. Follow the steps in "[Displaying the Datasets Page](#)".
The Backup: Datasets page appears.
2. Select a dataset file from the **Path** list and click **Check Dataset**.

 **Note:**

You can only check a dataset file, not a dataset directory.

3. Click **Check Dataset.**

If the dataset syntax has no errors, then the Oracle Secure Backup Web tool displays a message verification. If the dataset syntax has an error, then the Oracle Secure Backup Web tool displays a message indicating the error.

4. Fix any errors that appear and recheck the dataset syntax.

Editing a Dataset File

You can use the Web tool to edit an existing dataset file. You must have the `modify administrative domain's configuration` right to edit a dataset file.

To edit parameters in an existing dataset file:

1. Follow the steps in "[Displaying the Datasets Page](#)".
The Backup: Datasets page appears.
2. Select a dataset file from the **Path** list and click **Open**.

The Backup: Datasets > *dataset_name* page appears.

3. Make whatever changes you want to the dataset template and click **Save**.

You cannot change the dataset file name from this page. If you want to rename a dataset file, then see "[Renaming a Dataset File](#)".

Oracle Secure Backup automatically checks the dataset file for errors. If it finds no errors, then the Backup: Datasets page displays a success message. If an error was found, then see "[Checking a Dataset File](#)".

Renaming a Dataset File

You can use the Web tool to rename a dataset file or dataset directory. You must have the `modify administrative domain's configuration` right to use the `rends` command.

To rename a dataset file or dataset directory:

1. Follow the steps in "[Displaying the Datasets Page](#)".

The Backup: Datasets page appears.

2. Select the dataset file or directory from the **Path** list and click **Rename**.

A different page appears.

3. Enter the name for the dataset file or directory in the **Rename /dataset_name to /** field and click **Yes**.

The Backup: Datasets page displays a success message, and your dataset file or directory appears in the Path list.

Removing a Dataset File

You can use the Web tool to remove a dataset file or dataset directory. You must have the `modify administrative domain's configuration` right to remove a dataset file.

To remove a dataset file or dataset directory:

1. Follow the steps in "[Displaying the Datasets Page](#)".

The Backup: Datasets page appears.

2. Select a dataset file or directory from the **Path** list and click **Remove**.

3. Click **Remove**.

A confirmation page appears.

4. Click **Yes** to remove the dataset file or directory.

The Backup: Datasets page displays a success message, and the dataset file or directory no longer appears in the Path list.

Configuring Backup Windows

This section describes backup windows, which are user-specified time ranges within which Oracle Secure Backup can perform a scheduled backup job. The default backup window is daily 00:00-24:00 and should only be changed if necessary for your environment.

This section contains these topics:

- [Displaying the Backup Windows Page](#)

- [Adding a Backup Window](#)
- [Removing a Backup Window](#)



See Also:

"[Scheduled Backups](#)" for a conceptual overview of backup windows

Displaying the Backup Windows Page

To display the Backup Windows page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)"
2. Click **Configure**.
3. On the Configure page, click **Backup Windows** in the Advanced section to display the Configure: Backup Windows page.

You can perform all backup window creation and configuration tasks in this page or in pages to which it provides links.



See Also:

Oracle Secure Backup Reference to learn about the backup window commands in `obtool`

Adding a Backup Window

You can use the Web tool to add a backup window, which is a time and day range, to an existing list of backup windows. You must have the `modify administrative domain's configuration` right to add a backup window.

To add a backup window:

1. Perform the procedure in "[Displaying the Backup Windows Page](#)".
The Configure: Backup Windows page appears.
2. Click **Add**.
3. In the **Type** list, select a backup window type. Your choices are:
 - **Day range**
 - **Date**
4. If you selected **Day range** in step 3, then select the days for which you want to set the backup window. Your choices are:
 - **Daily**
Specify this option to set the backup window for each day of the week.
 - **Weekdays**
Specify this option to set the backup window for Monday through Friday.
 - **Weekend**

Specify this option to set the backup window for Saturday and Sunday.

5. If you selected **Date** in step 3, then specify the date on which you want the backup to run in the **Month**, **Day**, and **Year** fields.

Enter a local time range of day in which to run a backup job in the **Time range** field. The time is expressed in 24-hour format.

6. Enter a local time range in the **Time range** field.

Oracle Secure Backup starts each scheduled backup during this time range.

The Time range option is a time-of-day specifier in the form hour:minute:second or a 4-digit hour-minute specifier. An example of a 4-digit specifier is 1430, equivalent to 2:30 pm. Time ranges are expressed in 24-hour format. The time range is based on local time and takes into account Daylight Savings Time, if it applies to your locale.

When the backup window close time arrives, Oracle Secure Backup completes any backups that have been started. No more backups are started until the window opens again.

If the close time precedes the open time, then Oracle Secure Backup assumes that the close time refers to the following day. For example, 20:00-11:00 indicates 8:00 pm as the open time and 11:00 a.m. the next day as the close time.

7. Click **OK** to add the backup window.

The Configure: Backup Windows page displays a success message, and your backup window appears in the list. If you added a backup window that differs from an existing backup window only in its time range, then the backup window does not appear as a separate entry in the list. It appears instead as a second time range value for the existing backup window.

For example, if you have an existing daily backup window with a 12:00-12:30 time range, and you add another daily backup window with a 14:00-14:30 time range, then the Configure: Backup Windows page displays the following:

```
daily      12:00-12:30, 14:00-14:30
```

Removing a Backup Window

You can use the Web tool to remove a backup window or specific time ranges. Oracle Secure Backup displays an error if no backup windows within the specified range exist. You must have the `modify administrative domain's configuration` right to remove a backup window.

To remove an existing backup window:

1. Perform the procedure in "[Displaying the Backup Windows Page](#)".

The Configure: Backup Windows page appears.

2. Select the backup window to remove.
3. Click **Remove**.

A confirmation page appears.

4. Click **Yes** to remove the backup window.

The Configure: Backup Windows page displays a success message, and the backup window no longer appears in the list.

If you have multiple time ranges specified for a backup window type, then they are all removed. If you want to retain one or more of multiple time ranges, then you must add them back in.

 **See Also:**

["Adding a Backup Window"](#)

Configuring Backup Schedules

This section explains how to create and configure a backup schedule. Backup schedules tell Oracle Secure Backup what data to back up and when. In the backup schedule you specify:

- Days of the week, month, quarter, or year on which you want to perform a backup job
- Time (on each day) that a backup is to begin
- Name of a [media family](#) to use

Oracle Secure Backup uses the characteristics of volume sets eligible to use for the backup from the media family name.

This section contains these topics:

- [Displaying the Schedules Page](#)
- [Adding a Backup Schedule](#)
- [Editing or Viewing Backup Schedule Properties](#)
- [Removing a Backup Schedule](#)
- [Renaming a Backup Schedule](#)

Displaying the Schedules Page

To Display the Schedules page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Backup**.
3. On the Backup page, click **Schedules** to display the Backup: Schedules page.

You can perform all backup schedule creation and configuration tasks in this page or in pages to which it provides links.

 **See Also:**

Oracle Secure Backup Reference to learn about the schedule commands in `obtool`

Adding a Backup Schedule

You can use the Web tool to create a backup schedule. A schedule contains 0 or more triggers. A trigger is a user-defined set of days and times 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.

To add a backup schedule:

1. Perform the procedure in "[Displaying the Schedules Page](#)".

The Backup: Schedules page appears.

2. Click **Add**.

The Backup: Schedules > New Schedules page appears.

3. Enter a name for the schedule in the **Schedule** field.

The name you enter must start with an alphanumeric character. It can contain letters, numerals, dashes, underscores, or periods. It cannot contain spaces. The maximum character length is 127 characters.

4. Enter a priority number for the backup job in the **Priority** field.

The priority for a job is a positive numeric value. The lower the value, the greater the importance assigned to the job by the scheduler. The scheduler gives preference to dispatching more important jobs over those having lesser importance. The default priority is 100.

5. In the **State** field, select Enabled to enable the backup schedule.

If you want to disable the backup schedule at creation and then enable it at a later time, then select Disabled.

6. In the **Encryption** field, select Yes to encrypt the backup regardless of the settings for the global or host-specific encryption policies.

7. In the **Run as User** field, select the Oracle Secure Backup user under whose identity and privileges the backup job must run. Ownership of the backup job is transferred to the specified user, who can list, view the transcript, or cancel the newly-created backup job. After the backup is created, it is owned by the specified user.

You must have the following rights to use this option: *perform file-system backups as privileged user, modify any backup, regardless of its owner, and modify any job, regardless of its owner.*

8. Select the dataset file or dataset directory to include in the backup job in the **Datasets** list.

9. Select a restriction in the **Restrictions** field.

This step is optional. You can restrict a scheduled backup to a specific backup container. If you do not select a restriction, then the backup defined by the schedule can use any available tape device on any media server, at the discretion of the Oracle Secure Backup scheduling system.

10. Enter any information that want to store with the backup schedule in the **Comments** field.

This step is optional

11. Click **OK**.

The Backup: Schedules page displays a success message, and your additional backup schedule appears in the list of schedules.

Editing or Viewing Backup Schedule Properties


You can use the Web tool to display information about backup, vaulting scan, and duplication scan schedules. You must have the `display administrative domain's configuration` right to view backup schedules.

To edit or view properties for an existing backup schedule:

1. Perform the procedure in "[Displaying the Schedules Page](#)".

The Backup: Schedules page appears.

- In the Schedules page, select the schedule you want to edit or view and click **Edit**.
The Backup: Schedules > *schedule_name* page appears.
- Make whatever changes you want.
You cannot rename a backup schedule from this page. To rename a backup schedule, see "[Renaming a Backup Schedule](#)".
- Click Apply to apply the changes and remain on the Backup: Schedules > *schedule_name* page.
- Click **OK** to accept the changes you made.
The Backup: Schedules page displays a success message, and your edited schedule appears in the schedules list.
- Click **Triggers** to define triggers for a backup schedule.
A trigger is a calendar-based time at which a scheduled backup becomes eligible to run. Without at least one trigger, a backup you have scheduled never runs.

 **See Also:**
"[Configuring Triggers](#)"

- Click **Cancel** to return to the Backup: Schedules page without changing anything.
If you have clicked Apply, then clicking Cancel does not undo the changes you requested. If you click Apply and later change your mind, then you must enter the values you want and click Apply or OK again.

Removing a Backup Schedule

You can use the Web tool to remove a backup schedule. You must have the `modify administrative domain's configuration` right to remove a schedule.

To remove an existing backup schedule:

- Perform the procedure in "[Displaying the Schedules Page](#)".
The Backup: Schedules page appears.
- Select the backup schedule to remove from the list of schedules and click **Remove**.
A page appears with a confirmation message.
- Click **Yes**.
The Backup: Schedules page displays a success message, and the backup schedule no longer appears in the list of schedules.

Renaming a Backup Schedule

You can use the Web tool to rename a backup schedule. You must have the `modify administrative domain's configuration` right to rename a schedule.

To rename a backup schedule:

- Perform the procedure in "[Displaying the Schedules Page](#)".
The Backup: Schedules page appears.

2. Select the backup schedule to rename from the list of schedules and click **Rename**.
A different page appears.
3. Enter a name for the backup schedule in the **Rename *schedule_name* to** field and click **Yes**.
The Backup: Schedules page displays a success message, and your backup schedule appears in the list of schedules with its changed name.

Configuring Triggers

This section explains how to create and configure backup triggers. A trigger is a calendar-based time at which a scheduled backup becomes eligible to run. For example, you can specify that a backup is eligible to run on the first and third Sunday of the month. You can add multiple triggers to a backup schedule. Without at least one trigger, a backup you have scheduled never runs.

You can create triggers to perform backups only once or at intervals ranging from daily to yearly.

This section contains these topics:

- [Displaying the Triggers Page](#)
- [Creating a One-Time Backup Trigger](#)
- [Creating a Daily Backup Trigger](#)
- [Creating a Monthly Backup Trigger](#)
- [Creating a Quarterly Backup Trigger](#)
- [Creating a Yearly Backup Trigger](#)
- [Editing a Trigger](#)
- [Removing a Trigger](#)
- [Displaying a Trigger Schedule](#)

Displaying the Triggers Page

You can use the Backup: Schedules > *schedule_name* > Triggers page to display, create, modify, and delete triggers.

To display the Triggers page:

1. Follow the steps in "[Displaying the Schedules Page](#)".
The Backup: Schedules page appears.
2. Select the schedule to which you want to add a trigger and click **Edit**.
The Backup: Schedules > *schedule_name* appears.
3. Click **Triggers**.
The Backup: Schedules > *schedule_name* > Triggers page appears, as shown in [Figure 5-4](#).

Figure 5-4 Triggers Page

Home Configure Manage Backup Restore

Backup: Schedules > OSB-CATALOG-SCHED > Triggers

Add Edit Remove Cancel Preview

ID	Level	Time	Day and Date
1	full	00:00	(none)

Backup Image Name

Backup level: full Media family: null

Backup at: 00 hours 00 minutes Expire after: disabled

Trigger type: Day

Select daily
 Select weekdays
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Select weekend
 Sunday
 Saturday

Week in month: All Selected First Second Third Fourth Fifth Last

Weekday exceptions: Except: none Time: none Specify day: none none

Creating a One-Time Backup Trigger

You can use the Web tool to add a trigger to an existing backup schedule. You must have the modify administrative domain's configuration right to create a trigger.

To create a one-time backup trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".

The Backup: Schedules > *schedule_name* > Triggers page appears.

2. Select **One time** from the **Trigger type** list.
3. Select a backup level from the **Backup level** list:

- **full** (default)

Select this option to back up all data in a dataset, regardless of when they were last backed up. This option is identical to backup level 0.

- **1 to 9**

Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.

- **incr**

Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.

 **Note:**

Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.

- **offsite**

Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup in such a manner that it does not affect the full or incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.

4. Select the time at which you want to start the backup in the **Backup at** hours and minutes lists.
The time is in military format.
5. Select a media family to which the data of this scheduled backup should be assigned in the **Media family** list.
6. Enter an expiration time period for the backup job in the **Expire after** field.
7. Select the date for the one-time backup to run in the **Month**, **Day**, and **Year** lists.
8. Click **Add** to accept your entries and add the trigger.

The Backup: Schedules > schedule_name > Triggers page displays a success message, and your trigger appears in the list of triggers.

Creating a Daily Backup Trigger

You can use the Web tool to add a repeating trigger to an existing backup schedule. You must have the `modify administrative domain's configuration` right to create a trigger.

To create a daily backup trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > schedule_name > Triggers page appears.
2. Select **Day** from the **Trigger type** list.
3. Select a backup level from the **Backup level** list:
 - **full** (default)
Select this option to back up all data in a dataset, regardless of when they were last backed up. This option is identical to backup level 0.
 - **1 to 9**
Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.
 - **incr**
Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.

 **Note:**

Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.

- **offsite**

Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup in such a manner that it does not affect the full or incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.
- 4. Select the time at which you want to start the backup in the **Backup at** hours and minutes lists.

The time is in military format.
- 5. Select a media family to which the data of this scheduled backup should be assigned in the **Media family** list.
- 6. Enter an expiration time period for the backup job in the **Expire after** field.
- 7. Select the days during which Oracle Secure Backup runs the scheduled backup:
 - **Select daily**

Check this option to trigger the schedule to run on all 7 days of the week.
 - **Select weekdays**

Check this option to trigger the backup to run Monday through Friday.
 - **Select weekend**

Check this option to trigger the backup to run Saturday and Sunday.
 - Alternatively, from both the **Select weekdays** and **Select weekends** options you can select a mix of individual days on which you can trigger scheduled backups to run. For example, you can trigger the backup on Monday, Tuesday, and Saturday.
- 8. Select an option from the **Week in month** group to limit which week in the month the backup schedule runs. Your choices are:
 - **All**

Select this option to include all weeks.
 - **Selected**

Select this option to specify the week to include. For example, select **First** to trigger the backup in the first week of the month.
- 9. Specify weekday exceptions in the **Except** list.

An exception prevents Oracle Secure Backup from backing up data on the day you specify. Your choices are:

 - **none** (default)

Select this option to specify that there are no exceptions.
 - **except**


Select this option to enable an exception.

10. Select a time for the exception in the **Time** list. Your choices are:
 - **before**
Select this option to specify an exception before a specified day.
 - **after**
Select this option to specify an exception after a specified day.
11. Select the day of the exception in the **Specify day** lists.
12. Click **Add** to accept your entries and add the trigger.
The Backup: Schedules > schedule_name > Triggers page displays a success message, and your trigger appears in the list of triggers.

Creating a Monthly Backup Trigger

You can use the Web tool to add a trigger that repeats every month to an existing backup schedule. You must have the `modify administrative domain's configuration` right to create a trigger.

To schedule a monthly backup trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > schedule_name > Triggers page appears.
 2. Select **Month** from the **Trigger type** list.
 3. Select a backup level from the **Backup level** list:
 - **full** (default)
Select this option to back up all data in a dataset, regardless of when they were last backed up. This option is identical to backup level 0.
 - **1 to 9**
Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.
 - **incr**
Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.
-  **Note:**
Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.
- **offsite**
Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup in such a manner that it does not affect the full/incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.

4. Select the time at which you want to start the backup in the **Backup at** hours and minutes lists.
The time is in military format.
5. Select a media family to which the data of this scheduled backup should be assigned in the **Media family** list.
6. Enter an expiration time period for the backup job in the **Expire after** field.
7. In the **Day in month** group, select a day of the month.
8. Click **Add** to accept your entries and add the trigger.

The Backup: Schedules > schedule_name > Triggers page displays a success message, and your trigger appears in the list of triggers.

Creating a Quarterly Backup Trigger

You can use the Web tool to add a trigger that repeats every quarter to an existing backup schedule. You must have the `modify administrative domain's configuration` right to create a trigger.

To schedule a quarterly backup trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".

The Backup: Schedules > schedule_name > Triggers page appears.

2. Select **Quarter** from the **Trigger type** list.
3. Select a backup level from the **Backup level** list:

- **full** (default)

Select this option to back up all data in a dataset, regardless of when they were last backed up. This option is identical to backup level 0.

- **1 to 9**

Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.

- **incr**

Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.

Note:

Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.

- **offsite**

Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup in such a manner that it does not affect the full or incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.

4. Select the time at which you want to start the backup in the **Backup at** hours and minutes lists.
The time is in military format.
5. Select a media family to which the data of this scheduled backup should be assigned in the **Media family** list.
6. Enter an expiration time period for the backup job in the **Expire after** field.
7. Select one of these options:
 - **Day of quarter** (day 01 to 92)
Select this option to specify a day of the quarter. Day 92 is treated as the last day in the quarter even if there are less than 92 days in the quarter.
 - **Month and day of quarter**
Select a month of the quarter (01, 02, 03) and day in the month.
8. Click **Add** to accept your entries and add the trigger.
The Backup: Schedules > schedule_name > Triggers page displays a success message, and your trigger appears in the list of triggers.

Creating a Yearly Backup Trigger

You can use the Web tool to add a trigger that repeats every year to an existing backup schedule. You must have the `modify administrative domain's configuration` right to create a trigger.

To create a yearly backup trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > schedule_name > Triggers page appears.
2. Select **Year** from the **Trigger type** list.
3. Select a backup level from the **Backup level** list:
 - **full** (default)
Select this option to back up all data in a dataset, regardless of when they were last backed up. This option is identical to backup level 0.
 - **1 to 9**
Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.
 - **incr**
Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.

 **Note:**

Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.

- **offsite**

Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup in such a manner that it does not affect the full or incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.

4. Select the time at which you want to start the backup in the **Backup at** hours and minutes lists.
The time is in military format.
5. Select a media family to which the data of this scheduled backup should be assigned in the **Media family** list.
6. Enter an expiration time period for the backup job in the **Expire after** field.
7. Select one of these options:
 - **Day of the year**
Select this option to specify a day of the year (1 to 366).
 - **Date each year**
Select this option to specify a month (1 to 12) and day (1 to 31)
8. Click **Add** to accept your entries and add the trigger.
The Backup: Schedules > schedule_name > Triggers page displays a success message, and your trigger appears in the list of triggers.

Editing a Trigger

You can use the Web tool to edit a trigger that already exists in a backup schedule. You must have the `modify administrative domain's configuration` right to edit a trigger.

To edit a trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > schedule_name > Triggers page appears.
2. Select the trigger you want to edit in the list of triggers and click **Edit**.
3. Make whatever changes you want.
4. Click **Apply**.

The Backup: Schedules > schedule_name > Triggers page displays a success message, and your edited trigger appears in the list of triggers.

Note:

You can quickly add a trigger that differs only slightly from an existing trigger by editing the existing trigger and then clicking **Add**.

Removing a Trigger

You can use the Web tool to remove a trigger that already exists in a backup schedule. You must have the `modify administrative domain's configuration` right to remove a trigger.

To remove a trigger:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > *schedule_name* > Triggers page appears.
2. Select the trigger you want to remove and click **Remove**.
The Backup: Schedules > *schedule_name* > Triggers page displays a success message, and the trigger no longer appears in the list of triggers.

Displaying a Trigger Schedule

You can use the Web tool to preview the schedules of existing triggers.

To display a trigger schedule:

1. Perform the procedure in "[Displaying the Triggers Page](#)".
The Backup: Schedules > *schedule_name* > Triggers page appears.
2. Select the trigger you want displayed and click **Preview**.

Performing Scheduled File-System Backups

This section describes the steps to create a scheduled file-system backup.

The basic steps for configuring a backup schedule are as follows:

1. Log in to the administrative domain as `admin` or an Oracle Secure Backup user with the `modify administrative domain's configuration` right.

 **See Also:**

Oracle Secure Backup Reference for more information about the `modify administrative domain's configuration` right

["Displaying the Oracle Secure Backup Web Tool Home Page"](#)

2. Create a dataset file for each backup to perform.


Dataset files are text files that describe the contents of a backup, that is, the files and directories to be included in the backup. You can create dataset files for the hosts in your administrative domain and specify which paths should be included in the backup of each host.

 **See Also:**


["Creating Dataset Files"](#)

3. Create at least one backup window.

This step is optional. Backup windows are time ranges within which Oracle Secure Backup can run a scheduled backup. If no backup windows exist, then no scheduled backups run. The default backup window is daily 00:00-24:00 and should only be changed if necessary for your environment.

 **See Also:**
["Configuring Backup Windows"](#)

4. Create a backup schedule.
Backup schedules specify the dataset, media family, backup priority, and so on.

 **See Also:**
["Adding a Backup Schedule"](#)

5. Create at least one trigger.
Triggers are the days and times that the scheduled backups run. If you create a backup schedule but do not configure triggers for this schedule, then no backups occur.

 **See Also:**
["Configuring Triggers"](#)

Performing On-Demand File-System Backups

This section contains these topics:

- [Steps to Perform On-Demand File-System Backups](#)
- [Displaying the Backup Now Page](#)
- [Adding an On-Demand Backup Request](#)
- [Removing a Backup Request](#)
- [Sending Backup Requests to the Scheduler](#)

 **See Also:**
["On-Demand Backups"](#)

Steps to Perform On-Demand File-System Backups

An on-demand backup is an ad hoc or one-time-only backup of the data in a dataset. On-demand backups are useful for supplementing a scheduled backup and testing whether the administrative domain is correctly configured.

The basic steps for creating on-demand backups are as follows:

1. Create a dataset to describe the files to be backed up.

 **See Also:**

- ["Creating Dataset Files"](#)
- *Oracle Secure Backup Reference* for more information about Oracle Secure Backup rights

2. Log in to the administrative domain as an Oracle Secure Backup user with the rights to perform the backup and the UNIX, Linux, or Windows account needed to access the data to be backed up.

You need the `perform backups as self` right to perform [unprivileged backups](#) and the `perform backups as privileged user` right to perform [privileged backups](#).

 **See Also:**

["Displaying the Oracle Secure Backup Web Tool Home Page"](#)

3. Create at least one [backup request](#).

Oracle Secure Backup saves each backup request locally in your Oracle Secure Backup Web tool or `obtool` session until you send it to the scheduler. In this state, the backup is not eligible to run.

 **See Also:**

- ["About Jobs and Requests"](#)
- ["Adding an On-Demand Backup Request"](#)

4. Review, delete, or add to the list of backup requests.

This step is optional.

 **See Also:**

- ["Displaying the Backup Now Page"](#)
- ["Removing a Backup Request"](#)

5. Send all queued backup requests to the Oracle Secure Backup scheduler.
After requests are sent to the scheduler, they are jobs and are eligible to run.

 **See Also:**

["Sending Backup Requests to the Scheduler"](#)

Displaying the Backup Now Page

To display the Backup Now page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click Backup.
3. On the Oracle Secure Backup Web tool Backup page, click **Backup Now** to display the page shown in [Figure 5-5](#). This page displays each backup request that you have created but not yet sent to the scheduler. Backup requests are identified by a backup name and number.

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. You can perform all on-demand backup creation and configuration tasks in the Backup Now page or in pages to which it provides links.

Figure 5-5 Backup Now Page



See Also:

Oracle Secure Backup Reference to learn about the backup commands in `obtool`

Adding an On-Demand Backup Request

This section explains how to create a backup request. Note that creating a backup request is not the same as sending the request to the scheduler.

To add an on-demand backup request:

1. Perform the procedure in "[Displaying the Backup Now Page](#)".
The Backup: Backup Now page appears.
2. Click **Add**.
The Backup: Backup Now > Options page appears.

3. Select a dataset file or dataset directory in the **Datasets** list.
4. (Optional) In the **Backup Image Name** field, specify a name for the backup image created by this backup job. The backup image name must be unique within the Oracle Secure Backup catalog.
5. Select a future date and time for the backup to run in the **Backup date** and **Backup time** lists.

If you leave these fields unchanged, then Oracle Secure Backup considers your backup job as eligible to run immediately.

6. Enter a time interval using the **Expire after** field and units list.

This option instructs Oracle Secure Backup to automatically expire this backup job if it has not started within the specified expiration period after the date and time intervals defined earlier in the **Backup date** and **Backup time** lists.

By default the expiration is **disabled**, which means that it never expires.

 **See Also:**

Oracle Secure Backup Reference for more information

7. Select a backup level from the **Backup level** list. Your choices are:
 - **full** (default)
Select this option to back up all data in a dataset, regardless of when it was last backed up. This option is identical to backup level 0.
 - **1 to 9**
Select an integer value to back up only those files that have changed since the last backup at a lower numeric backup level.
 - **incr**
Select this option to back up only data modified since the last backup, regardless of its backup level. This option is identical to backup level 10.

 **Note:**

Oracle Secure Backup does not support the **incr** backup level with some platforms, including NAS devices. In particular, the **incr** option does not apply to a Network Appliance filer.

- **offsite**
Select this option to specify a full (level 0) backup and instruct Oracle Secure Backup to keep a record of this backup so that it does not affect the full or incremental backup schedule. This option is useful when you want to create a backup image instance for off-site storage without disturbing your incremental backup schedule.
8. Select a media family to which this backup should be assigned in the **Media family** list.
 9. Select restrictions on this backup in the **Restrictions** field. You can select a particular backup container. You can also use click and shift-click to select a range of devices or control-click to select additional individual devices. Restrictions come in the following forms:

- *device*
This form specifies a particular backup container.
- *@hostname*
This form specifies any backup container attached to the specified host.
- *device@hostname*
This form specifies any drive-host [attachment](#).

If no device is selected, then Oracle Secure Backup uses tape device polling to find any available tape device for use in backup and restore operations.

10. Enter a priority for the backup job in the **Priority** list.

The priority of a job is a positive integer value. The default value is **100**.

The lower this value, the greater the priority assigned to the job by the scheduler. It considers priority 20 jobs, for example, more important than priority 100 jobs. The scheduler always gives preference to dispatching higher priority jobs over lower priority ones.

11. Choose whether you want the backup to operate in **unprivileged** or **privileged** mode. Unprivileged mode is the default.

You must have the `perform file system backups as privileged user` right if you specify **privileged**. Otherwise, you must have the `perform file system backups as self` right.



See Also:

"On-Demand Backups"

12. Select one of these encryption options:

- **yes**
This option specifies that the backup is encrypted.
- **no**
This option specifies that the backup is not encrypted. This is the default.
- **forced off**
This option specifies that the backup is not encrypted, overriding the host-required encryption setting
- **transient**
This option specifies a backup encrypted by Oracle Secure Backup with a user-supplied one-time passphrase. If you select this option, then you must also select an encryption algorithm option and enter a passphrase in the **specify passphrase** field.

13. In the **Specify Algorithm** field, select one of the following encryption algorithms: aes128, aes192, or aes256.
14. Select **disable hardware encryption** to disable hardware-based encryption for the backup.
15. Select **Store key** to add the transient passphrase used to encrypt this backup to the appropriate key store.

16. In the **Run as User** field, select the Oracle Secure Backup user under whose identity and privileges the backup job must run. Ownership of the backups is transferred to the specified user after the backup job is completed.
17. Click **OK**.
The Backup: Backup Now page displays a success message, and your backup request appears in the list of requests.

Removing a Backup Request

This section explains how to remove a backup request you have created, but have not yet sent to the scheduler with the Oracle Secure Backup Web tool.

To remove a backup request:

1. Perform the procedure in "[Displaying the Backup Now Page](#)".
The Backup: Backup Now page appears.
2. Select a backup request from the list and click **Remove**.
The Backup: Backup Now page displays a success message, and the backup request no longer appears in the list of backup requests.

Sending Backup Requests to the Scheduler

You can use the Web tool to send all backup requests that are queued in the request queue to the Oracle Secure Backup scheduler. Backup requests are held locally until you specify the **Go** option.

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 you specified a future date or time 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`.

To send every pending backup request to the scheduler:

1. Perform the procedure in "[Displaying the Backup Now Page](#)".
The Backup: Backup Now page appears.
2. Click **Go**.
The Oracle Secure Backup Web tool sends each backup request that appears on the page to the Oracle Secure Backup scheduler.
The Backup: Backup Now page displays a message for each request acknowledged by the scheduler. For example:

```
backup request 1 (dataset datadir.ds) submitted; job id is admin/6.
```

Oracle Secure Backup deletes each backup request upon its acceptance by the scheduler. As a result, the page displays no requests upon completion of the **Go** operation.

 **See Also:**

["Displaying Job Transcripts"](#) to view the output for each job

Backing Up Critical Data on the Administrative Server

["About the Oracle Secure Backup Catalog"](#) explains the importance of administrative data for the administrative domain. If you lose the critical data stored on the administrative server, then you lose the configuration data for the administrative domain and all backup and volume records.

Oracle Secure Backup is configured on installation to perform automatic regular catalog backup jobs. The backup administrator is required only to specify a trigger, to define the frequency of backup. No other configuration is required, but you can customize the backup by adding device restrictions, more triggers, or both.

 **See Also:**

- ["Configuring Triggers"](#)
- [Disaster Recovery of Oracle Secure Backup Administrative Data](#)

6

Restoring File-System Data

This chapter explains how to restore file-system objects backed up by Oracle Secure Backup.

This chapter contains these sections:

- [About File-System Restore Operations](#)
- [Performing a Catalog-Based Restore Operation](#)
- [Performing a Raw Restore Operation](#)

See Also:

- ["About Recovery Manager and Oracle Secure Backup"](#)
- [Disaster Recovery of Oracle Secure Backup Administrative Data](#)
- *Oracle Secure Backup Reference* for a description of the restore commands in `obtool`

About File-System Restore Operations

With Oracle Secure Backup, you can restore file-system data in the following ways:

- Catalog-based restore operation

In this type of restore operation, you browse the Oracle Secure Backup [catalog](#) for the file-system objects to be restored. When you have located their names and selected the instances, you can restore the objects. You can use [Oracle Secure Backup wildcard pattern matching](#) while performing the restore operation.

See Also:

- ["About the Oracle Secure Backup Catalog"](#) for an overview of the Oracle Secure Backup catalog
- ["About Oracle Secure Backup Wildcard Pattern Matching"](#) for more information about wildcard pattern matching

- Raw restore operation

In this type of restore operation, you identify the backup from which to restore files using the secondary storage location ([volume ID](#) and [backup image](#) file number) of a backup. A raw restore operation can be performed without using the backup catalog. You can either restore all data in the backup or specify an individual file or directory to restore.

 **See Also:**

["About Volumes"](#) for an explanation of volume IDs and backup image instances

- `obtar` restore operation

You can use the `obtar` command-line interface to operate directly on a [tape drive](#), outside the Oracle Secure Backup [scheduler](#). The `obtar` utility is intended for advanced users only.

 **See Also:**

Oracle Secure Backup Reference for more information about `obtar`

About Browsing the Oracle Secure Backup Catalog

Oracle Secure Backup maintains a discrete backup catalog for every client in the administrative domain. The catalog for each host is stored in a subdirectory of `admin/history/host` named after the client. For example, `admin/history/host/brhost2` stores the catalog for the client named `brhost2`. The catalog itself is a binary file named `indices.cur`.

To specify backups to restore, you can use `obtool` or the Oracle Secure Backup Web tool to browse the contents of any client's backup catalog, providing you have necessary permissions. The [class](#) of which your Oracle Secure Backup user is a member defines your right to browse the catalog.

While browsing the catalog through the Oracle Secure Backup Web Tool, if you see `<dirname> (E)` in red, then this indicates that a user made an attempt to specify a non-existent directory in the dataset description due to which the backup failed. This directory cannot be restored.

 **See Also:**

["Overview of Oracle Secure Backup Classes and Rights"](#) for more information about user [rights](#)

Oracle Secure Backup provides two means to control how time affects the data you select when browsing backup catalogs:

- [Catalog Data Selectors](#)
- [Example: Usage of Oracle Secure Backup Data Selectors](#)
- [Catalog View Modes](#)

Catalog Data Selectors

When you browse a backup catalog to select data to restore, you can choose specific instances of backed up data by using one of the data selectors shown in [Table 6-1](#). The data selector describes, either explicitly or by inference, the identity of each backup image section containing the data of interest.

Table 6-1 Data Selectors

Selector	Description
latest	Shows the most recent backup instance of an object
earliest	Shows the first backup instance of an object
all	Shows all backup instances of an object
<i>backup-id</i>	Shows the instance contained in the backup section identified by the backup ID. Within a backup catalog, Oracle Secure Backup identifies each backup image section with a numeric backup ID. It assigns backup IDs without regard to the time order of backups. For example, backup ID 25 can represent the Monday backup of the root directory on a host, whereas backup ID 6 represents the Tuesday backup.
<i>date-time</i>	Shows the most recent backup instance of an object backed up on or before the given date-time
<i>date-time range</i>	Shows all file-system objects backed up only during the date-time range specified

When applied to a file-system object, a data selector yields the identity of zero or more backup image sections in which the file-system object is stored.



See Also:

Oracle Secure Backup Reference for the use of data selectors in the `find` command

"[Example: Usage of Oracle Secure Backup Data Selectors](#)"

"[About Backup Image Instances and Tape Volumes](#)" for more information about backup image instances and backup sections

Example: Usage of Oracle Secure Backup Data Selectors

As an example of how Oracle Secure Backup applies data selectors to specific instances of backed up data, consider a directory called `/numbers` that you back up fully on each of three days at the beginning of May. The contents of `/numbers` changes each day.

[Table 6-2](#) shows the files that are backed up and the volume and [backup image file](#) to which they are written. The May 1 and May 2 backups were written to volume `FULL-02`. The May 3 backup filled volume `FULL-03` while writing `file2.dat`. Oracle Secure Backup continued the May 3 backup on volume `FULL-04` by writing the remainder of `file2.dat`, followed by `file4.dat`.

Table 6-2 Backup of the /numbers Directory

Date	Contents of /numbers	Backup volume and image	Backup ID
5/1/09	<code>file1.dat</code> <code>file2.dat</code> <code>file3.dat</code>	volume <code>FULL-02</code> , file 5	20

Table 6-2 (Cont.) Backup of the /numbers Directory

Date	Contents of /numbers	Backup volume and image	Backup ID
5/2/09	file2.dat file3.dat	volume FULL-02, file 9	30
5/3/09	file1.dat file2.dat	volume FULL-03, file 3, section 1	40
5/3/09 (continued)	file2.dat file4.dat	volume FULL-04, file 3, section 2	46

Table 6-3 describes the effect of various data selectors on the file-system object references.

Table 6-3 Data Selectors for Backups of the /numbers Directory

Data Selector	Object Reference	Backup Image Sections Selected (Backup IDs)
latest	/numbers/file4.dat	FULL-04, file 3, section 2 (46)
latest	/numbers/file2.dat	FULL-03, file 3, section 1 (40) and FULL-04, file 3, section 2 (46)
latest	/numbers	FULL-03, file 3, section 1 (40) and FULL-04, file 3, section 2 (46)
earliest	/numbers/file1.dat	FULL-02, file 5 (20)
earliest	/numbers	FULL-02, file 5 (20)
all	/numbers	FULL-02, file 5 (20) and FULL-02, file 9 (30) and FULL-03, file 3, section 1 (40) and FULL-03, file 3, section 2 (46)
all	/numbers/file1.dat	FULL-02, file 5 (20) and FULL-03, file 3, section 1 (40)
20,30	/numbers/file1.dat	FULL-02, file 5, section 1 (20)
20, 30	/numbers	FULL-02, file 5 (20) and FULL-02, file 9 (30)
05/09	/numbers/file1.dat	(none)
05/09	/numbers	FULL-02, file 9 (30)
05/04-05/09	/numbers/file4.dat	(none)
05/04-05/09	/numbers/file1.dat	FULL-02, file 5 (20)
05/04-05/09	/numbers	FULL-02, file 5 (20) and FULL-02, file 9 (30)

Catalog View Modes

Oracle Secure Backup consults the view mode each time it searches or displays a catalog directory. You control the view mode setting from the Oracle Secure Backup Web tool or command-line interface. There are three view modes:

- Inclusive

When you browse a directory in inclusive mode, Oracle Secure Backup displays the name of every file-system object backed up from the directory. The data selector is ignored. For example, a listing of the `/numbers` directory in [Table 6-2](#) in inclusive mode displays `file1.dat`, `file2.dat`, `file3.dat`, and `file4.dat`.

This display behavior assumes the that you did not do the following:

- Overwrite either backup image
- Manually clean up the backup catalog
- Explicitly direct Oracle Secure Backup to retire any backup catalog data
- Exact

When you browse a directory in exact mode, you display only the contents of a directory identified by a data selector, from the path that contains the backup specified. You can browse in this mode only if you are in the exact directory that contains the required backup entry. If you set the view mode to exact, then the `latest` setting in [Table 6-3](#) would display only `file1.dat`, `file2.dat`, and `file4.dat` only if you are currently browsing the `/numbers` directory.

- Specific

When you browse a directory in specific view mode, you display only the contents of a directory identified by the data selector. You can browse in this mode from the path that contains the backup entry or from a parent path. When no data selector is specified, inclusive view mode and specific view mode have the same output. If you set up the view mode to specific, and choose backup ids `20` and `40` as the data selectors, then the listing of the `/numbers` directory in [Table 6-2](#) would display `file1.dat`, `file2.dat`, and `file3.dat`.

About Oracle Secure Backup Wildcard Pattern Matching

Oracle Secure Backup enables you to search for selected files and directories within the backup catalog. You can search for a specific backup entry from a given path by providing relevant information. The `find` command allows searching for multiple entries with the use of [Oracle Secure Backup wildcard pattern matching](#). [Table 6-4](#) explains wildcard pattern matching with a few examples.

Table 6-4 Oracle Secure Backup Wildcard Pattern Matching

Pattern	Output
*	Matches zero or more characters in a string of characters. For example, pattern <code>back*</code> will match <code>backup</code> , <code>backpp</code> , and <code>back</code> .
?	Matches exactly one character. For example, pattern <code>back?p</code> will match <code>backup</code> and <code>backpp</code> . However, it will not match with <code>backuup</code> .
[] with -	Matches exactly one character in the given range. For example, <code>back[m-u]p</code> will match <code>backup</code> , <code>backmp</code> , and <code>backop</code> . However, it will not match with <code>backkp</code> and <code>backwp</code> .
[] with ^	Matches any character that is not mentioned inside []. For example, <code>back[^km]p</code> will match with <code>backup</code> . However, it will not match with <code>backkp</code> or <code>backmp</code> .

Table 6-4 (Cont.) Oracle Secure Backup Wildcard Pattern Matching

Pattern	Output
[]	Matches exactly one character listed within []. For example, pattern <code>back[mnu]p</code> will match with <code>backup</code> , <code>backmp</code> , and <code>backnp</code> . However, it will not match with <code>backkp</code> or <code>backmnp</code> .

 **Note:**

Some wildcard patterns hold a different, specific meaning on certain platforms. To avoid overlap and to perform restore successfully, these special characters must be escaped while using wildcard pattern matching with `obtool`. On Unix, use `\` as an escape character for `*`. On Windows, use `^` as an escape character for `*`.

About Filter Options Used for Wildcard Pattern Matching

You can use the following options to filter your output while using the `find obtool` command or while using the find option on the Browse Catalog page while accessing the Oracle Secure Backup web tool:

Host

You can perform the find operation on a single host or multiple hosts: the find option searches the catalog for each specified host. Oracle Secure Backup performs the search operation on a host depending on the following factors:

- If the user specifies the hostname, then the given hostname is selected overriding other settings. Multiple host names can be specified as a comma separated list.
- If the user does not provide the hostname but adds the current host option, the results for the current host are displayed.
- If user neither provides the hostname nor provides the current host option, then the host set in the variable host setting is selected.
- If none of the above conditions are met, an error is displayed.

Data Selectors

The find option searches for the path of the given file or directory based on the specified data selector. The default data selector is `latest`. For detailed information about data selectors, see "[Catalog Data Selectors](#)".

Path

The find option enables you to search for backup entries by using the path that contains the required file or directory. The following criteria is used in selecting the path while performing the find operation:

- If the user provides the pathname then search would begin from the given path.
- If the user does not provide the pathname and chooses the current path in a directory, then this particular path is considered.
- If the none of the above conditions are met, then an error is displayed.

**Note:**

Oracle Secure Backup wildcard pattern matching is not supported for path names.

Type of Entry

The Backup Catalog contains information about all files and directories that have been backed up using Oracle Secure Backup. In certain cases, you may want to search for a particular file or directory. To help you obtain the required backup, the find option lets you choose the type of entry, file or directory, while browsing the catalog. By default, Oracle Secure Backup lists both files and directories.

Volumes

You can filter the catalog content by providing the volume that contains the required backup. A file or directory can be backed up to many volumes. A comma-separated list of multiple volumes can be specified.

Disk Pools

The find option supports searching across disk pools. A comma-separated list of disk pools can be provided to customize the output of the search operation.

**See Also:**

Oracle Secure Backup Reference for the usage and examples of the `find` command

Performing a Catalog-Based Restore Operation

This section describes how to create a restore request by browsing a backup catalog.

This section contains the following topics:

- [Steps to Perform Catalog-Based File-System Restore Operations](#)
- [Displaying the Backup Catalog Page](#)
- [Browsing the Backup Catalog Page](#)
- [Creating a Catalog-Based Restore Request](#)
- [Removing a Catalog-Based Restore Request](#)
- [Sending Catalog-Based Restore Requests to the Scheduler](#)
- [Listing All Backups of a Client](#)

Steps to Perform Catalog-Based File-System Restore Operations

This section outlines the steps to perform a catalog-based restore of file-system objects that were backed up using Oracle Secure Backup.

To perform a catalog-based restore, create a file-system restore job using the following steps:

1. Log in to the [administrative domain](#) as `admin` or an [Oracle Secure Backup user](#) with the [rights](#) needed to browse and restore files. You need the following rights:

- To restore files in privileged mode or restore to an **NDMP** host, you need the `perform restores as privileged user` right.
- To restore files in unprivileged mode, you need the `perform restores as self` right.
- To browse the catalog, you need the `browse backup catalogs` with this access right set to a value other than `none`.

The possible access values are `privileged`, `notdenied`, `permitted`, `named`, and `none`.

 **See Also:**

Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

["Displaying the Oracle Secure Backup Web Tool Home Page"](#)

2. Access the Backup Catalog page by following the steps in ["Displaying the Backup Catalog Page"](#).
3. Identify the backups to restore by locating the files in the catalog.

 **See Also:**

["About Browsing the Oracle Secure Backup Catalog"](#)

4. Create one or more restore requests.

 **See Also:**

["Creating a Catalog-Based Restore Request "](#)

 **Note:**

All restore requests that have not yet been sent to the `scheduler` persist until the background timeout expires. The background timeout value identifies the maximum idle time of certain `obtool` background processes. See *Oracle Secure Backup Installation and Configuration Guide* for more information about background timeout.

5. Optionally, delete the queued restore requests if necessary.

 **See Also:**

["Removing a Catalog-Based Restore Request"](#)

6. Send the restore requests to the Oracle Secure Backup scheduler so that the requests become jobs and are eligible to run.

The Oracle Secure Backup scheduler runs the jobs according to their priority.

 **See Also:**

["Sending Catalog-Based Restore Requests to the Scheduler"](#)

Displaying the Backup Catalog Page

To display the Backup Catalog page:

1. Follow the steps in ["Displaying the Oracle Secure Backup Web Tool Home Page"](#).
2. Click **Restore**.
3. On the Restore page, click **Backup Catalog**. The Restore: Backup Catalog page appears, as shown in [Figure 6-1](#). You can use this page to browse the catalog for backups of files and directories.


Figure 6-1 Backup Catalog Page

Browsing the Backup Catalog Page

You can use the Web tool to browse the Oracle Secure Backup catalog and specify data to restore.

To browse the catalog and designate specific data to restore:


1. Perform the procedure in ["Displaying the Backup Catalog Page"](#).
The Restore: Backup Catalog page appears.
2. Select one or more data selectors in the **Data Selector** list.

 **See Also:**
["Catalog Data Selectors"](#)

3. Select a host name from the **Host Name** list.
The host should be the one on which data was originally backed up.
4. Specify the Oracle Secure Backup browse options like hostname, view mode, list options, and browse path.

 **See Also:**
["Specifying the Backup Catalog Browse Options"](#) for information on how to specify the browse options.

5. Specify the Oracle Secure Backup search options, if you are looking for the contents of a particular backup.


 **See Also:**
["Specifying the Backup Catalog Search Options"](#) for information on how to specify the browse options.

6. You can change the data selector settings and the view mode settings by adjusting the respective field selections before clicking **Browse** or **Search**.

Specifying the Backup Catalog Browse Options

To specify the browse options for restore:

1. Perform the steps in "[Displaying the Backup Catalog Page](#)".
2. Under **Browse Options**, select a host name from the **Host Name** list.
The host should be on which data was originally backed up.
3. Select a **View mode**.

 **See Also:**
["Catalog View Modes"](#) for detailed description of the inclusive, specific, and exact view modes

4. Select **Yes** to list all the files and directories that were backed up while performing this backup job. **No** is the default option.
5. You can enter the path name of the directory to browse in the **Browse Path** field. If you do not enter a path, then Oracle Secure Backup displays the top-most directory in the client naming hierarchy.
6. Click **Browse**.

The Restore: Backup Catalog > *host_name* page appears with the selected directory contents displayed.

Specifying the Backup Catalog Search Options

To specify the search options for restore:

1. Perform the steps in "[Displaying the Backup Catalog Page](#)".
2. Under **Search Options**, select the host name from the **Host Name** list.
3. You can enter the path name of the directory in the **Search Path** field.
Click a directory name to make it your current directory and view its contents.
4. You can enter the name of the file that was backed up for in the **File** field.
5. Enter the backup container where the backup is stored: tape volume or disk pool.
6. Select **Yes** to ignore the case of the information that you enter. **No** is the default option.
7. Click **Search**.

Creating a Catalog-Based Restore Request

This section explains how to specify various restore options to finalize the restore request.

To create a catalog-based restore request:

1. Follow the steps in "[Browsing the Backup Catalog Page](#)".
2. Select the name of each file-system object you want to restore.

By performing this action, you are requesting that Oracle Secure Backup restore each instance of the object identified by the data selector. To learn the identity of those instances, click the adjacent properties button view to display the object's properties page. When you are done viewing the page, click **Close**.

3. Click **Add**.

Note:

You must click **Add** before leaving the page containing your selections. If you do not, then Oracle Secure Backup discards those selections.

The New Restore page appears.

4. The original path name of each object you previously selected appears in the lower left portion of this page. To its right is a text box in which you can enter the alternate path name. If you leave this box blank, then Oracle Secure Backup restores the data to its original path.

Note:

Some NAS data servers, including Network Appliance's Data ONTAP, limit your ability to rename restored data. If you try to violate that constraint, then the restore job fails.

5. Optionally, select **Device** to specify a backup container to use to perform the restore operation.

By default, Oracle Secure Backup automatically selects the best tape drive.

6. In **Privileged restore**, select **Yes** or **No**.

An unprivileged restore runs under your Linux or UNIX user or Windows account as configured in your Oracle Secure Backup user profile. Your access to file-system data is constrained by the [rights](#) of the account having that identity. Unprivileged mode is the default.

A privileged restore job runs under the `root` user identity on Linux and UNIX systems. On Windows systems, the job runs under the same account identity as the Oracle Secure Backup service on the Windows client.

 **See Also:**

["Managing Users"](#)

7. In **Priority**, enter a priority or accept the default value of 100.

The priority for a job is a positive numeric value. The lower the value, the greater the priority assigned to the job by the scheduler. For example, priority 20 jobs are higher priority than priority 100 jobs. The scheduler dispatches higher over lower priority jobs, providing all resources required to run the job are available.

8. Optionally, in **Restore options**, enter one or more `obtar` options.

For example, `-J` enables debug output and provides a high level of detail in restore transcripts.

 **See Also:**

Oracle Secure Backup Reference for a summary of `obtar` options

9. Select **No high speed positioning** if you do not want to use available position data to speed the restore.
10. Select **NDMP incremental restore** to direct [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`.

Restore operations are usually additive. Each file and directory restored from a [full backup](#) 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 select **NDMP incremental restore**, NAS data servers restore each directory to its state in the last incremental backup image instance applied during the restore job. 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 an

ordinary restore of `/home`, the directory would contain `file1` and `file2`; after an NDMP incremental restore of `/home`, the directory would contain only `file2`.

11. Select one of the following:
 - **Replace existing files**

This option overwrites any existing files with those restored from the backup image instance.
 - **Keep existing files**

This option keeps any existing files instead of overwriting them with files from the backup image instance.
12. If you are restoring to a Windows system, then select one of these:
 - **Replace in use files**

This option replaces in-use files with those from the backup image instance. Windows deletes each in-use file when the last user closes it.
 - **Keep in use files**

This option leaves any in-use Windows files unchanged.
13. In **To host**, select the host on which to restore the files, or accept the default.
14. Optionally, in **Optional (For transient restores only)**, select **Transient** to restore backups encrypted by Oracle Secure Backup with a user-supplied one-time passphrase.

See "[About Transient Backup Encryption](#)" to learn about transient encrypted backups.
15. Optionally, click **Preview**.

The Preview page appears.

This page shows the files to be restored, the volume ID of the volume containing the backup, and the backup container in which the volume is located.
16. Optionally, in Preview click **Recall**.

The Recall page appears.

See "[Recalling and Releasing Volumes](#)" to learn how to recall volumes.
17. In the New Restore page, click **OK**.

Oracle Secure Backup displays the Browse Host page.

The restore request appears in the **Restore items** list. Oracle Secure Backup displays the message "Success: file(s) added to restore list" in the **Status** area.
18. To create additional catalog-based restore requests, return to "[About Browsing the Oracle Secure Backup Catalog](#)".

Removing a Catalog-Based Restore Request

This section explains how to remove a catalog-based restore request that you have created, but have not yet sent to the scheduler.

To remove a catalog-based restore request:

1. Follow the steps in "[Displaying the Backup Catalog Page](#)".
2. On the Backup Catalog page, select a host from the **Host Name** list.
3. Click **Browse Host**.

Oracle Secure Backup displays the **Browse Host** page.

4. In the **Restore items** list, select the restore request you want to remove.
5. Click **Remove**.

Oracle Secure Backup redisplay the page. The restore request you selected no longer appears in the **Restore items** list.

Sending Catalog-Based Restore Requests to the Scheduler

This section explains how to send all pending catalog-based restore requests to the scheduler.

To send catalog-based restore requests to the scheduler:

1. Follow the steps in "[Displaying the Backup Catalog Page](#)".
2. On the Backup Catalog page, select a host from the **Host Name** list.
3. Click **Browse Host**.

Oracle Secure Backup displays the Browse Host page.

4. Click **Go**.

The Oracle Secure Backup Web tool sends each restore request that appears in the **Restore items** list to the scheduler. A message appears in the Info bar for each request acknowledged by the scheduler. For example:

```
1 catalog restore request item submitted; job id is admin/240.
```

Oracle Secure Backup deletes each restore request upon its acceptance by the scheduler. As a result, the **Restore items** list is empty upon completion of the **Go** operation.

5. Display the transcript of the job to ensure that it completed successfully.

 **See Also:**

["Displaying Job Transcripts"](#)

Listing All Backups of a Client

This section explains how to obtain a detailed listing of all backups of a client.

To list all backups of a client host:

1. Follow the steps in "[Browsing the Backup Catalog Page](#)".
2. From the Backup Catalog page, select a host from the **Host Name** list box.
3. Click **Browse Host**.

Oracle Secure Backup displays the Browse Host page.

4. Click **List Host Backups**.

A properties page appears.

Performing a Raw Restore Operation

This section explains how to restore data without using a backup catalog.

This section contains the following topics:

- [Displaying the Directly From Media Page](#)
- [Creating a Raw Restore Request](#)
- [Steps to Perform Raw Restore Operations](#)
- [Removing a Raw Restore Request](#)
- [Sending Raw Restore Requests to the Scheduler](#)

Displaying the Directly From Media Page

To display the Directly From Media page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Restore**.
3. On the Restore page, click **Directly from Media** to display the Directly from Media page. You can use this page to perform a raw restore operation.

See Also:

Oracle Secure Backup Reference to learn about the browser commands in `obtool`

Creating a Raw Restore Request

To perform a raw restore of file-system objects, you must know the following:

- The absolute path names of file-system objects you want to restore
You must know the path names for the files when they were backed up. If you do not know these path names, then you can use `obtar -tvf` to find them or restore an entire backup image instance.
- The identity of the backup container to which they were backed up
This can be a volume ID or a [barcode](#).
- The backup image file number in which they are stored

To create a raw restore request:

1. Follow the steps "[Displaying the Directly From Media Page](#)".
2. On the Directly from Media page, click **Add**.
The Options page appears.
3. Select **Device** to specify a backup container for the restore operation.
This step is optional. By default, Oracle Secure Backup automatically selects the best tape drive.

4. Choose whether you want the restore to operate in **unprivileged** or **privileged** mode.
Unprivileged mode is the default.
5. Enter the backup image file number from which to restore data in the **File Number** text field.

 **See Also:**

"[About Volume Sets](#)" to learn about file numbers

6. Do at least one of these:
 - Enter the first volume ID from which to begin data restore in the **Volume ID(s)** field

 **See Also:**

"[About Volume Sets](#)" to learn about volume IDs

- Enter the [volume tag](#) of the first volume from which to begin restoring in the **Tag(s)** text box.
A tag is a computer-readable barcode affixed to a volume.

 **See Also:**

"[About Volumes](#)"

7. Enter one or more `obtar` options in the **Obtar option(s)** box.
This step is optional.

 **See Also:**

Oracle Secure Backup Reference for more information about `obtar`

8. Select **NDMP incremental restore** to direct certain NAS data servers to apply incremental restore rules.

Restore operations are usually additive. Each file and directory restored from a full or incremental backup is added to its destination directory. When you select NDMP incremental restore, NAS data servers that implement this feature restore each directory to its exact state as of the last incremental backup image applied during the restore job. Files that were deleted before the last incremental backup are deleted by the NAS data service upon restore of that incremental backup.

9. Select one of these:
 - **Replace existing files**
This option overwrites any existing files with those restored from the backup image instance.
 - **Keep existing files**

This option keeps any existing files instead of overwriting them with files from the backup image instance.

10. If you are restoring to a Windows system, then select one of these:

- **Replace in use files**

This option replaces in-use files with those from the backup image instance. Windows deletes each in-use file when the last user closes it.

- **Keep in use files**

This option leaves any in-use Windows files unchanged.

11. Select one of these:

- **All**

This option restores the entire contents of the backup image file you selected.

- **File**

This option restores a specific file or directory. If you select **File**, then enter the name of the file or directory to restore in the text box to the right of the **File** option.

If you know the position of the file in the backup image instance as reported previously by Oracle Secure Backup, then enter it in the **Position** field. If you do not, then leave this field blank.

12. Select a host to which to restore the data in the **To host** list.

13. Enter a path name in the **Alternate path** field to restore data using a different name than the one that was saved.

Suppose you want to restore the home directory for brhost2. The absolute path for the directory on the brhost2 file system was `/export/home/brhost2`. To restore to an alternative directory, enter the alternative path and the desired final directory name. For example, you could restore `/export/home/brhost2` to `/tmp/brhost2-restored`.

The same technique works for individual files. For example, you could restore `/export/home/brhost2/.cshrc` to `/tmp/.cshrc-restored`.

14. Click **OK** to accept your selections or **Cancel** to discard them.

Oracle Secure Backup returns you to the **Restore from Media** page. If you clicked **OK**, then the raw restore request you just made appears in the list. Oracle Secure Backup displays the message, "Success: restore task created" in the **Status** area.

Steps to Perform Raw Restore Operations

Use the following steps to perform a raw restore operation of file-system backup:

1. Log in to the [administrative domain](#) as `admin` or an [Oracle Secure Backup user](#) with the [rights](#) needed to browse and restore files. You need the following rights:

- To restore files in privileged mode or restore to an [NDMP](#) host, you need the `perform restores as privileged user` right.
- To restore files in unprivileged mode, you need the `perform restores as self` right.
- To browse the catalog, you need the `browse backup catalogs with this access` right set to a value other than `none`.

The possible access values are `privileged`, `notdenied`, `permitted`, `named`, and `none`.

 **See Also:**

Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

["Displaying the Oracle Secure Backup Web Tool Home Page"](#)

2. Identify the backups to restore.

To identify the backups, first identify the volumes and [backup section](#) file numbers from which to restore the backups.

 **See Also:**

["Displaying Backup Sections"](#)

3. Create one or more restore requests.

 **See Also:**

["Creating a Raw Restore Request"](#)

 **Note:**

All restore requests that have not yet been sent to the [scheduler](#) persist until the background timeout expires. The background timeout value identifies the maximum idle time of certain `obtool` background processes. See *Oracle Secure Backup Installation and Configuration Guide* for more information about background timeout.

4. Optionally, delete the queued restore requests if necessary.

 **See Also:**

["Removing a Raw Restore Request"](#)

5. Send the restore requests to the Oracle Secure Backup scheduler so that the requests become jobs and are eligible to run.

The Oracle Secure Backup scheduler runs the jobs according to their priority.

 **See Also:**

["Sending Raw Restore Requests to the Scheduler"](#)

Removing a Raw Restore Request

This section explains how to remove a raw restore request that you have created, but have not yet sent to the scheduler.

To remove a raw restore request:

1. Follow the steps in "[Displaying the Directly From Media Page](#)".
2. On the Directly from Media page, select the request to remove.
3. Click **Remove**.

Oracle Secure Backup redisplay the page. The restore request that you selected no longer appears in the list.

Sending Raw Restore Requests to the Scheduler

This section explains how to send all pending raw restore requests to the scheduler.

To send raw restore requests to the scheduler:

1. Follow the steps in "[Displaying the Directly From Media Page](#)".
2. On the Directly from Media page, click **Go**.

The Oracle Secure Backup Web tool sends each restore request that appears in the Restore from Media list box to the scheduler. A message appears in the status area for each request acknowledged by the scheduler. For example:

```
raw restore request 1 submitted; job id is admin/7.
```

Oracle Secure Backup deletes each restore request upon its acceptance by the scheduler. As a result, the **Restore from Media** list is empty upon completion of the **Go** operation.

3. Display the transcript of the job to ensure that it completed successfully.

See Also:

["Displaying Job Transcripts"](#)

Part III

Managing Operations

This part explains how to manage backup containers and media and perform routine maintenance operations.

This part contains these chapters:

- [Managing Backups](#)
- [Managing Backup Containers](#)
- [Managing Backup and Restore Jobs](#)
- [Performing Maintenance](#)

7

Managing Backups

This chapter explains how to manage backup images and backup image instances.

This chapter contains the following sections:

- [Managing Backup Images](#)
- [Managing Backup Image Instances](#)

Managing Backup Images

A [backup image](#), created as a product of a backup operation, stores metadata related to the backup. As a part of managing backup images, you can view their properties and rename them.



See Also:

["Backup Images"](#) for more information about backup images

This section contains the following topics:

- [Displaying Backup Images](#)
- [Renaming Backup Images](#)

Displaying Backup Images

The Web tool enables you display existing [backup images](#) in the administrative domain. You must have the `list any backup`, regardless of its owner **OR** `list any backups owned by user` class right to display backup images.

To display the existing backup images:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Management section, click **Backup Images**.

The Manage: Backup Images page is displayed.

4. Use the **View Options** section to specify criteria that filter the backup images displayed on this page. You can specify one or more criteria.

The View Options section contains the following fields:

- Backup Image Attributes

Select **File system** to display only backup images of file-system backup operations. Select **Database** to display only backup images of Oracle Database backup operations. Select both options to display all backup images.

- **Container Type**
Select **Disk Pool** to display backup images stored on [disk pools](#). Select **Tape** to display backup images stored on tape devices. Select both options to display backup images stored on all storage media.
 - **Container Name**
Specify the name the [backup container](#). Only backup images stored on this container are displayed.
 - **Barcode**
Specify the barcode of the tape library. Only backup images stored on the library with the specified barcode reader are displayed.
 - **Filters**
Use the **Hosts** field to select the host that stores the backup images.

Select **Today** to display backup images that were created today. Select **From** and then select that to display backup images created after this date. Select **To** and specify a date to specify a date range, along with **From**, so that backup images created during the specified date range are displayed.
5. Click **Apply**.
- Oracle Secure Backup displays backup images that satisfy the specified criteria.

Renaming Backup Images

You must have the `modify any backup, regardless of its owner` or `modify any backups owned by user class` right to rename [backup images](#).

When you rename a backup image, Oracle Secure Backup renames all the backup image instances that are associated with this backup image to reflect the new name.

To rename backup images:

1. Display the required backup image as described in "[Displaying Backup Images](#)".
2. Select the backup image that to want to rename by clicking **Select** to the left of the backup image.
3. Click **Rename**.
4. In the **Rename *backup_image_name* to** field, enter the new name of the backup image and click **Yes**.

Managing Backup Image Instances

Backup image instances contain the backup data. Managing backup image instances includes creating, editing, deleting, and moving backup image instances.



See Also:

["Overview of Backup Images and Backup Image Instances"](#) for more information about backup image instances

This section contains the following topics:

- [Creating Backup Image Instances](#)
- [Displaying Backup Image Instances](#)
- [Editing Backup Image Instances](#)
- [Removing Backup Image Instances](#)

Creating Backup Image Instances

You can create a backup image instance, for a specific backup image, on a different [backup container](#). You must have the `modify any backup`, regardless of its owner or `modify any backups owned by user class` right to create [backup image instances](#).

To create a backup image instance:

1. Display the backup image for which you want to create a backup image instance as described in "[Displaying Backup Images](#)".
2. Click **Select** to the left of the backup image for which you want to create a backup image instance.
3. Select **Copy**.

The Manage: Backup Images > Copy page is displayed.

4. Provide details required to create the backup image instance.

The backup image instance details are specified using the following fields:

- **Media Family:** Select the media family for this backup image instance.
- **Restrictions:** Select the backup containers in which the backup image instance can be created. If you do not select a backup container, Oracle Secure Backup creates the backup image instance on any available backup container.
- **Encryption:** Specify the type of encryption to be used for the backup image instance. Select one of the following options:
 - **yes:** Specifies that the backup image instance must be encrypted.
 - **no:** Specifies that the backup image instance must not be encrypted. This is the default.
 - **forcedoff:** Specifies that backup image instances must not be encrypted regardless of global or client policy settings.
 - **transient:** Specifies that the backup image instance must be encrypted using a transient passphrase using the `--passphrase` or `--querypassphrase` option.

Also specify the following additional options:

Select **disable hardware encryption** to use hardware encryption while creating the backup image instance. This is applicable only for tape devices that support hardware encryption.

Select **Store key** to store the transient passphrase for this backup in the appropriate key stores.

- **Migrate:** Select this option to delete the existing backup image instance that is associated with the backup image after the new backup image instance is created.
- **Priority:** Specify the priority for this copy instance job.
- **Create Now:** Specifies that the backup image instance must be created immediately.

- **Create at:** Specifies that the backup image instance must be created at the specified date and time.
5. Click **OK**.

Displaying Backup Image Instances

You can use filters to specify the criteria that must be applied for displaying [backup image instances](#). You must have the `list any backup`, regardless of its owner or `list any backups owned by user class` right to display backup image instances.

To display backup image instances:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Advanced section, click **Backup Image Instances**.

The Manage: Backup Image Instances page is displayed.

4. In the **View Options** section, specify the criteria that will be used to filter and display the backup image instances.

The options in this section have the same meaning as those specified for backup images in Step 4 of "[Displaying Backup Images](#)".

5. Click **Apply** to display backup image instances that satisfy the specified criteria.

Editing Backup Image Instances

You must have the `modify any backup`, regardless of its owner or `modify any backups owned by user class` right to edit the properties of a [backup image instance](#). You can modify the expiry date or retention time of backup image instances that are stored on disk pools only.

To edit a backup image instance:

1. Display the required backup image instance as described in "[Displaying Backup Image Instances](#)".
2. From the list of backup image instances, click **Select** to the left of the backup image instance that you want to edit.
3. Click **Edit**.
4. Use one of the following options to modify when the selected backup image instance expires.
 - **Expire time:** Specifies the date and time at which the backup image instance expires.
 - **Retain time:** Enter a value and choose the unit of time to specify the amount of the time that the backup image instance must be retained.
5. Click **OK**.

Copying or Moving Backup Image Instances

Backup instances can be copied or moved (migrated) from a source container (such as a disk pool, tape volume, or cloud container) to a target container.

Keep in mind the following points with regard to containers in Oracle Cloud Infrastructure:

- Only encrypted backup instances that are contained in a disk pool can be copied or moved to an Oracle Cloud Infrastructure container.
- Backup instances contained in Oracle Cloud Infrastructure Object Storage Classic containers can be copied or moved to Oracle Cloud Infrastructure Archive Storage Classic containers.

Backup instances can be copied or moved using a scheduled automatic process or an on-demand manual process. Backup instances that are contained in a disk pool can be automatically copied or moved by using the `copyinstance` or `stagescan` staging commands.

When copying or moving a backup image instance, Oracle Secure Backup can compute a checksum for the backup image instance and store it along with the backup metadata. This checksum can subsequently be used to validate the backup image instance. Whether a checksum is computed depends on the device policies and the configuration of the device on which the backup image instance is stored.

See Also:

- [Staging](#) for more information about staging
- [Oracle Secure Backup Reference](#) for information about commands associated with staging
- [About Validating Backups by Computing Checksums](#)

Removing Backup Image Instances

You must have the `modify any backup`, regardless of its owner or `modify any backups owned by user class` right to remove [backup image instances](#). Removing a backup image instance from a particular backup container does not impact backup image instances of the same backup that may be stored in other backup containers. The other instances will continue to exist.

To remove a backup image instance:

1. Display the required backup image instance as described in "[Displaying Backup Image Instances](#)".

Use the filters to limit the number of backup image instances that are displayed. For example, to display expired backups, select **Expired** in the Filters section of the Manage: Backup Image Instances page.

2. From the list of backup image instances displayed, click **Select** to the left of the backup image instance that you want to remove.
3. Click **Remove** to remove the backup image instance.
A confirmation message is displayed asking you to confirm the delete operation.
4. Click **Yes** to confirm the deletion of the backup image instance.

8

Managing Backup Containers

This chapter explains how to manage tapes, tape devices, disk pools, and cloud storage devices with Oracle Secure Backup.

This chapter contains these sections:

- [Overview of Managing Backup Containers](#)
- [Managing Tape Drives](#)
- [Managing Tape Libraries](#)
- [Managing Disk Pools](#)
- [Managing Device Reservations](#)
- [Managing Cloud Storage Devices](#)

Overview of Managing Backup Containers

While configuring your administrative domain, you configure the [backup containers](#) that are attached to media servers as devices in the administrative domain. This includes tape devices and [disk pools](#). You can manage these configured backup containers by performing tasks such as mounting volumes in a tape drive, updating the library inventory, importing volumes, monitoring disk pool usage, reserving tape devices, and deleting expired [backup image instances](#) on disk pools.

See Also:

- ["Managing Tape Drives"](#)
- ["Managing Tape Libraries"](#)
- ["Managing Disk Pools"](#)
- ["Managing Device Reservations"](#)

Managing Tape Drives

This section describes how to display tape drive properties and mount or unmount a volume in a tape drive.

This section contains the following topics:

- [Displaying Tape Drive Properties](#)
- [Mounting a Volume in a Tape Drive](#)
- [Automatically Unloading Volumes](#)

Displaying Tape Drive Properties

This section explains how to display properties for a tape drive.

To view tape drive properties:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, under Devices, click **Libraries**.
4. On the Libraries page, select a tape drive in the Devices list.
5. Click **Show Properties**.

The Oracle Secure Backup Web tool displays a page with the properties for the tape drive you selected.

6. Click **Close** to return to the Libraries page.

Mounting a Volume in a Tape Drive

This section explains how to mount and unmount volumes in a [tape drive](#). A [volume](#) is a unit of media, such as the LTO5 tape drive. The [mount mode](#) indicates the way in which Oracle Secure Backup can use a volume physically loaded into a tape drive.

To mount or unmount a volume in a tape drive:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, click **Drives**.

The Tape Drives page appears. This page lists every [dataset file](#) and [dataset directory](#). You can use this page to mount and unmount volumes.

4. Select a tape drive from the drives list.

The Oracle Secure Backup [Web tool](#) displays the names of all tape drives that are attached to a [media server](#). A tape drive can have one of these status values:

- **In Service**
The tape drive is logically available to Oracle Secure Backup.
- **Not in Service**
The tape drive is not logically available to Oracle Secure Backup.
- **Unmounted**
The tape drive is unmounted.
- **Mounted**
The tape drive is mounted.

5. Choose a mount option from the **Mount options** provided.

These options let you logically mount a volume. When a volume is mounted, the `obscheduled` daemon is notified that a given volume is available for use. You can then set the mode of use for the volume.

The following mount options are available:

- **Read**
Specify this option to tell the [scheduler](#) to use this volume for reading only.
- **Write**
Specify this option to tell the scheduler that it can append any additional backups to the end of this volume.
- **Overwrite**
Specify this option to automatically mount a volume on the tape drive and position 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. An unexpired volume is not eligible to be overwritten according to its [expiration policy](#).

**Caution:**

Use this mode only in situations that warrant or require overwriting unexpired volumes.

6. From the **Mount and Unmount** options group, optionally choose one of these options:
 - **Unmount**
Select this option to perform an unmount operation on the selected tape drive before it attempts a requested mount operation.
 - **No rewind**
Select this option to specify that the tape is not rewound when Oracle Secure Backup finishes writing to it. Oracle Secure Backup remains in position to write the next [backup image](#).
7. Click **Mount** to mount the volume.
The Oracle Secure Backup Web tool displays the tape drive name and [volume ID](#) in the status area.
8. Click **Unmount** to unmount the volume.
When a volume is unmounted, the `obscheduled` daemon is notified that a given volume is no longer available for use.

**See Also:**

- *Oracle Secure Backup Reference* to learn about the `mountdev` and `unmountdev` commands in [obtool](#)
- "[Backup Image Instances and Volume Labels](#)" for details about volumes and volume IDs

Automatically Unloading Volumes

Oracle Secure Backup can automatically unload a volume from a tape drive when it has been idle for a set amount of time after a backup or restore operation. Automatic volume unloading has two main advantages:

- Continuous loading on a powered tape drive affects volume reliability.
- Because the `exportvol` command does not query loaded tape drives, idle volumes are never exported.

The amount of time the volume can be idle before being unloaded is controlled by the global policy `maxdriveidletime`. The default value is five minutes, but you can modify this to as little as zero seconds or as much as 24 hours. You can also set `maxdriveidletime` to `forever`, in which case the idle volume is never automatically unloaded.

See Also:

Oracle Secure Backup Reference for more information about the `maxdriveidletime` policy

A volume is automatically unloaded only after a backup or restore operation. If you manually load a volume into a tape drive, then it is not unloaded automatically.

When an unload operation completes successfully, Oracle Secure Backup writes a success message to the `observed` log. The success message includes the name of the tape drive from which the volume was unloaded. If a volume cannot be unloaded for some reason, then Oracle Secure Backup writes an error message to the `observed` log.

Managing Tape Libraries

This section explains how to view tape library properties and control [tape library](#) operations such as importing volumes into the library, labeling volumes, load volumes, and other such operations as described in [Table 8-1](#).

This section contains these topics:

- [Displaying the Libraries Page](#)
- [Displaying Library Properties](#)
- [Displaying Tape Drive Properties](#)
- [Displaying Library Volumes](#)
- [Running Library Commands](#)

Displaying the Libraries Page

To display the Libraries page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, under Devices, click **Libraries**.

The Libraries page appears as shown in [Figure 8-1](#). This page lists the tape libraries in your administrative domain. You can perform all tape library configuration tasks in this page or in pages to which it provides links.

Figure 8-1 Libraries Page

Displaying Library Properties

This section explains how to display properties for a tape library.

To view tape library properties:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library in the Devices list.
3. Click **Show Properties**.

The Oracle Secure Backup Web tool displays a page with the properties for the tape library you selected.

4. Click **Close** to return to the Libraries page.

Displaying Library Volumes

This section explains how to display a volume list for a tape library.

To display tape library volumes:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library in the Devices list.
3. Click **List Volumes**.

The Oracle Secure Backup Web tool displays a page with the volumes for the tape library you selected.

4. Click **Close** to return to the Libraries page.

Running Library Commands

You can use the Manage > Libraries page to list the tape libraries in your [administrative domain](#). You can perform all tape library configuration tasks in this page or in pages to which it provides links.

To manage a tape drive or tape library:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. In the Devices list, select a tape library or drive.
3. Choose one of the commands from the **Library commands** menu shown in [Table 8-1](#). The last column of the table indicates the corresponding command in the `obtool` command-line interface.

 **Note:**

Depending on the command, you must specify either a tape library or drive. For those commands that apply to libraries, however, you can optionally specify a tape drive, because specification of a tape drive always implies the tape library in which it resides.

Table 8-1 Library Commands

Menu Command	Applies to	Description	Section	obtool Command
Inventory	Library or Drive	Updates the current library inventory display and lets you force a physical inventory of the selected library.	"Updating an Inventory"	inventory
Import volume	Library or Drive	Moves one or more volumes from the import/export mechanism of a library to storage elements.	"Importing a Volume"	importvol
Export volume	Library or Drive	Moves one or more volumes to the import/export mechanism for removal from the library.	"Exporting a Volume"	exportvol
Insert Volume	Library or Drive	Notifies Oracle Secure Backup that you have manually inserted a volume in the library. You can specify the destination and the type of volume that you have inserted.	"Inserting a Volume"	insertvol
Extract Volume	Library or Drive	Notifies Oracle Secure Backup that you have manually removed a volume from the library. You can specify the source of the volume you are extracting.	"Extracting a Volume"	extractvol
Move Volume	Library or Drive	Moves a tape from an occupied storage element to a vacant storage element or import/export element. You can specify the location from which you are moving a tape and the location to which you are moving it.	"Moving a Volume"	movevol
Open Door	Library	Opens the import/export door of a tape library. This command only works for libraries that support it.	"Opening a Door"	opendoor
Close Door	Library	Closes the import/export door if the library. This command only works for libraries that support it.	"Closing a Door"	closedoor

Table 8-1 (Cont.) Library Commands

Menu Command	Applies to	Description	Section	obtool Command
Identify Volume	Drive	Loads selected volumes, reads their volume labels and returns the volumes to their original storage elements.	" Identifying a Volume "	identifyvol
Load Volume	Drive	Moves a volume from the indicated storage element to the selected drive.	" Loading a Volume "	loadvol
Unload Volume	Drive	Moves a tape from the selected drive to the storage element you specify.	" Unloading a Volume "	unloadvol
Label Volume	Drive	Loads selected volumes and physically labels them. Oracle Secure Backup updates its catalog and the inventory display	" Labeling a Volume "	labelvol
Unlabel Volume	Drive	Loads selected volumes and physically removes their Oracle Secure Backup volume labels and backup data.	" Unlabeling a Volume "	unlabelvol
Clean	Drive	Requests that a cleaning be performed on the selected tape drive.	" Cleaning a Tape Drive "	clean
Borrow	Drive	Borrows the selected drive.	" Borrowing a Tape Drive "	borrowdev
Return	Drive	Returns a currently borrowed drive.	" Returning a Tape Drive "	returndev
Reuse Volume	Drive	Loads selected volumes and relabels them to be reusable.	" Reusing a Volume "	reusevol

- Click **Apply** to accept your selections.

The Oracle Secure Backup Web tool displays a page with options specific to the command just specified. Refer to the relevant section for more information.

Updating an Inventory

This command updates the current tape library inventory and enables you to force a physical inventory of the selected tape library.

To update the inventory:

- Follow the steps in "[Displaying the Libraries Page](#)".
- On the Libraries page, select a tape library or tape drive in the Devices list.
- From the Library commands list, select **Inventory (Library | Drive)** and click **Apply**.
A different page appears.
- Optionally, select the **Force** option to force an inventory. Instead of reading from its cache, the tape library updates the inventory by physically scanning all tape library elements.
- Optionally, enter a range of storage elements to inventory in the **Storage element range** field. If no storage element range is specified, then all storage elements are included in the inventory update.

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.

- Click **Apply**, **OK**, or **Cancel**.

Importing a Volume

This command moves a [volume](#) from the import/export mechanism of a tape library to a [storage element](#).

To import a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.
3. From the **Library commands** list, select **Import Volume (Library | Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Options** group, select one of these options:
 - **Identify**
Select this option to read the first [volume label](#) on each volume. This option is equivalent to the operation described in "[Identifying a Volume](#)". This option requires specification of a tape drive.
 - **Import**
Select this option to read all backup image labels on each volume. You can use this option if you are importing volumes from another administrative domain or if you want information about what [backup section](#) is associated with each file number on the tape. This option requires specification of a tape drive.

Note that **Import** does not catalog the files stored on the volume.
 - **Unlabeled**
Select this option to make each imported volume unlabeled.
6. In the **IEE Range** field, enter a range of import/export elements containing the volumes to be imported.
7. Click **Apply**, **OK**, or **Cancel**.

 **Note:**

You cannot specify the Unlabeled option if the selected tape library has an enabled and functioning barcode reader. See *Oracle Secure Backup Reference* for more information.

Exporting a Volume

This command moves one or more volumes to the import/export mechanism for removal from the tape library.

To export a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.
3. From the **Library commands** list, select **Export Volume (Library | Drive)**.
4. Click **Apply** to accept your selection.

5. Specify the volumes to be exported in either of the following ways:
 - In the **Volume specification** field, enter the volume ID or barcode of each volumes you want to export.
 - In the **Storage element range** field, enter a storage element number or storage element range. For example, enter **1-20**.
6. Click **Apply**, **OK**, or **Cancel**.

Inserting a Volume

This command notifies Oracle Secure Backup that you have manually inserted volumes into the specified destinations in the tape library and specifies the properties of the inserted volumes.

To insert a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.
3. From the **Library commands** list, select **Insert Volume (Library | Drive)**.
4. Click **Apply** to accept your selection.
5. If you have inserted a volume with a known volume ID or barcode, then select one of these from the **Volume specification** group:
 - **Volume ID**
Enter the volume ID of the tape.
 - **Barcode**
Enter the barcode value of the tape.

 **Note:**

If you do not know the volume ID or the barcode of the volume, then leave this field blank and select **Unlabeled**, **Unknown**, or **Clean** in Step 6.

6. In the **Storage element** field, enter the storage element number for the inserted volume.
7. Select one of these options from the **Insert volume** options group:
 - **(vol-spec)**
Select this option if you specified a **Volume ID** or **Barcode** in the **Volume specification** (vol-spec) group.
 - **Unlabeled**
Select this option if the tape is unlabeled or a new volume.
 - **Unknown**
Select this option if the tape is of unknown format.
 - **Clean**
Select this option if the tape is a cleaning tape. Ensure that you inserted the cleaning tape into the destination storage element that you specified. Enter values for the following options:

- **Uses**
Enter the number of times you have used the cleaning tape.
- **Max uses**
Enter the maximum number of times you can use the cleaning tape.

 **Note:**

You cannot select the vol-spec or Unlabeled options if the selected library has an enabled and functioning barcode reader. See *Oracle Secure Backup Reference* for more information.

8. Click **Apply**, **OK**, or **Cancel**.

Extracting a Volume

This command notifies Oracle Secure Backup that you have manually removed a volume from the tape library. You specify the source of volumes you are extracting.

To extract a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.
3. From the **Library commands** list, select **Extract Volume (Library | Drive)**.
4. Click **Apply** to accept your selection.
5. Specify the volumes to be extracted in either of the following ways:
 - **Volume specification**
Select this option to specify the extracted volume by volume ID or barcode. Select one of these options:
 - **Volume ID**
Select this option and enter the volume ID of the tape you extracted.
 - **Barcode**
Select this option and enter the barcode value of the tape you extracted.
 - **Storage element range**
Select this option to specify a storage element range containing the extracted volumes. In the text field, enter a range of elements. For example, enter **1-20**.
6. Click **Apply**, **OK**, or **Cancel**.

Moving a Volume

This command moves a tape from an occupied storage element to a vacant one. For example, you could move a tape from storage element 1 to import/export element 2.

To move a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.

3. From the **Library commands** list, select **Move Volume (Library | Drive)**.
4. Click **Apply** to accept your selection.
5. Specify the volume to be moved in either of the following ways:
 - **Volume specification**

Select this option to specify the volume by volume ID or barcode. Select one of these options:

 - **Volume ID**

Enter the volume ID of the tape to be moved.
 - **Barcode**

Enter the barcode value of the tape to be moved.
 - **Element spec**

Select this option to specify the slot containing the volume to be moved. In the text field, enter a storage element number. For example, enter **1**.
6. In the **Element spec** field, enter the slot to which the volume should be moved. For example, enter **iee2**.
7. Click **Apply**, **OK**, or **Cancel**.

Opening a Door

This command opens the import/export door of a tape library.

To open the import/export door:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library in the Devices list.
3. From the **Library commands** list, select **Open Door (Library)**.
4. Click **Apply**, **OK**, or **Cancel**.

Closing a Door

This command closes the import/export door of a tape library.

To close the import/export door:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library in the Devices list.
3. From the **Library commands** list, select **Close Door (Library)**.
4. Click **Apply**, **OK**, or **Cancel**.

Identifying a Volume

This command loads selected volumes, reads each volume label, and returns the volumes to their original storage elements. You can use this command to verify the state of occupied tape library slots and update the tape library inventory accordingly.

To identify a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select the **Identify Volume (Drive)** option.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive to be used in the volume identification.
6. Select the **Import** option to read all backup image labels on each volume. You can use this option if you are importing volumes from another administrative domain or if you want information about what backup section is associated with each file number on the tape. This option requires specification of a tape drive.

Note that **Import** does not catalog the files stored on the volume.

7. In the **Storage element range** field, enter the storage element range for the volumes to be identified. For example, enter **1-20**.
8. Click **Apply**, **OK**, or **Cancel**.

Loading a Volume

This command moves a volume from the indicated storage element to the selected tape drive.

To load a volume into a tape drive:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Load Volume (Drive)**.
4. In the **Drive** list, select the tape drive to contain the loaded volume.
5. Click **Apply** to accept your selection.
6. Specify the volume to be loaded in either of the following ways:

- **Volume specification**

Select this option to specify the volume by volume ID or barcode. Select one of these options:

- **Volume ID**

Enter the volume ID of the tape to be loaded.

- **Barcode**

Enter the barcode value of the tape to be loaded.

- **Element spec**

Select this option to specify the slot containing the volume to be loaded. In the text field, enter a storage element number. For example, enter **1**.

7. From the **Load volume options** groups, optionally select one of these:

- **Mount (option)**

The mount mode indicates the way in which the scheduling system can use a volume physically loaded into a tape drive. Valid values are:

- **Read**

Select this option to tell the scheduler to use this volume for reading only.

– **Write**

Select this option to tell the scheduler that it can append any backups to the end of the volume.

– **Overwrite**

Select this option to automatically mount a volume on the tape device and position 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.

• **Load if Required**

Select this option to load the volume only if it is not loaded in the tape drive.

8. Click **Apply**, **OK**, or **Cancel**.

Unloading a Volume

This command moves a tape from the selected tape drive to the element you specify.

To unload a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Unload Volume (Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive that contains the loaded volume.
6. In the **Source element address** field, enter the element to which the volume should be moved. For example, enter **1**.
7. Click **Apply**, **OK**, or **Cancel**.

Labeling a Volume

This command loads selected volumes and writes a volume label for each volume. This command erases all existing data on the selected volumes.

To label a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Label Volume (Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive into which the volume should be loaded.
6. Optionally, select the **Force** option to force the labeling of a volume. Selecting this option overrides any conditions that would otherwise prevent the labeling operation to complete. This option enables you to overwrite unexpired volumes or to overwrite an incorrect manual entry for a barcode without the currently required prior step of unlabeled a volume.
7. Select the **Barcode** option and enter the barcode for the volume.

8. Enter a storage element range in the **Storage element range** field. For example, enter **1-3**.
9. Click **Apply**, **OK**, or **Cancel**.

Unlabeling a Volume

This command loads selected volumes and physically unlabels them.

To unlabel a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Unlabel Volume (Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive into which the volume should be loaded.
6. Click **Force** to ignore the expiration time on a time-managed volume and the deletion status of each contained [backup piece](#) on a content-managed volume. If you do not select **Force** and the volume is not expired, then the unlabeling operation fails.
7. In the **Storage element range** field, enter a storage element range. For example, enter **1-3**.
8. Click **Apply**, **OK**, or **Cancel**.

Cleaning a Tape Drive

This command lets you request that a manual cleaning be performed on a tape drive.

To clean a tape drive:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Clean (Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive into which the cleaning tape should be loaded.
6. Click **Force** to force the tape drive to be cleaned. If there is a tape loaded in the tape drive, then selecting 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.
7. In the **Source element address** field, enter an element address of a storage element containing a cleaning tape.
8. Click **Apply**, **OK**, or **Cancel**.

Borrowing a Tape Drive

This command enables you to borrow a tape drive. You must belong to a user [class](#) having the `manage devices` and `change device state` rights.

You can borrow a tape drive if a backup or restore operation is requesting assistance. Borrowing the tape drive temporarily overrides the tape device reservation made by the requesting job and enables you to run arbitrary tape library or tape drive commands. Afterwards, you can return the tape drive and resume the job.

To borrow a tape drive:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Borrow (Drive)**.
4. In the **Drive** list, select the tape drive to be borrowed.
5. Click **Apply**, **OK**, or **Cancel**.

Returning a Tape Drive

After a tape drive has been borrowed, you can return it.

To return a borrowed tape drive:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Return Device (Drive)**.
4. In the **Drive** list, select the tape drive to be returned.
5. Click **Apply**, **OK**, or **Cancel**.

Reusing a Volume

This command loads selected volumes and deletes every [backup image instance](#) on them. The volume attributes (volume ID, media family, and so on) are retained, but the contents of the volume are erased. Reusing a volume is similar to unlabeleding it, but reusing directs Oracle Secure Backup to preserve the existing volume label.

To reuse a volume:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape drive in the Devices list.
3. From the **Library commands** list, select **Reuse (Drive)**.
4. Click **Apply** to accept your selection.
5. In the **Drive** list, select the tape drive to be returned.
6. In the **Storage element range** field, enter a storage element range containing the volumes to be reused.
7. Click **Apply**, **OK**, or **Cancel**.

Displaying the Error Log

This section explains how to display error messages associated with a tape library or tape drive.

To display error messages:

1. Follow the steps in "[Displaying the Libraries Page](#)".
2. On the Libraries page, select a tape library or tape drive in the Devices list.
3. Select a tape library or tape drive from the **Library Management** list.

4. Click **Error Log**.

The Oracle Secure Backup Web tool displays a page with error messages displays for the tape library or tape drive you selected.

5. Optionally, select **Since (date)** and specify a date range for specific error messages.

6. Optionally, select **Read device dump file** and enter the filename and path of the file to read.

7. Choose one of these:

- Click **Apply** if you have either specified a date range or entered a filename.
- Click **Clear** to eliminate error history. New error messages appear from the time of the clear.
- Click **Close** to return to the Libraries page.

Managing Disk Pools

Managing disk pools includes performing tasks such as deleting expired [backup image instances](#), moving disk pools across domains, and monitoring space utilization.

This section contains the following topics:

- [Displaying Disk Pool Properties](#)
- [Monitoring Disk Pool Space Utilization](#)
- [Moving Disk Pools between Domains](#)
- [Moving Disk Pools to a New Hardware Within the Same Domain](#)
- [Moving Disk Pools to a New Hardware in a New Domain](#)
- [Deleting Expired Backup Image Instances from Disk Pools](#)

Displaying Disk Pool Properties

You must have the `query` and `display` information about devices right to display disk pool properties.

To display the properties of a disk pool:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Configure**.
The Configure page is displayed.
3. In the Basic section, click **Devices**.
The Configure: Devices page is displayed.
4. Select the disk pool whose properties you want to display and click **Show Properties**.
The Device Properties page displays the properties of the selected disk pool.

Monitoring Disk Pool Space Utilization

You can use the Web tool to view information about the space utilization and free space goal threshold of disk pools.

**See Also:**

"[Space Utilization in Disk Pools](#)" for more information about the free space goal threshold of disk pools

To monitor disk pool space usage:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Devices section, click **Disk Pools**.

The Manage: Disk Pools page is displayed. This page displays all the currently configured disk pools.

4. For each disk pool, the space utilization information is contained in the following fields:
 - **Status:** Displays the current status of the disk pool. Backup images instances can be written to the disk pool if the status is in service.
 - **Capacity:** Displays the space allocated to the disk pool.
 - **Consumption:** Displays the amount of space used by [backup image instances](#).
 - **Reclaimable Space:** Displays the amount of space that can be freed by deleting expired backup image instances from the disk pool.

Use this information to manage your disk pool. For example, if the Consumption for a disk pool is nearing its Capacity, you may want to create additional space in the disk pool by increasing its capacity or deleting some backup image instances that are no longer required.

Moving Disk Pools between Domains

Similar to tape, you can use the Web tool to move disk pools between existing domains. You can do this to manage storage space on your administrative domain.

To move a disk pool to a new domain:

1. From the Oracle Secure Backup Home page, select **Configure**.
The Oracle Secure Backup: Configure page appears.
2. On the Configure page, select **Devices**.
The Configure: Devices page appears.
3. Turn off all services for the concerned disk pool. Ensure that you let all pending jobs complete on this disk pool before performing this step.

To change the status of the disk pool, complete the following steps:

- a. Select the disk pool that you want to move to a different domain.
 - b. Click **Edit**.
 - c. Change the status of the disk pool to not in service.
 - d. Click **Apply**.
4. Remove this disk pool from its current domain.
To remove the disk pool from its existing domain, complete the following steps:

- a. Select the disk pool you want to move to a different domain.
 - b. Click **Remove**.
5. Add the disk pool in the new domain.
To add the disk pool in the new domain, complete the following steps:
 - a. Log on to the Web tool of the new domain.
 - b. On the home page, click **Configure**.
 - c. On the Configure page, click **Devices**.
 - d. On the Configure: Devices page, click **Add**.
 - e. Specify the properties of the disk pool. In the Attachments field, enter the path where the disk pool directory is located on this domain.
 - f. Click **Apply**.
6. Import the disk pool catalog by completing the steps in "[Importing and Cataloging Backups](#)".

Moving Disk Pools to a New Hardware Within the Same Domain

You can use the Web tool to move a disk pool to a new hardware within the same administrative domain.

To relocate a disk pool to a new hardware within the same domain:

1. From the Oracle Secure Backup Home page, select **Configure**.
The Oracle Secure Backup: Configure page appears.
2. On the Configure page, select **Devices**.
The Configure: Devices page appears.
3. Turn off all services for the concerned disk pool. Ensure that you let all pending jobs complete on this disk pool before performing this step.
To change the status of this disk pool, complete the following steps:
 - a. Select the disk pool that you want to move to a different hardware.
 - b. Click **Edit**.
 - c. Change the status of the disk pool to not in service.
 - d. Click **Apply**.
4. Copy the disk pool directory from its existing location, using the operating system copy command, to its new location. Ensure that hidden files and subdirectories are included in the copy.
For example, on Linux, use the `cp -a` (archive) command.
5. Remove this disk pool from its current location.
To remove the disk pool from its existing location, complete the following steps:
 - a. Select the disk pool you want to move to a new location.
 - b. Click **Remove**.
6. Add the disk pool at the new location.
To add the disk pool at the new location, complete the following steps:

- a. On the Web tool Home page, click **Configure**.
 - b. On the Configure page, click **Devices**.
 - c. On the Configure: Devices page, click **Add**.
 - d. Specify the properties of the disk pool. In the Attachments field, enter the path of the new location of the disk pool directory.
 - e. Click **Apply**.
7. Import the disk pool catalog by completing the steps in "[Importing and Cataloging Backups](#)".
 8. Optionally, you can remove the disk pool directory from its original hardware.

Moving Disk Pools to a New Hardware in a New Domain

You can use the Web tool to a disk pool to a new hardware in an entirely different administrative domain.

To move a disk pool to a new hardware in a new domain:

1. From the Oracle Secure Backup Home page, select **Configure**.
The Oracle Secure Backup: Configure page appears.
2. On the Configure page, select **Devices**.
The Configure: Devices page appears.
3. Turn off all services for the concerned disk pool. Ensure that you let all pending jobs complete on this disk pool before performing this step.
To change the status of this disk pool, complete the following steps:
 - a. Select the disk pool that you want to move to a different hardware
 - b. Click **Edit**.
 - c. Change the status of the disk pool to not in service.
 - d. Click **Apply**.
4. Copy the disk pool directory to the new hardware by using the operating system copy command. Ensure that hidden files and subdirectories are included in the copy.
For example, on Linux, use the `cp -a` (archive) command.
5. Remove this disk pool from its current hardware.
To remove the disk pool from its existing domain, complete the following steps:
 - a. Select the disk pool you want to move to a different hardware.
 - b. Click **Remove**.
6. Add the disk pool in the administrative domain of the new hardware.
To add the disk pool to the new hardware, complete the following steps:
 - a. Log on to the web tool of the domain of the new hardware.
 - b. Click **Configure**.
 - c. On the Configure page, click **Devices**.
 - d. On the Configure: Devices page, click **Add**.

- e. Specify the properties of the disk pool. In the Attachments field, enter the path where the disk pool directory is located on this hardware's administrative domain.
 - f. Click **Apply**.
7. Import the disk pool catalog by completing the steps in "[Importing and Cataloging Backups](#)".
 8. Remove the disk pool directory from the original hardware as the data no longer belongs to that domain.

Deleting Expired Backup Image Instances from Disk Pools

Oracle Secure Backup deletes backup image instances from disk pools through the process of proactive reclamation, which occurs daily at midnight. The disk pool manager attempts to delete expired backup image instances to reach the free space goal of the disk pool device. The expired backups are deleted from oldest to newest. When the space consumed by backup image instances exceeds the storage capacity of the disk pool, no new backups are scheduled to be copied to this disk pool. The administrator must make additional space available on this disk pool by deleting expired jobs or allocating additional space. Similarly, if the disk pool gets filled when a backup job is in progress, reactive reclamation occurs. This implies that if there is no available space on a disk pool during an ongoing backup or copy instance operation, the disk pool manager attempts to create more space in the disk pool. If this fails, then the administrator must allocate additional space to the disk pool, delete existing backup image instances, or abort the ongoing job.



See Also:

["Monitoring Disk Pool Space Utilization"](#)

You must have the `manage devices` and `change device state` right to delete expired [backup image instances](#) from the disk pool.

To delete expired backup image instances from a disk pool:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Devices section, click **Disk Pools**.

The Manage: Disk Pools page is displayed. This page displays all the configured disk pools and the following properties for each disk pool: Status, Capacity, Consumption, and Reclaimable Space.

4. Select the disk pool from which you want to delete expired backup image instances and then click **Delete Expired**.

A confirmation is displayed asking if you want to delete expired backups from the selected disk pool.

5. Click **Yes** to delete the expired backup image instances from the selected disk pool.

Managing Device Reservations

In normal operations, Oracle Secure Backup temporarily assigns exclusive use of shared resources to its processes and jobs. It does so using a built-in resource reservation system managed by the [service daemon](#) of the administrative server.

You might encounter certain situations in which you want exclusive and explicit use of a tape device. When such cases arise, you can direct Oracle Secure Backup to reserve a tape device for your use and, when you are finished, to release that reservation (unreserve it). While you hold the reservation, no Oracle Secure Backup component accesses the tape device.

To manage tape device reservations:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, click **Device Reservations**.

The Device Reservations page appears. This page lists tape devices that you can reserve. You can perform all tape device reservation tasks in this page or in pages to which it provides links.

4. To reserve a tape library or drive, select it in the Devices list and click **Reserve**.

The tape device is now reserved solely for your use. The reservation persists until you end your Oracle Secure Backup Web tool session or unreserve the tape device.

5. To unreserve a tape library or tape drive, select it in the Devices list and click **Unreserve**.

The tape devices reserved in this instance of the Oracle Secure Backup Web tool are now available for other activities.

6. To unreserve all currently reserved tape libraries and tape drives, click **Unreserve all**.

All tape devices reserved in this instance of the Oracle Secure Backup Web tool are now available for other activities.

Managing Cloud Storage Devices

Topics

- [Displaying Cloud Storage Device Properties](#)
- [Monitoring Cloud Storage Device Space Utilization](#)
- [Deleting Expired Backup Image Instances from Cloud Storage Devices](#)
- [Enabling Client Direct to Cloud](#)
- [Using Immutable Buckets of Oracle Cloud Infrastructure](#)

Displaying Cloud Storage Device Properties

You must have the `query` and `display` information about devices `right` to display the properties of cloud storage devices.

To display the properties of a cloud storage device:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. In the Web tool, click **Configure**.
The Configure page is displayed.
3. In the Basic section, click **Devices**.
The Configure: Devices page is displayed.
4. Select the cloud storage device whose properties you want to display and click **Show Properties**.
The Device Properties page displays the properties of the selected cloud storage device.

Monitoring Cloud Storage Device Space Utilization

You can use the Web tool to view information about the space utilization and free space goal threshold of cloud storage devices.

To monitor cloud storage space usage:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Devices section, click **Cloud Storage**.
The Manage: Cloud Storage page is displayed. This page displays all the currently configured cloud storage devices.
4. For each cloud storage device, the space utilization information is contained in the following fields:
 - **Status:** Displays the current status of the cloud storage device. Backup images instances can be written to the cloud storage device if the status is in service.
 - **Capacity:** Displays the space allocated to the cloud storage device.
 - **Consumption:** Displays the amount of space used by [backup image instances](#).
 - **Reclaimable Space:** Displays the amount of space that can be freed by deleting expired backup image instances from the cloud storage device.
 - **Number of objects:** shows the actual number of objects in a cloud container.
 - **Bytes used:** shows the bytes consumed in a cloud container. This value might differ from the value shown for **Consumption** because Oracle Secure Backup stores additional metadata that is not considered by all operating systems when reporting a value for **Consumption**.

Use this information to manage your cloud storage device. For example, if the **Consumption** for a cloud storage device is nearing its **Capacity**, you may want to create additional space by increasing its capacity or deleting some backup image instances that are no longer required.

Deleting Expired Backup Image Instances from Cloud Storage Devices

Oracle Secure Backup deletes backup image instances from cloud storage devices through the process of proactive reclamation, which occurs daily at midnight. The pool manager (`obpoolmgr` daemon) attempts to delete expired backup image instances to reach the free space goal of the cloud storage device. The expired backups are deleted from oldest to newest. When the space consumed by backup image instances exceeds the storage capacity of the cloud storage device, no new backups are scheduled to be copied to this cloud storage device. The administrator must make additional space available on this cloud storage device

by deleting expired jobs or allocating additional space. Similarly, if the cloud storage device gets filled when a backup job is in progress, reactive reclamation occurs. This implies that if there is no available space on a cloud storage device during on ongoing backup or copy instance operation, then the cloud storage device manager attempts to create more space in the cloud storage device. If this fails, then the administrator must allocate additional space to the cloud storage device, or delete existing backup image instances, or abort the ongoing job.

You must have the `manage devices` and `change device state` right to delete expired backup image instances from a cloud storage device.

To delete expired backup image instances from a cloud storage device:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. In the Web tool, click **Manage**.
3. In the Devices section, click **Cloud Storage**.

The Manage: Cloud Storage page is displayed. This page displays all the configured cloud storage devices and the following properties for each one: Status, Capacity, Consumption, and Reclaimable Space, Number of objects, and Bytes used .

4. Select the cloud storage device from which you want to delete expired backup image instances and then click **Delete Expired**.

A confirmation is displayed asking if you want to delete expired backups from the selected cloud storage device.

5. Click **Yes** to delete the expired backup image instances from the selected cloud storage device.

Enabling Client Direct to Cloud

The Client Direct to Cloud feature is in disabled state by default. You must configure the client host and the cloud storage device to enable this feature.

Note:

You must enable the Client Direct to Cloud feature at both the client host and the cloud storage device. If enabled at only one place, that is, the client or the cloud storage device, then this feature remains in disabled state.

Prerequisites

Before enabling the Client Direct to Cloud feature, check the following prerequisites.

- The client host has Oracle Secure Backup 19.1 software running on it.
- The client has connectivity to the cloud object storage to upload the backups directly. If a client resides within Oracle Cloud Infrastructure, then create a service gateway and configure the route table to send backup data through the service gateway.

 **Note:**

For more information, see [Creating a Service Gateway](#) in Oracle Cloud Infrastructure documentation.

- The client has sufficient memory to upload backups directly to cloud storage devices.

Before uploading to cloud storage, the client stores the backup data temporarily in memory. Hence, the client requires additional memory to perform these tasks. The calculation for additional memory required at the client host is as follows:

```
Additional memory required = segment size * (number of streams per job + 1)
```

Example

For the default segment size of 10 MB and streams per job value of 4, the additional memory required at each client can be computed as:

```
Additional memory required = 10 MB * (4 + 1) = 50 MB
```

 **Note:**

To use the Client Direct to Cloud feature on a client host, you must update the Cloud wallet on that client.

Port Requirements

For moving data through the client, ensure that the required ingress ports are open. It enables the client to receive catalog portion of the data from the administrative server before uploading to the cloud storage device.

 **Note:**

The ingress port is in addition to the standard ports required by Oracle Secure Backup, which are port 400 for `observed` and port 10000 for NDMP daemon.

A client opens one ingress port for each backup job. Consider the following scenarios:

- If the client runs one backup job, then it requires only a single ingress port.
- If the client runs 10 jobs concurrently, then the client must open 10 ingress ports.

However, a client can use the same port opened by another client. For example, a single backup job running for multiple clients in a domain uses the same port 11000.

Required IAM Policy

Oracle Secure Backup uses Pre-Authenticated Request (PAR) URLs for securely uploading and reading data from cloud object storage. For using PAR URLs, you require the `PAR_MANAGE` permission to the object storage bucket.

Moreover, you require additional permissions, such as `OBJECT_CREATE`, `OBJECT_DELETE`, `OBJECT_WRITE`, and `OBJECT_LIST` for the target buckets. These permissions are required for backup and restore operations even if `PAR` is not used.

Steps to Enable Client Direct to Cloud

You can enable this feature in Oracle Secure Backup:

- Using `obtool` commands from the command-line interface
- From the Web tool

Using `obtool` Commands

Log in to the `obtool` command-line interface and enable the Client Direct to Cloud feature for the client and the cloud storage device as follows:

1. Configure the client host.

You can enable the Client Direct to Cloud feature for a client host in the following scenarios.

- **For a new client host**

Run the `mkhost` command with the `--clientdirect` option. The value `yes` enables this feature for the client. If you do not specify the `--clientdirect` option, then this feature is disabled. For more information, see `mkhost`.

- **For an existing client host**

Run the `chhost` command with the `--clientdirect` option. Specify `yes` to enable or `no` to disable this feature. For more information, see `chhost`.

To view the current settings of a client, whether the feature is enabled or disabled, run the `lshost` command. For more information, see `lshost`.

2. Configure the cloud storage device.

You can enable the Client Direct to Cloud feature for a client host in the following scenarios.

- **For a new cloud storage device**

Run the `mkdev` command with the `--clientdirect` option. The value `yes` enables this feature for the cloud storage device. If you do not specify the `--clientdirect` option, then this feature is disabled. For more information, see `mkdev`.

- **For an existing cloud storage device**

Run the `chdev` command with the `--clientdirect` option. Specify `yes` to enable or `no` to disable this feature for the cloud device. For more information, see `chdev`.

To view the current settings of a cloud storage device, whether the feature is enabled or disabled, run the `lsdev` command. For more information, see `lsdev`.

From the Web tool

Follow the steps in [Displaying the Oracle Secure Backup Web Tool Home Page](#) to access the Web tool. Enable the Client Direct to Cloud feature for the client and the cloud storage device as follows.

1. Configure the client host.

Click the **Configure** menu at the top and select **Basic > Hosts** to open the Hosts page. The Hosts page displays information about your hosts, such as host name, roles, and status.

You can enable the Client Direct to Cloud feature for a client host in the following scenarios.

- **For a new client host**

Click **Add** and specify details of your client. The **Client direct** field determines whether the Client Direct to Cloud feature is enabled or not. The default value is *no*, which means the feature is disabled.

Select *yes* from the drop-down list to enable this feature for the client. Click **Ok** to create the client host.

You have enabled the Client Direct option for your new client.

- **For an existing client host**

Click the host name to select the host and then click **Edit** to view the current settings of a client host, whether the Client Direct to Client feature is enabled or disabled.

If the **Client direct** field is set as *no*, then select *yes* from the drop-down list to enable the Client Direct option for your client host. Click **Ok** to save your changes.

2. Configure the cloud storage device.

Click the **Configure** menu at the top and select **Basic > Devices** to open the Devices page. The Devices page displays information about your devices, such as device name, type, and status.

You can enable the Client Direct to Cloud feature for a cloud storage device in the following scenarios.

- **For a new cloud storage device**

Click **Add** and specify details of your new cloud device. Select the device **Type** as *cloudstorage*.

The **Client direct** field determines whether the Client Direct to Cloud feature is enabled or not. The default value is *no*, which means the feature is disabled.

Select *yes* from the drop-down list to enable this feature for the cloud device. Click **Ok** to create the cloud storage device.

You have enabled the Client Direct option for your new cloud storage device.

- **For an existing cloud storage device**

Click the device name to select a cloud device and then click **Edit** to modify the settings of your cloud device.

If the **Client direct** field is set as *no*, then select *yes* from the drop-down list to enable the Client Direct option for your cloud device. Click **Ok** to save your changes.

To view the current settings of a cloud storage device, whether the Client Direct to Cloud feature is enabled or disabled, on the Devices page click the device name to select a cloud device and then click **Show Properties**.

In the Device Properties window, verify the value of the **Client direct** field. Click **Close** to exit the Device Properties window.

Using Immutable Buckets of Oracle Cloud Infrastructure

The immutable feature is in disabled state by default. Configure the cloud storage device to enable this feature.

Prerequisites

You require the device configuration role to configure and manage the immutable feature in a cloud storage device.

Required IAM Policy

You require permissions to create and manage buckets in the object storage. Moreover, you require additional permissions, such as `BUCKET_UPDATE`, `RETENTION_RULE_MANAGE`, and `RETENTION_RULE_LOCK` to create and manage immutable retention rules for the target buckets.

Steps to Enable Immutable Bucket

You can enable the immutable feature in Oracle Secure Backup:

- For a new cloud storage device
- For an existing cloud storage device

For a New Cloud Storage Device

You can enable the immutable feature for a new cloud storage device using `obtool` commands and from the Web tool.

Using `obtool` commands

1. Log in to the `obtool` command-line interface.
2. Run the `mkdev` command with the following options:
 - `compliancecerule`: to specify the time duration for preserving a backup in cloud storage.
 - `legalhold`: to indicate any regulatory obligations.
 - `complianceclock`: to apply a lock on the compliance rule. The `complianceclock` option is only applicable with `compliancecerule`.

For more information, see `mkdev`.

From the Web tool

1. Follow the steps in [Displaying the Oracle Secure Backup Web Tool Home Page](#) to access the Web tool.
2. Click the **Configure** menu at the top and select **Basic > Devices** to open the Devices page. The Devices page displays information about your devices, such as device name, type, and status.
3. Click **Add** and specify details of your new cloud storage device. Select the device **Type** as *cloudstorage*.
4. Enter the duration for **Compliance rule**.

From the drop-down list which reads *disabled*, select the period in *days*, *weeks*, *months*, or *years*. The object storage restricts modification or deletion of backup in the bucket until this time period.

- Optionally, you can apply a lock on this rule for additional security. The default value for the **Lock** field is *no*, which indicates that the rule is not locked.

Select Yes for the **Lock** field to lock the rule.

- Indicate whether any **Legal hold** is applicable for the backup.

By default, the legal hold is not enabled. Select Yes to enable legal hold for the backup.

5. Click **Ok** to create the cloud storage device.

You have enabled the immutable feature for your new cloud storage device.

For an Existing Cloud Storage Device

You can enable the immutable options for an existing cloud storage device using `obtool` commands and from the Web tool.

Note:

When you enable the immutable feature on an existing cloud storage device, it applies to all objects in the bucket. You can modify or delete an object in an immutable bucket depending on the time period defined in the retention rule.

Using `obtool` commands

1. Log in to the `obtool` command-line interface.
2. Run the `chdev` command with the following options:
 - `compliancecerule`: to specify the time duration for preserving a backup in cloud storage.
 - `legalhold`: to indicate any regulatory obligations.
 - `complianceclock`: to apply a lock on the compliance rule. The `complianceclock` option is only applicable with `compliancecerule`.

For more information, see `chdev`.

From the Web tool

1. Follow the steps in [Displaying the Oracle Secure Backup Web Tool Home Page](#) to access the Web tool.
2. Click the **Configure** menu at the top and select **Basic > Devices** to open the Devices page.
3. Click the device name to select a cloud device and then click **Edit** to modify the settings of your cloud device.
4. Enter the **Duration** for **Compliance rule**.

From the drop-down list which reads *disabled*, select the period in *days*, *weeks*, *months*, or *years*. The object storage restricts modification or deletion of backup in the bucket until this time period.

- Optionally, you can apply a lock on this rule for additional security. The default value for the **Lock** field is *no*, which indicates that the rule is not locked.

Select Yes for the **Lock** field to lock the rule.

- Indicate whether any **Legal hold** is applicable for the backup.

By default, the legal hold is not enabled. Select Yes to enable legal hold for the backup.

5. Click **Ok** to modify the cloud storage device.

You have enabled the immutable feature for your existing cloud storage device.

To view the current settings of a cloud storage device, whether the immutable bucket feature is enabled or disabled, on the Devices page click a device name to select the cloud device and then click **Show Properties**.

In the Device Properties window, verify the values of the **Compliance rule** duration, **Legal hold**, and **Lock** fields. Click **Close** to exit the Device Properties window.

9

Managing Backup and Restore Jobs

This chapter describes how to manage backup and restore jobs. This includes viewing jobs, running jobs, viewing job properties and transcripts, editing jobs, and removing jobs.

This chapter consists of the following sections:

- [Overview of Managing Backup and Restore Jobs](#)
- [Displaying Jobs](#)
- [Displaying Job Properties](#)
- [Displaying Job Transcripts](#)
- [Removing a Job](#)
- [Running a Job](#)
- [Canceling a Job](#)

Overview of Managing Backup and Restore Jobs

A backup or restore request is distinct from a job. A request is not yet eligible to run. When you send a [file-system backup](#) or restore request to the Oracle Secure Backup [scheduler](#), the request becomes a job and is eligible to run.

This section describes Oracle Secure Backup jobs and how to manage them.

Displaying the Jobs Page

To display the Jobs page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)"
2. Click **Manage**.
3. On the Manage page, click **Jobs** to display the page shown in [Figure 9-1](#). You can perform all job-related tasks in this page or in pages to which it provides links.

The View Options section enables you shows only jobs of specific types, status values, and hosts. The central text box contains details for each [backup job](#), including the following information:

- Job ID, which specifies the Oracle Secure Backup-assigned job identifier
- Type, which specifies the type of job
- State, which specifies the job status: pending, completed, or failed

Figure 9-1 Jobs Page

You can also monitor and manage jobs from the Oracle Secure Backup Home page, which contains sections that show failed, active, pending, and completed jobs.



See Also:

Oracle Secure Backup Reference to learn about the job commands in [obtool](#)

Displaying Jobs

This section describes how to display information about Oracle Secure Backup jobs. If you are attempting to list another user's jobs, then you must have the right to list any job, regardless of its owner. If you are attempting to list your own jobs, then you must have the right to list any jobs owned by user.

To display jobs:

1. Follow the steps in "[Displaying the Jobs Page](#)".
2. In the Job Types section, select one or more of the following job display options:
 - **File system backup**
Select this option to display backup jobs for files in the file system, that is, backups other than database backups.
 - **File system restore**
Select this option to display restore jobs for files in the file system.
 - **Dataset**
Select this option to display the status of jobs in which a dataset is specified (see "[File-System Backup Types](#)" to learn about datasets).
 - **Oracle backup**
Select this option to view the status of database backup jobs.
 - **Oracle restore**
Select this option to view the status of database restore jobs.
 - **Scan control**
Select this option to display scan control jobs (see "[About Vaulting Scans](#)").
 - **Media movement**

Select this option to view the status of media movement jobs (see "[About Media Movement Jobs](#)").

- **Duplication**

Select this option to view the status of volume duplication jobs (see "[About Volume Duplication](#)").

- **Catalog Import**

Select this option to view the status of catalog import jobs.

- **Copy Instance**

Select this option to view the status of copy instance jobs.

Oracle Secure Backup displays jobs that match any of the selected properties. For example, selecting **File system backup** and **Oracle backup** shows all jobs that are either file system backup or RMAN backups.

3. In Job Status section, check one or more of the following job display options:

- **Active**

Select this option to display the status of each [backup job](#) currently in progress.

- **Failed**

Select this option to display the status of backup jobs that failed.

- **Complete**

Select this option to display the status of completed jobs, whether they succeeded or not.

- **Pending**

Select this option to view the status of jobs that are pending, but not presently running.

- **Input pending**

Select this option to view the status of jobs currently running and requesting input.

Oracle Secure Backup displays jobs that match any of the selected properties. For example, selecting **Active** and **Failed** shows all jobs that are either active or failed.

4. Optionally, further restrict the display of the jobs of the selected status and type.

In the Filters section, check one or more of the following job display options:

- In **Host**, optionally select a host to limit the jobs displayed to those pertinent to a specific host.

The default is **none**, which means that no hosts are excluded from the job list.

- In the **User** list, optionally select an [Oracle Secure Backup user](#) to limit the jobs displayed to those instantiated by the specified user.

The default is **none**, which means that no users are excluded from the job list.

- In the **Dataset** list, select a [dataset file](#) to limit the jobs displayed to a particular dataset file or directory.

The default is **none**, which means that no datasets are excluded from the job list.

- Do one of the following to display jobs scheduled within a time range:

- Select **Today** to show only jobs created today.

- Select the **From date** box and enter a date and time to show only jobs whose state was updated at or later than the indicated time.

- Select the **To date** box and enter a date and time to show only jobs whose state was updated at or before the indicated time.

The format for dates is *year/month/day.hour:minute[:second]*, for example, 2009/5/19.12:43.

Oracle Secure Backup displays jobs that match all of the selected properties. For example, selecting **Host** and **Today** lists jobs for the specified host that occurred today and are of the specified job status and type.

5. Click **Apply** to accept your selections.

The page refreshes to show jobs that meet the criteria you selected.

Displaying Job Properties

This section explains how to view job properties. Job properties include the type, level, family, scheduled time, and so on.

To display job properties:

1. Follow the steps in "[Displaying the Jobs Page](#)".
2. Select a job from the central text box.
3. Click the **Show Properties** button.

The Job Properties page appears as shown in [Figure 9-2](#).

Figure 9-2 Job Properties Page

Job Properties	
admin/6	
Type	dataset mydatasets1/test1.ds
Level	full
Family	(null)
Encryption	off
Scheduled time	11/20.13:00
Introduction time	2013/11/19.22:40
Earliest exec time	11/20.13:00
Last update time	2013/11/19.22:41
Expire time	never
State	future work
Priority	10
Privileged op	yes
Run on host	(administrative server)
Requires	any device
Attempts	0
Log	

Close

4. Click **Close** to return to the Jobs page.

Displaying Job Transcripts

This section explains how to view job transcripts. Oracle Secure Backup maintains a running transcript for each job. The transcript describes the details of the job's operation. To display a transcript, you must be a member of a [class](#) that has the `list any jobs owned by user` or `list any job, regardless of its owner` right.

 **See Also:**

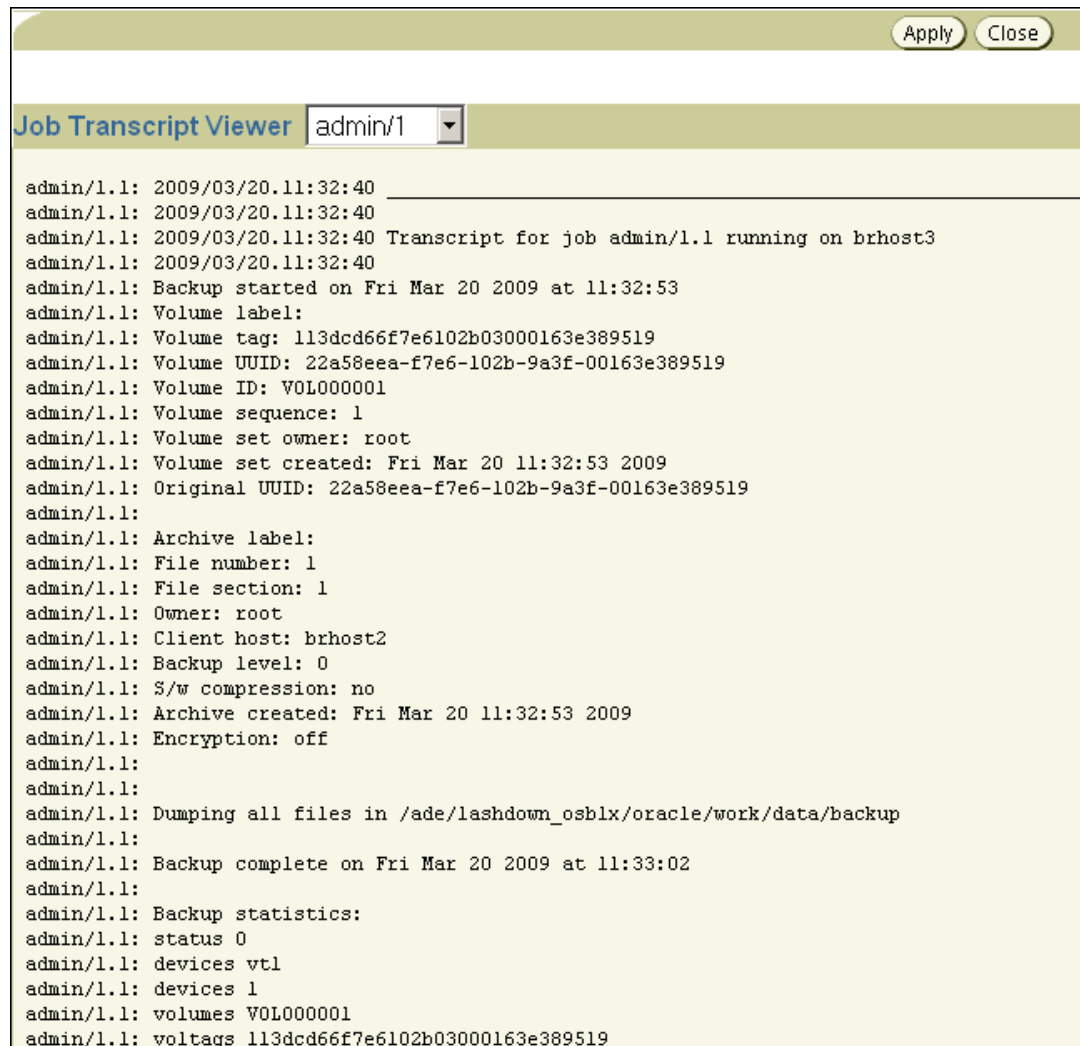
Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

To display a job transcript:

1. Follow the steps in "Displaying the Jobs Page".
2. Select a job and click **Show Transcript**.

The Oracle Secure Backup Web tool displays a page with the transcript.

Figure 9-3 shows a portion of a transcript for job `admin/1.1`.

Figure 9-3 Job Transcript


```

admin/1.1: 2009/03/20.11:32:40
admin/1.1: 2009/03/20.11:32:40
admin/1.1: 2009/03/20.11:32:40 Transcript for job admin/1.1 running on brhost3
admin/1.1: 2009/03/20.11:32:40
admin/1.1: Backup started on Fri Mar 20 2009 at 11:32:53
admin/1.1: Volume label:
admin/1.1: Volume tag: 113dcd66f7e6102b03000163e389519
admin/1.1: Volume UUID: 22a58eea-f7e6-102b-9a3f-00163e389519
admin/1.1: Volume ID: VOL000001
admin/1.1: Volume sequence: 1
admin/1.1: Volume set owner: root
admin/1.1: Volume set created: Fri Mar 20 11:32:53 2009
admin/1.1: Original UUID: 22a58eea-f7e6-102b-9a3f-00163e389519
admin/1.1:
admin/1.1: Archive label:
admin/1.1: File number: 1
admin/1.1: File section: 1
admin/1.1: Owner: root
admin/1.1: Client host: brhost2
admin/1.1: Backup level: 0
admin/1.1: S/w compression: no
admin/1.1: Archive created: Fri Mar 20 11:32:53 2009
admin/1.1: Encryption: off
admin/1.1:
admin/1.1:
admin/1.1: Dumping all files in /ade/lashdown_osb1x/oracle/work/data/backup
admin/1.1:
admin/1.1: Backup complete on Fri Mar 20 2009 at 11:33:02
admin/1.1:
admin/1.1: Backup statistics:
admin/1.1: status 0
admin/1.1: devices vtl
admin/1.1: devices 1
admin/1.1: volumes VOL000001
admin/1.1: voltags 113dcd66f7e6102b03000163e389519

```

3. Scroll down the page to view more information.
At the end of the page, you can modify the transcript viewing criteria.
4. In the **Level** list, optionally select a message level.

Oracle Secure Backup tags each message it writes to a transcript with a severity level. These levels range from 0 to 9. The severity level describes the importance of the message.

When displaying a transcript, you can direct Oracle Secure Backup to display only messages of a certain severity level or higher. Its default level is 4 (Request), meaning normal messages produced by Oracle Secure Backup. Refer to the `catxcr` command description in *Oracle Secure Backup Reference* for more information.

5. Optionally, check **Suppress input** to suppress input requests. When a request for input is recognized, Oracle Secure Backup prompts for a response. Specifying this option suppresses this action.
6. Optionally, check **Show line numbers** to prefix each line with its message number.
7. Optionally, select one of these options to control the transcript display:
 - **Start at line**
Select this option and enter a number with which you want the transcript view to start. For example, if you enter '10,' then the view starts with message 10. Message 1 through 9 are not displayed.
 - **Head lines**
Select this option and enter a number to display the first specified number of lines of the transcript having a message severity level at or higher than the value you selected.
 - **Tail lines**
Select this option and enter a number to display the last specified number lines of the transcript having a message severity level at or higher than the value you selected.
8. In the **Page refresh (in seconds)** box, optionally enter a value in seconds. The default is 60 seconds.
9. Choose one of these:
 - Click **Apply** to apply your selections.
 - Click **Close** to close the page.

Backup Statistics

The transcript for a backup job contains the statistics shown in [Table 9-1](#).

Table 9-1 Job Transcript Backup Statistics

Statistic	Description
status	Overall status of backup. See <code>samples/obexit.h</code> in your Oracle Secure Backup home directory for more information about status codes
devices	Name(s) of tape drive(s) or disk pool(s) used during the backup
devices	Number of tape drives or disk pools used
volumes	Volume ID(s) used during the backup
voltags	Volume tags (barcodes) used during the backup
file	File number
host	Name of client host

Table 9-1 (Cont.) Job Transcript Backup Statistics

Statistic	Description
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>
start_time	Time at which backup started
end_time	Time at which backup completed
backup_time	Time at which backup started. This is normally the same as <code>start_time</code> . It might differ if an archive is being read, in which case the <code>backup_time</code> comes from the archive label.
entries_scanned	Number of file-system entries scanned
kbytes_scanned	Number of file-system kilobytes scanned
entries_excluded	Number of file-system entries excluded, either because the file matches an exclusion statement in the dataset or it is an Oracle file that is being excluded
entries_skipped	<p>Number of file-system entries skipped, either because the file was not modified sufficiently recently during an incremental backup or because the file is an obfuscated wallet.</p> <p>An obfuscated wallet (<code>cwallet.sso</code> file) is only backed up when the backup is encrypted or when the <code>cwallet.sso</code> file is explicitly included in the dataset.</p>
mount_points_skipped	Number of file-system entries that were skipped because they were mount points, either local or remote, and <code>obtar</code> was told to skip that mount point type
files	Number of files scanned
directories	Number of directories scanned
hardlinks	Number of hard links scanned
symlinks	Number of symbolic (soft) links scanned
sparse_files	Number of files that were discovered to be sparse. A sparse file is a file that has areas that do not correspond to any valid data.
filesystems_errors	Number of file-system errors encountered
unknown_type	Number of files of unknown type that were encountered
file_kbytes	Total kilobytes of file-system data written to tape
dev_kbytes	Total kilobytes of data written to tape
dev_iosecs	Total seconds that the tape drive was open, beginning with the <code>open()</code> operation and ending with the <code>close()</code> operation

Table 9-1 (Cont.) Job Transcript Backup Statistics

Statistic	Description
<code>dev_iorate</code>	Rate at which data was written to tape
<code>wrt_iosecs</code>	Total seconds during which data was being written to tape. This excludes time spent on such activities as positioning the tape and reading labels.
<code>wrt_iorate</code>	Rate at which data was written to tape during write operations
<code>physical_blks_written</code>	Number of physical blocks written, as reported by the tape drive
<code>write_errors</code>	Number of physical blocks that encountered unrecoverable write errors and therefore had to be rewritten to tape
<code>physical_blks_read</code>	Number of physical blocks read, as reported by the tape drive
<code>read_errors</code>	Number of physical blocks that encountered unrecoverable read errors and therefore had to be reread from tape
<code>error_rate</code>	The sum of read errors and write errors divided by the sum of total blocks read and total blocks written
<code>path path_name</code>	Final status of the backup of the path <i>path_name</i> . There are separate entries for each path named in the dataset.

 **Note:**

Both `dev_iorate` and `wrt_iorate` are calculated using the same amount of data written, but the elapsed times used in the calculations are different. Because `dev_iosecs` is typically larger than `wrt_iosecs`, `dev_iorate` is typically less than `wrt_iorate`.

Removing a Job

This section explains how to remove a job. Removing a job has the effect of canceling it and deleting all record of its, and its subordinates, existence. You can remove a job only if it is not running. After removing a job, you can no longer view its status.

 **Note:**

As explained in "[Canceling a Job](#)", you can cancel a job and retain its history and transcript.

To remove a job:

1. Follow the steps in "[Displaying the Jobs Page](#)".
2. Select a job from the central text box.
3. Click **Remove**.

The Oracle Secure Backup Web tool prompts you to confirm the job removal.

4. Click **Yes** to remove the job.

Running a Job

This section explains how to direct Oracle Secure Backup to run a job at other than the scheduled time or priority, or using a specific backup container. To use this function, you must be a member of a class that has the `modify any jobs owned by user` or the `modify any job`, regardless of its owner right enabled.



See Also:

Oracle Secure Backup Reference for more information about Oracle Secure Backup rights

You can direct Oracle Secure Backup to start a job:

- Immediately
- In an order different from that chosen by the scheduler
- On a specific tape device or a tape device from which the job was previously restricted

To alter when Oracle Secure Backup runs a job:

1. Follow the steps in "[Displaying the Jobs Page](#)".
2. Select a job from the central text box.
3. Click **Run**.
4. In **Devices**, optionally select a tape device on which to run the job.

If the job was restricted to another tape device or set of tape devices, then your selection here overrides that restriction. Note that if you select **Now** in the next step, then you must choose a tape device.

5. Optionally select one of these options:
 - **Now**
Select this option to run the job immediately. If the preceding tape device you selected is not currently available, then Oracle Secure Backup displays an error and this operation has no effect.
 - **ASAP**
Select this option to run the job as soon as possible by lowering it to priority 1.
 - **Job Priority**
Select this option and enter a job priority in the Priority box. The default priority is 100.

The priority for a job is a positive numeric value. The lower the value, the greater the priority assigned to the job by the scheduler. For example, priority 20 jobs are higher priority than priority 100 jobs. The scheduler dispatches higher priority jobs over lower priority ones, providing all resources required to run the job are available.
6. Do one of the following:
 - Click **Apply** to accept your changes and remain in the page.
 - Click **Cancel** to void the operation and move back one page.

Canceling a Job

This section explains how to cancel a job. Canceling a job aborts the job if it is running, then marks its job record as "canceled." Oracle Secure Backup considers canceled jobs as no longer runnable. If you cancel a job that has subordinates, then each of its subordinate jobs is also canceled.

To cancel a job:

1. Follow the steps in "[Displaying the Jobs Page](#)".
2. Select a job from the central text box.
3. Click **Cancel**.

10

Performing Maintenance

This chapter describes how to perform maintenance tasks with Oracle Secure Backup. Oracle Secure Backup task maintenance includes managing volumes and volume properties, importing and maintaining cataloged backups, and monitoring checkpoints and daemons.

This chapter contains these sections:

- [Managing Volumes](#)
- [Managing Catalog Imports](#)
- [Managing Checkpoints](#)
- [Managing Daemons](#)

Managing Volumes

Volumes are the media on which backup data is stored. This section describes how to display information about a [volume](#).

This section includes these topics:

- [Displaying the Manage: Volumes Page](#)
- [Displaying Volume Details](#)
- [Displaying Backup Sections](#)
- [Changing Volume Properties](#)
- [Duplicating Volumes](#)
- [Recalling and Releasing Volumes](#)
- [Removing Volumes](#)

Displaying the Manage: Volumes Page

You can use the Manage: Volumes page to list the volumes in the volumes catalog.

To display information from the volumes catalog:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Home page, click **Manage**.
The Manage page appears.
3. In the Management section, click **Volumes**.
The Manage: Volumes page appears as shown in [Figure 10-1](#).

Figure 10-1 Manage Volumes Page

The screenshot shows the 'Manage_Volumes' page. At the top, there's a 'View Options' section with an 'Apply' button. Below it are 'Volume Attributes' with checkboxes for 'Unexpired volumes', 'Expired volumes', 'Open volumes', 'Closed volumes', 'Volumes with no barcodes', 'Volumes with no volume IDs', and 'Recyclable volumes'. There's a 'Single Selection' section with input fields for 'Volume ID', 'Barcode', 'Locations' (dropdown set to 'Media_Recycle_Bin'), and 'Media family' (dropdown set to 'OSB-CATALOG-MF'). Below that is an 'Other' section with a checkbox for 'Group volume set members'. A row of action buttons includes 'Edit', 'Duplicate', 'Recall', 'Release', 'Show Backup Sections', and 'Remove'. Below this is another row of buttons: 'Show Properties', 'Show Backup Pieces', 'Show Volume Set', and 'Show Duplicates'. A table with columns: 'Select', 'Volume ID', 'Barcode', 'Seq', 'Rotation policy', 'Duplication Policy', 'Location', 'Media family', 'Created', 'Expires', 'Space', and 'Status'. The table has one row with '(empty)' in the 'Volume ID' column. At the bottom right of the table are buttons: 'Edit', 'Duplicate', 'Recall', 'Release', 'Show Backup Sections', and 'Remove'.

Note:

The Manage: Volumes page does not contain information about volumes that have been loaded into a tape library but have not yet been written to. To list unlabeled volumes in a specified [tape library](#), go to the Libraries page described in "[Running Library Commands](#)" and click **List Volumes**.

By default, the Manage: Volumes page displays the following information about all volumes in the volumes catalog:

- Volume ID
- Sequence
- Rotation policy
- Duplication policy
- Location
- Media family
- Creation date
- Expiration date
- Space available
- Barcode

Note:

The rotation policy, duplication policy, and location fields contain information only if you have set up a vaulting environment. For more information about vaulting, see [Vaulting](#).

If the Oracle Secure Backup volumes catalog contains more volumes than fit on the Manage: Volumes page, then you can scroll through the volumes listing. Alternatively, you can click **Prev** or **Next** to view information for other volumes.

4. In **View Options**, select a filtering method for the volume display.

Choose either of the following mutually exclusive filtering methods:

- In **Volume Attributes**, optionally select one or more attributes to restrict the display of volumes and click **Apply**:
 - **Unexpired volumes**

Select this option to display volumes that have not yet expired.
 - **Expired volumes**

Select this option to display volumes that have expired, either because they have passed their expiration dates or because they are content-managed.
 - **Open volumes**

This is a default viewing option. If you deselect it without selecting another viewing option and click **Apply**, then Oracle Secure Backup automatically selects it again.
 - **Closed volumes**

Select this option to display volumes that are closed.
 - **Volumes with no barcodes**

Select this option to display volumes with no tags.
 - **Volumes with no volume IDs**

Select this option to display volumes with no volume IDs.
 - **Recyclable volumes**

Select this option to display all volumes that can be recycled.

Oracle Secure Backup displays jobs that match *any* of the selected properties. For example, selecting **Open volumes** and **Volumes with no barcodes** shows all volumes that are either open or lack barcodes.

- In **Single Selection**, select any *one* of the following options and click **Apply**:
 - **Volume ID**

Enter a volume ID in this field to limit the Manage: Volumes list to the matching volume.
 - **Volume set ID**

Enter a volume set ID in this field to limit the Manage: Volumes list to volumes in the matching volume set.
 - **Barcode**

Enter a barcode in this field to limit the Manage: Volumes list to the matching volume.
 - **Locations**

Select a location from the Locations list to limit the Manage: Volumes list to volumes at the selected location.

You can select multiple locations by shift-clicking. The default value is None, which results in the display of volumes at all locations. See [Vaulting](#) for more information about locations.
 - **Media family**

Select a media family from the Media family list to limit the Manage: Volumes list to volumes in the selected media family. You can select multiple media families by shift-clicking.

The default value is None, which results in the display of volumes belonging to all media families.

For example, selecting a media family shows only volumes in the selected media family. You cannot combine the single-selection options with each other or with a volume attribute. For example, you cannot combine open volumes and media family to produce a listing of volumes that are open and in the specified media family.

5. Optionally, select **Group volume set members** to group the filtered volumes by volume set.

Displaying Volume Details

This section describes how to display additional information about volumes managed by Oracle Secure Backup.

To display volume details:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. In the **Select** column, select the volume or volumes for which you want additional information.

Selected volumes show a check mark in the **Select** column.

3. Perform any of the following action to display volume details:
 - Click **Show Properties** to display the properties of the selected volume or volumes. The Volume(s) Properties page appears.
 - Click **Show Backup Pieces** to display information about backup pieces contained in the selected volume or volumes.
 - Click **Show Duplicates** to display information about duplicates of the selected volume or volumes.
 - Click **Show Volume Set** to display information about the volume set to which the selected volume or volumes belong.

Displaying Backup Sections

This section describes how to display information about backup sections contained in volumes listed on the Oracle Secure Backup Web tool Manage: Volumes page:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. In the list of volumes, select the volume or volumes whose backup sections you want to display.
3. Click **Show Backup Sections**.

The Manage: Volumes > Backup Sections page appears as shown in [Figure 10-2](#).

Figure 10-2 Manage Backup Sections

Manage: Volumes > Backup Sections

Remove OK

Show Properties

Select All Clear

Select	OID	Containing Volume	Containing Volume OID	File	Section	Backup level	Client	Encryption	Created	Size
<input type="checkbox"/>	106	RMAN-DEFAULT-000002	1	1	0	brhost1	off	2009/03/20.17:27	2.9 MB	
<input type="checkbox"/>	108	RMAN-DEFAULT-000002	2	1	0	brhost1	off	2009/03/20.17:29	2.9 MB	

This page displays the following information for each selected backup piece:

- Backup section OID
- Containing volume
- Containing volume OID
- File
- Section
- Backup level
- Client
- Encryption
- Created
- Size

See Also:

["Backup Image Instances and Backup Sections"](#)

- To display additional information for a backup section, specify the section by clicking its **Select** option and then click **Show Properties**.
- To remove a backup section, specify the section by clicking its **Select** option and then click **Remove**.

A confirmation page appears. Click **Yes** to remove the backup section or **No** to return to the Manage: Volumes > Backup Sections page.

When you remove a backup section from the Manage: Volumes page, Oracle Secure Backup does not physically remove the section from the volume, but updates the [catalog](#) to indicate that the [backup section](#) has been removed. Typically, you remove a backup section only when the catalog requires manual update. This action is meaningful only for content-managed volumes. When all sections are deleted from a content-managed volume, Oracle Secure Backup considers the volume eligible for overwriting.

 **Note:**

If you remove a backup section that contains an RMAN [backup piece](#), then Oracle Secure Backup responds to RMAN queries concerning the backup piece by saying that it does not exist.

6. When you are finished with the Manage: Volumes > Backup Sections page, click **OK** to return to the Manage: Volumes page.

Changing Volume Properties

You can use the Web tool to change volume attributes, including the rotation policy applied to the volume and its current location. You must have the `modify administrative domain's configuration right` to use the modify volume properties.

To change the properties of a volume:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. In the list of volumes, select the volume or volumes whose properties you want to edit.
3. Click **Edit**.

The Manage: Volume > Edit page appears.

4. Oracle Secure Backup allows users to change the expiration date of time-managed volumes. This change applies to all volumes within a volume set.

To change the expiration date of a volume, choose one of the following mutually exclusive techniques:

- Select **Expire date** and enter a new expiration date in the adjacent list.
The new expiration date cannot be earlier than the current expiration date.
- Select **Retain**, enter a value in the adjacent field, and select a unit of measure from the adjacent list.

By increasing the retain time of the volume, you change the expiration date. The retain time uses the creation date of the volume to calculate the new expiration date.

 **Note:**

You cannot specify a different expiration date when selecting a different location, duplication policy, or rotation policy. See [Vaulting](#) for more information.

5. Select **Set new duplication policy** and a duplication policy from the adjacent list to set a different duplication policy for the volume.
6. Select **Set new rotation policy** and a rotation policy from the adjacent list to set a different rotation policy for the volume.
7. Select **Set new location** and a different location from the adjacent list to set a different location for the volume.

Optionally, select one of the following options:

- Select **Override rotation policy** to set a location different from the location specified by the current rotation policy for the specified volume.

This option does not create a media movement job.

- Select **Do not create movement job** to set a different location without creating a corresponding media movement job.
8. Select the **Not in transit** option for a volume that is now in a tape library but was formerly designated as in transit from a remote location.

This option cannot be specified when selecting a different location or rotation policy.

9. In **Missing Attribute**, do one of the following:
- Select **Yes** for a volume that is not currently in the location specified by its rotation policy.
 - Select **No** for a volume that was previously designated as missing but which is now in its expected location.

When you select a different location or rotation policy.

10. Select **Set Volume Status** to set the availability status of the volume for use.

Select one of the following:

- Select **Usable** to make the volume available for use to store backups.
- Select **Read Only** to make the only volume information available.
- Select **Out Of Service** to disable the volume.

11. Do one of the following to process your changes:

- Click **OK** to make the specified changes and return to the Manage: Volumes page.
- Click **Cancel** to return to the Manage: Volumes page without changing any volume properties.
- Click **reset** to reset all options on the page.

Duplicating Volumes

You can use Oracle Secure Backup to duplicate a volume on demand.

To duplicate a volume:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. Select the volume to duplicate in the list of volumes and click **Duplicate**.

The Manage: Volumes > Duplicate page appears.

Select a media family for the duplicate volume in the **Media family** list. The media family of the duplicate volume can be different from the media family of the original volume.

3. Restrict the duplication job to a specified tape device by selecting it in the **Device Restrictions** list.

You can specify multiple tape devices by shift-clicking.

4. Select the **Migrate** option if you want the duplicate to replace the original.
5. Specify a priority for the duplication job in the **Priority** field.

The default priority is 100.

6. Click **OK** to submit the duplication job and return to the Manage: Volumes page.
7. Click **Cancel** to return to the Manage: Volumes page without duplicating the selected volume.

You can also duplicate volumes automatically according to one or more duplication schedules. See [Vaulting](#) for more information.

 **Note:**

To duplicate a volume that contains an archive from a transient hardware encrypted backup, you must perform the original transient encrypted backup while storing the transient passphrase.

 **See Also:**

For more information on hardware transient encryption, see [About Hardware-Encrypted Transient Backups](#)

For more information on performing a backup with the `-storekey` option, see the `backup` command in the *Oracle Secure Backup Reference*

Recalling and Releasing Volumes

When a restore operation requires a volume that is stored at a remote storage location, the volume must be recalled. When the restore operation is complete, the volume can be released back to its remote storage location. This section explains how to recall and release a volume from the Manage: Volumes page.

 **See Also:**

[Vaulting](#) for more information about recalling and releasing volumes

To recall a volume:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. Select the volume or volumes to be recalled and click **Recall**.
The Manage: Volumes > Recall page appears.
3. Select a location destination for the recall in the **Relocate all volumes to location** field.
4. Optionally select **Recall immediately**.
If the Recall immediately option is not selected, then Oracle Secure Backup creates a media movement job in a pending state. This job does not run until an Oracle Secure Backup operator explicitly runs it.
5. Click **OK** to recall the volume or volumes and return to the Manage: Volumes page.
The Manage: Volumes page displays a success message, and the recalled volume appears in the list with its changed location. Oracle Secure Backup has created an active or pending media movement job to move the recalled volume to its changed location.

 **See Also:**

["Running Media Movement Jobs"](#)

6. Click **Cancel** to return to the Manage: Volumes page without recalling the selected volume or volumes.

To release a recalled volume:

1. Select the volume or volumes to be recalled and click **Release**.
2. The Manage: Volumes page displays a success message, and the released volume appears in the list at its original location. Oracle Secure Backup has created a pending media movement job to move the recalled volume back to its original location.

 **See Also:**

["Running Media Movement Jobs"](#)

Removing Volumes

You can use the Web tool 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. You must have the `modify catalog` right to remove volumes from the catalog.

To remove a volume or volumes from the Oracle Secure Backup volumes catalog:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. Select the volume or volumes to be removed in the list of volumes and click **Remove**.
The Manage Volumes: Remove page appears.
3. Select the location from which the volume is to be removed from the **Locations** list.
4. Optionally, select **Force**.

By default, you can only remove the records of expired volumes. You can specify the Force option to override this restriction and remove the records of unexpired volumes as well.

5. Click **OK** to remove the selected volume and return to the Manage: Volumes page.
6. Click **Cancel** to return to the Manage: Volumes page without removing the selected volume.

 **Note:**

The only way to undo the removal is to import the volume again, so that the Oracle Secure Backup catalog is repopulated.

The following section displays the task information for feature 27301, catalog on tape.

Managing Catalog Imports

You can use the [import catalog](#) function to import database backups and file-system backups from disk pools or tape volumes into your Oracle Secure Backup domain. Once you import these backups, you can browse and select them for restore.

This section contains the following topics:

- [Displaying the Catalog Imports Page](#)
- [Importing and Cataloging Backups](#)

Displaying the Catalog Imports Page

You can use the Manage: Catalog Imports page to select backups that you need to import from disk or tape.

To view and select information on the Catalog Imports page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. On the Oracle Secure Backup Home page, click **Manage**.
3. Under the Advanced section, click **Catalog Imports**.

The Manage: Catalog Imports page appears.

[Figure 10-3](#) displays the **Catalog Imports** page on the Oracle Secure Backup Web tool.

Figure 10-3 Catalog Imports Page

Home Configure **Manage** Backup Restore

Manage: Catalog Imports

Go

Priority 100

Import from Disk none

Import from Tape Volume ID VOL000001

Barcode

Tape drive vt1 Begin import starting with the first full image on the tape

Force import (catalogs from available volumes(s) in a set - use when missing one or more volumes)

Fast import (imports metadata associated with existing backup images only)

Importing and Cataloging Backups

This section describes how to perform the [import catalog](#) function from disk and tape.

See Also:

"[About Importing Backup Catalog Data from Tape](#)" for more information about importing and cataloging data

To import and catalog backups using the Oracle Secure Backup Web tool:

1. Follow the steps in "[Displaying the Manage: Volumes Page](#)".
2. Enter a value in the **Priority** field.

The lower the value, the greater the priority assigned to the [import catalog](#) job. The default priority is 100. Priority 1 is the highest priority that you can assign.

3. To import catalog from disk, specify the necessary options.

 **See Also:**

"[Importing Backup Catalog Data from Disk](#)" for information on how to import backup metadata from disk

4. To import catalog from tape, specify the required options.

 **See Also:**

"[Importing Backup Catalog Data from Tape](#)" for information on how to import backup metadata from tape

5. Click **Go**.

Importing Backup Catalog Data from Disk

This section describes how to import backup metadata from disk.

To import catalog data from disk:

1. Select the **Import from Disk** option.
2. Select the configured disk on your domain from the list of disk pools.

Importing Backup Catalog Data from Tape

This section describes how to import backup metadata from tape.

To import catalog data from tape:

1. Select the **Import from Tape** option.
2. Optionally, enter one of the following backup details:
 - Enter the volume id of the backup in the **Volume ID** field.
 - Enter the barcode of the backup in the **Barcode** field.
3. Select a tape drive from the **Tape drive** list.

The selected tape drive must contain the stored backup.
4. Select **Begin import starting with the first full image on the tape** to start importing from the backup image that contains the first backup section.
5. Select **Force import** to start importing from the first available volume.

6. Select **Fast import** to start importing backup images that contain the associated [backup catalog data](#).

Managing Checkpoints

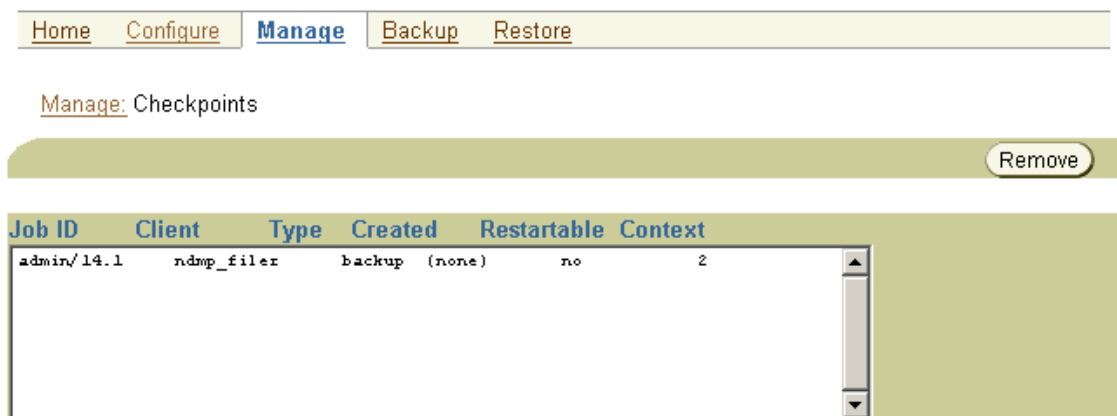
You can restart some [filer](#) backups from a midpoint if they fail before completing. A checkpoint is a collection of state information that describes a specific midpoint in a backup job and how to restart from it. Some information for each checkpoint resides on the [administrative server](#); the remainder resides on the [client](#).

Displaying the Checkpoints Page

To display the Checkpoints page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, click **Checkpoints** to display the page shown in [Figure 10-4](#). This page displays all checkpoints for hosts in the administrative domain.

Figure 10-4 Manage Checkpoints Page



Job ID	Client	Type	Created	Restartable	Context
admin/14.1	ndmp_filer	backup	(none)	no	2



See Also:

Oracle Secure Backup Reference to learn about the checkpoint commands in `obtool`

Removing a Checkpoint

Although normally not required, you can manually remove checkpoint data for any job. This action has the effect of reclaiming disk space as follows:

- On the administrative server immediately
- On the client at the start of the next backup job, or within 24 hours, whichever occurs first

 **Note:**

If you remove a checkpoint for an incomplete backup job, then the job restarts from its beginning if it fails before completing.

To remove a checkpoint:

1. Follow the steps in "[Displaying the Checkpoints Page](#)".
2. In the main box, select the job whose checkpoint you want to remove.
3. Click **Remove**.
A confirmation page appears.
4. Click **Yes** to confirm the deletion.
The Status area displays the result of the operation.

Managing Daemons

Daemons are background processes that perform Oracle Secure Backup operations. This section explains how to view the status of and manage Oracle Secure Backup [daemons](#).

 **See Also:**

["About Oracle Secure Backup Daemons"](#)

This section contains these topics:

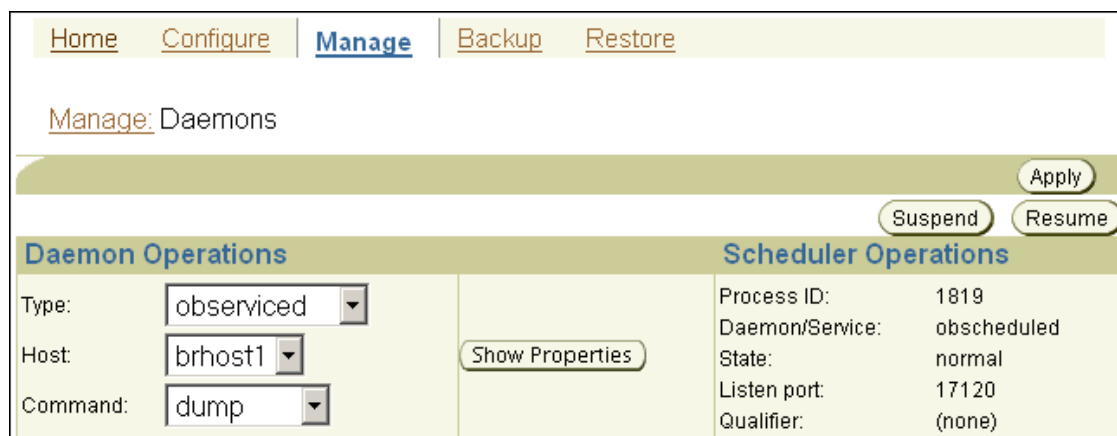
- [Displaying the Daemons Page](#)
- [Performing Daemon Operations](#)
- [Viewing Daemon Properties](#)
- [Suspending and Resuming Job Dispatching](#)

Displaying the Daemons Page

To display the Daemons page:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. Click **Manage**.
3. On the Manage page, click **Daemons** to display the page shown in [Figure 10-5](#). This page enables you to manage the Oracle Secure Backup daemons.

Figure 10-5 Daemons Page



Daemon Operations		Scheduler Operations	
Type:	observed	Process ID:	1819
Host:	brhost1	Daemon/Service:	obscheduled
Command:	dump	State:	normal
		Listen port:	17120
		Qualifier:	(none)

 **See Also:**

Oracle Secure Backup Reference to learn about the daemon commands in `obtool`

Performing Daemon Operations

Oracle Secure Backup daemons respond to a common set of control commands. Sending these commands is rarely needed and is considered advanced usage.

 **See Also:**

["About Oracle Secure Backup Daemons"](#)

To send a command to a daemon:

1. Follow the steps in ["Displaying the Daemons Page"](#).
2. In the **Type** list, select the daemon to control.
3. In the **Host** list, select the host on which the daemon runs.
4. In the **Command** list, select one of these options:
 - **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 information to its log file.
 - **debugoff**
Cancels debugon. This is the default state.

5. Click **Apply** to accept your selections.

A Success or Error message displays the result of the operation.

Viewing Daemon Properties

This section explains how to view daemon properties.



See Also:

["About Oracle Secure Backup Daemons"](#)

To view daemon properties:

1. Follow the steps in "[Displaying the Daemons Page](#)".
2. In the **Type** list, select the daemon to control.
3. In the **Host** list, select the host on which the daemon runs.
4. Click the **Show Properties** button.

The Daemon Properties page displays the following information:

- **Process ID**
Specifies an integer number assigned by the operating system identifying the process in which the daemon is running.
- **Daemon/Service**
Specifies the name of the daemon.
- **Qualifier**
Specifies a text string that augments the daemon/service name. For example, for `obrobotd`, this is the name of the tape library that the daemon is servicing. For `obixd`, this is the name of the client on whose behalf `obixd` is running.
- **Listen port**
Specifies the TCP port number on which the daemon or service is listening.

Suspending and Resuming Job Dispatching

This section explains how to temporarily suspend and later resume Oracle Secure Backup's dispatching of jobs. When job dispatching is suspended, running jobs are allowed to complete, but the scheduler starts no additional jobs.

The scheduler resumes job dispatching for suspended jobs when you click **Resume** or restart Oracle Secure Backup on the administrative server.



See Also:

["Displaying the Daemons Page"](#)

To suspend job dispatching:

- Click **Suspend** button on the Daemon Operations page.

In the Status area, a confirmation displays the result of the operation.

Any pending backup and restore (scheduled or one-time) are no longer dispatched. Jobs that are running are permitted to finish.

To resume job dispatching:

- Click **Resume** on the Daemon Operations page.

In the Status area, a confirmation displays the result of the operation.

Part IV

Advanced Topics

This part contains these chapters:

- [Vaulting](#)
- [Managing Backup Encryption](#)
- [Disaster Recovery of Oracle Secure Backup Administrative Data](#)
- [Staging](#)

11

Vaulting

This chapter describes vaulting and explains how to use an Oracle Secure Backup volume [rotation policy](#) to track a backup [volume](#) as it moves from its [originating location](#) to a [storage location](#) and is eventually recycled. It also explains how to set up and use automatic volume duplication, which can enhance both the security and convenience of a vaulting environment.

Volume rotation policies and automatic volume duplication are optional and independent. You can enable both simultaneously, either by itself, or neither. You can also enable either of them for some volumes, leaving the movement or duplication of other volumes unmanaged by Oracle Secure Backup.

This chapter contains the following sections:

- [Overview of Vaulting](#)
- [Setting Up a Vaulting Environment](#)
- [Tracking Volumes Through a Vaulting Environment](#)
- [Managing an Existing Vaulting Environment](#)
- [Recovery Manager and Vaulting](#)
- [Troubleshooting Vaulting](#)

Overview of Vaulting

This section discusses Oracle Secure Backup vaulting concepts. For step-by-step instructions on setting up a vaulting environment for the first time, see "[Setting Up a Vaulting Environment](#)".

This section contains these topics:

- [About Locations](#)
- [About Rotation Policies](#)
- [About Vaulting Scans](#)
- [About Media Movement Jobs](#)
- [About Reports](#)
- [About The Vaulting Process](#)
- [About Volume Duplication](#)
- [About Volume Duplication Policies](#)
- [About Volume Duplication Schedules](#)
- [About Volume Duplication Jobs](#)
- [About Volume Duplication Widows](#)
- [About NDMP Copy-Enabled Virtual Tape Library](#)

About Locations

A [location](#) is a physical place where a volume can reside. Oracle Secure Backup vaulting enables you to organize your volumes as they move from location to location. Oracle Secure Backup recognizes the following location types:

- Active locations

An [active location](#) is the starting point of a rotation. They are tape libraries and standalone tape drives, where volumes are either being written to or reside in storage elements. They are part of your Oracle Secure Backup [administrative domain](#) and are created when you configure your tape libraries and standalone tape drives during the Oracle Secure Backup installation process.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for more information about configuring tape devices

- Storage locations

These are places you put volumes when they are not being written to. Oracle Secure Backup creates a default storage location called the `Media_Recycle_Bin` that you can use for volumes at the end of their rotation cycle. You can create as many additional storage locations as you want. Examples include fireproof closets, offsite data warehouses, and third-party storage vendors such as Iron Mountain.

About Rotation Policies

You organize the movement of volumes from location to location by creating rotation policies. A rotation policy defines:

- The starting point for a volume rotation, which must be an active location
- All locations the volume can be moved to
- The order of movement among locations
- The length of time a volume is required to stay at each location before it is eligible to move to its next location
- The event from which that length of time is measured

Each volume has its own rotation policy, which it inherits from its media family.

An example of a simple rotation policy is as follows:

- A volume in a library is eligible to be moved one week after it was last written to.
The library, an active location, is the starting point for the rotation. Its *duration* at this location is one week past the last-write *event*.
- The next location the volume moves to is a storage closet.
Oracle Secure Backup knows about the storage closet, because you have configured it following the procedure in "[Adding Locations](#)".
- The volume is eligible to be moved out of the storage closet one day after it has expired.
Its *duration* in the storage closet is one day past the expiration *event*.

- The volume then is moved to the media recycle bin.

About Vaulting Scans

After you have created both active and storage locations, you can specify the days and times that Oracle Secure Backup performs vaulting scans. During a vaulting scan, Oracle Secure Backup searches its catalog for volumes eligible to be moved. If it finds one or more eligible volumes at a location, then it creates a media movement job for all eligible volumes at that location. A vaulting scan can scan one or more locations.

Setting up vaulting scans is a necessary part of creating a vaulting environment. If no vaulting scans exist, then Oracle Secure Backup creates no media movement jobs, which means that rotation policies are not enforced.

You want to schedule the vaulting scans to finish shortly before the times you have set aside for media movement jobs because the jobs are based on volume events and durations at the time of the scans. If there is a long lag between vaulting scans and media movement jobs, then media movement is based on stale data.

About Media Movement Jobs

A media movement job is created whenever one or more volumes at a location are eligible to be moved. Only one media movement job is created for each location with volumes eligible to be moved. Media movement includes changing the location of a volume or recalling a volume. A media movement job can move volumes into or out of both active and storage locations.

The media movement jobs resulting from vaulting scans are not run automatically. They are created in a pending state and require action by an operator to run. You can override this behavior with the `vaulting/autorunmmjobs` policy.



See Also:

Oracle Secure Backup Reference to learn about the `autorunmmjobs` policy

About Reports

Oracle Secure Backup produces several reports to assist you in the movement of volumes from location to location.

This section contains these topics:

- [Location Report](#)
- [Schedule Report](#)
- [Pick Report](#)
- [Distribution Report](#)
- [Exception Report](#)
- [Missing Volumes Report](#)

Location Report

A location report displays a list of volumes at a particular location, ordered by volume ID. For each volume listed, it shows the next location it is expected to move to and the date that the volume is eligible to be moved to that next location. The next location and eligibility move date come from the rotation policy in effect for that volume. For volumes that are not associated with any rotation policy, the next location and move date fields display *n/a*. Missing volumes are excluded from this location report.

For content-managed volumes associated with an expiration event rotation policy, a specific Move Date cannot be provided until the volume expires. Until the volume expires, the location report will display the following text in the Move Date column: Volume not expired, not eligible to be moved

If a volume has been flagged as *in-transit* by the media movement job that processes volumes eligible to be moved out of a storage location, then that volume shows the move date as *in-transit since date-volume-was-marked-in-transit*. You can limit the location report to *in-transit* volumes only, as in the following example:

```
ob> catrpt -t location -L vault -intransit
                                Location: vault
-----
Volume ID      Next Location      Move Date
mf1-000001    library_1          in-transit since 2008/02/01.9:00
mf3-000001    library_2          in-transit since 2008/02/01.9:00
```

This location report shows that volumes `mf1-000001` and `mf3-000001` are *in-transit* from location `vault` to location `library_1` and `library_2` respectively.



See Also:

- ["Missing Volumes Report"](#)
- *Oracle Secure Backup Reference* for full syntax and semantics for the `catrpt` command

Schedule Report

A schedule report contains the same information as a location report, but it is limited to volumes whose move-eligibility dates fall within a range that you specify.

Pick Report

The pick report is created and emailed (if email IDs have been configured) when the media movement job is created and scheduled. The pick report lists all volumes to be picked for distribution to another location and the customer ID (if any) that was assigned to the next location. You can think of the pick report as a shopping list used to gather the volumes from a tape library or storage location to box and ship to their next location.

Distribution Report

Oracle Secure Backup creates a distribution report at the end of a media movement job. Unlike the pick report, it lists only the volumes that were actually ejected during that job. If a volume

ejection fails during the media movement job for any reason, then that volume is not listed in the distribution report even though it might appear in the pick report created at the beginning of the media movement job.

The distribution report lists all volumes being sent to a particular location as the result of a media movement job and the customer ID (if any) that was assigned to the next location. You can think of the distribution report as a packing list to be included in the shipment of volumes to a location.

Exception Report

This report shows the current and expected locations for all volumes whose current and expected locations are different. If a volume is recalled from a storage location back into a tape library, for example, then that volume appears in the exception report for that tape library.

Missing Volumes Report

You can generate on-demand missing volume reports for one or more specific locations with the `catrpt` command in `obtool`. If no locations are specified, then the missing volumes report is generated for all locations. The following examples show the outputs of two `catrpt` commands. The first specifies the `vault` location, and the second applies to all locations:

```
ob> catrpt -t missing -L vault
```

Volume ID	Last location	Expected location	Missing since
mf1-000001	vault	library_1	2008/12/01.12:21
mf3-000001	vault	library_2	2008/12/01.12:21

```
ob> catrpt -t missing
```

Volume ID	Last location	Expected location	Missing since
mf1-000001	vault	library_1	2008/12/01.12:21
mf3-000001	vault	library_2	2008/12/01.12:21
mf4-000001	ironmtn	library_1	2008/12/01.12:21



See Also:

Oracle Secure Backup Reference for full syntax and semantics for the `catrpt` command

About The Vaulting Process

After you have set up storage locations, rotation policies, and vaulting scan schedules, managing the movement of your volumes through their respective life cycles becomes routine. At intervals defined by the vaulting scan schedule, Oracle Secure Backup performs the following actions:

- Scans its catalog
- Identifies volumes eligible to move to their respective next locations
- Creates a media movement job for each location having at least one move-eligible volume
- Creates pick and distribution reports to facilitate the movement of volumes from existing to different locations

The operator manually performs the following tasks:

- Running the media movement jobs
- Extracting volumes from their present active or storage locations with the help of pick reports
- Packing the volumes with their distribution reports
- Transporting volumes to their locations

For a greater margin of safety for your backup data, or to use different media families for on-site backups and off-site storage, combine the Oracle Secure Backup vaulting process with automatic volume duplication.

About Volume Duplication

Volume duplication can safeguard critical data. For example, multiple copies of a volume stored in different geographic locations protect against data loss from a site disaster. One copy could be shipped to a secure storage facility for long-term storage, while another is kept at the data center for ready access. In a restore operation, Oracle Secure Backup can intelligently select the volume that can be retrieved most quickly.

The contents of the original and duplicate volumes are the same. If the original volume is compressed, then the duplicate volume is also compressed. Each original or duplicate volume has a unique object identifier, referred to as `VOID` in `lsvol` output, and also shows the object identifier of the originating volume, referred to as `OOID` in `lsvol` output. The `VOID` and `OOID` of original volumes are identical. If the `VOID` and `OOID` of a volume are not identical, then that volume is a duplicate volume made from the volume whose object identifier is `OOID`.

The [write window](#) for a duplicate volume is always closed. This makes the duplicate volume read only. The duplicate volume can be reused only if it has expired, you forcibly unlabel the volume, or you rewrite the volume label. The write window of the original volume is closed after the first duplicate is created. This prevents writing to the original volume and maintains the integrity of the duplicate volume.

Oracle Secure Backup always tries to use the original volume for a restore operation. If the original volume is not available because it has been destroyed or is in an offsite location, for example, and a duplicate volume is in an active location, then Oracle Secure Backup automatically uses the duplicate volume for the restore operation.



See Also:

Oracle Secure Backup Reference for more information about the `lsvol` command

About Volume Duplication Policies

A volume duplication policy specifies the number of duplicate volumes to be created, the [media family](#) to be used for the duplication (which can be different from the media family of the original volume), and the [trigger](#) that makes a volume eligible for duplication. It can also specify that the duplicate volume is to replace the original volume. This is referred to as volume migration.

Volumes are associated with a duplication policy through their media families. A media family can have only one duplication policy.

About Volume Duplication Schedules

A volume duplication schedule determines where and when volume duplication is scheduled, what priority the volume duplication job has, and how long Oracle Secure Backup waits before expiring a duplication job that has not run.

Scheduling volume duplication is similar to scheduling a vaulting scan. Oracle Secure Backup scans its catalog to determine which volumes are eligible for duplication, according to the duplication policies of their respective media families. If Oracle Secure Backup finds a volume eligible for duplication, then it creates a volume duplication job for that volume. Volume duplication jobs are performed automatically during a volume duplication window.

About Volume Duplication Jobs

When a volume duplication job is scheduled to run within a duplication window, the Oracle Secure Backup scheduler reserves the required resources and dispatches the job to a media server.

If a resource restriction has been specified for the volume duplication job, then the scheduler picks up the specified resources for running the job. If no restriction has been specified, then the scheduler tries to pick up the best set of tape devices to be used for the duplication. The scheduler initially looks for tape devices attached to the same media server. If tape devices are available on the same media server, then the volume duplication job runs on that media server.

If the volume to be duplicated resides in an NDMP copy-enabled virtual tape library (VTL) and you have included the `mkdev --class vtl` option when creating its Oracle Secure Backup library object, then Oracle Secure Backup gives preference to the physical library or libraries connected to the VTL.

The duplicated volume retains the encryption state of each backup section on the original volume. Therefore, an encrypted section on the original volume is also encrypted on the duplicated volume. If the volume to be duplicated was hardware-encrypted, then Oracle Secure Backup attempts to mount a tape capable of hardware-based encryption. If no such volume is found, then the job goes into a pending state and requires input from the backup operator.

 **Note:**

An original volume can be duplicated only to another volume whose capacity at least equals the capacity of the original volume.

You can also run on-demand volume duplication jobs with the `dupvol` command in `obtool`.

 **See Also:**

- ["About NDMP Copy-Enabled Virtual Tape Library"](#)
- *Oracle Secure Backup Reference* for complete syntax and semantics for the `mkdev` command in `obtool`
- *Oracle Secure Backup Reference* for complete `dupvol` syntax and semantics

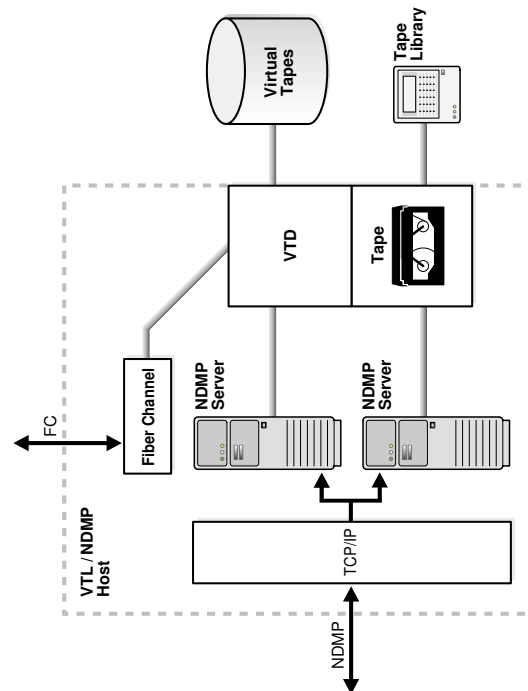
About Volume Duplication Widows

A volume duplication window is the interval during which Oracle Secure Backup schedules duplication jobs to run. Oracle Secure Backup automatically generates a daily volume duplication window that begins at 10:00 and ends at 20:00.

About NDMP Copy-Enabled Virtual Tape Library

An NDMP copy-enabled virtual tape library (VTL) is a [virtual tape library](#) with an embedded [NDMP](#) server and multiple access paths. The embedded NDMP server allows offloading the I/O associated with volume duplication from the application running on the media server to the VTL. [Figure 11-1](#) shows a typical physical layout.

Figure 11-1 Typical NDMP Copy-Enabled VTL



A traditional SCSI or Fibre Channel (FC) interface provides a direct access path from a media server to the virtual library and its drives. An embedded NDMP server provides network access to the virtual library and its drives. The NDMP server also provides network access to the physical library and drives attached to the VTL/NDMP host. The physical library is connected to the virtual library with a Fibre Channel path.

The SCSI/FC direct access path to a virtual drive is typically used for backing up data on the attached media server, because it can provide more bandwidth than a network connection.

The physical drive in the illustration is accessible only by way of the NDMP access path, because it is connected directly to the VTL. Another common arrangement is a physical library connected to a shared storage area network.



See Also:

["NDMP Volume Duplication"](#)

Setting Up a Vaulting Environment

This section contains step-by-step instructions for configuring a vaulting environment.

This section contains these topics:

- [Adding Locations](#)
- [Adding Rotation Policies](#)
- [Associating Rotation Policies with Media Families](#)
- [Adding a Vaulting Scan Schedule](#)
- [Performing an On-Demand Vaulting Scan](#)
- [Running Media Movement Jobs](#)
- [Viewing Location Reports](#)
- [Recalling a Volume](#)
- [Releasing a Volume](#)
- [Viewing Pick and Distribution Reports](#)
- [Adding Volume Duplication Policies](#)
- [Associating Volume Duplication Policies with Media Families](#)
- [Adding Volume Duplication Windows](#)
- [Adding Volume Duplication Schedules](#)
- [Running Volume Duplication Jobs](#)
- [On-Demand Volume Duplication](#)
- [Exporting Duplicate Volumes to Another Domain](#)
- [NDMP Volume Duplication](#)

Adding Locations

During the media life cycle, a volume can be located in an active location, such as a tape library, or in a storage location, such as an on-site storage room. Oracle Secure Backup automatically stores information about each active location in its administrative domain.

Storage locations represent any place outside of tape libraries or tape drives that a volume can be while being managed by Oracle Secure Backup. Oracle Secure Backup does not automatically gather information about storage locations. You must supply this information using the Web tool or `obtool` location commands.

 **See Also:**

Oracle Secure Backup Reference for complete syntax and semantics of `obtool` location commands

To add a storage location:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Media Life Cycle section, click **Locations**.

The Configure: Locations page appears.

This page lists active locations corresponding to tape libraries and tape drives in your administrative domain. The page also lists a storage location called `Media_Recycle_Bin` generated by Oracle Secure Backup.

4. Click **Add**.

The Configure: Locations > New Locations page appears.

5. Enter a name for the storage location in the **Location** field.

This is the name you use for this location when you create rotation policies. This name also appears in the reports generated in the vaulting process.

The name you enter must start with an alphanumeric character. It can contain only letters, numerals, dashes, underscores, and periods. The maximum character length that you can enter is 127 characters.

6. Enter a customer ID in the **Customer ID** field.

If a vaulting vendor requires an ID for your vaulting process, then you can set this field to that ID. Because the customer ID appears in all distribution reports created for media movement jobs for this location, it accompanies all volumes that are moved at the location.

This step is optional.

7. Select a type of notification that can be sent to the off-site vault vendor when requesting media to be moved. Your choices are **none** or **Iron Mountain FTP**.

Iron Mountain has published an FTP format required for handling electronic communication. If you select **Iron Mountain FTP**, then whenever Oracle Secure Backup requests a volume to be returned from this location, it creates additional pick and distribution reports in this format that you can send by FTP to your vault vendor. These reports contain a list of barcodes for all volumes being requested from an off-site location. Pick and distribution reports are distinguished by a `P` or `D` in the report name and are placed in the `db/report` directory on all platforms.

 **Note:**

Oracle Secure Backup does not automatically send these reports to your vault vendor. You must send them by FTP yourself.

 **See Also:**

"[Viewing Pick and Distribution Reports](#)" for more information about pick and distribution reports

8. Enter one or more e-mail addresses in the **Mail to** field.

The e-mail addresses specified here receive the pick or distribution reports for media movement involving volumes at this location. If user intervention is required for the processing of a media movement job, then the emails configured in the location object receive the notification.

An e-mail system must be operational on the administrative server for this feature to operate. Separate multiple entries with commas.

9. Enter a recall time in the **Recall time** field.

This option enables you to specify the time taken to recall a volume from this storage location back to the administrative domain. You can use this setting to determine whether to fail an RMAN-initiated restore request that requires use of volumes that cannot be supplied within the specified resource wait time period. If duplicate volumes exist, then this value determines which duplicate volume has the shortest recall time. This volume is used for the restore operation.

10. Enter a description of the storage site or other information in the **Comments** field.

11. Click **OK**.

The Configure: Locations page displays a success message, and your additional storage location appears in the list of locations.

Adding Rotation Policies

The rotation policy associated with a volume defines the physical management of that volume as it progresses through its life cycle. The policy determines in what sequence and at which times the volume moves from its initial active location where it is written, to another location, and so on, until it is reused.

A rotation policy is an ordered list of rotation rules. Each rotation rule specifies a location, the amount of time that a volume is retained at that location, and an event that starts the retention clock running. A rotation policy can consist of a single rotation rule, in which case the volume is eligible for recycling at the end of the [retention period](#) specified in its single rule.

A rotation policy is either of the following types:

- Constrained rotation policy

This type of rotation policy names a specific [tape drive](#) or [tape library](#) where volumes controlled by the policy begin their life cycle. A backup adheres to the constraints of this policy. The backup uses only the resources defined by this constraint. It does not apply to volumes that begin their life cycle in any other active location.

- Unconstrained rotation policy

This type of rotation policy specifies a wildcard (*) as its first location. It can apply to volumes that begin their life cycle at any active location.

A **buffer location** is a storage location that you can specify in a rotation policy. Buffer locations have the following important properties:

- Buffer locations are the final stops in the media life cycle.

If a buffer location is specified, then Oracle Secure Backup moves volumes to this location before they are recycled. If a buffer location is not specified, then Oracle Secure Backup returns the volumes using the rotation policy to their original location. Volumes returned from storage locations to your data center can be inserted directly into a tape library or standalone tape drive when received, or they can be stored in buffer locations until they are needed.

- Buffer locations do not have durations.

Volumes in buffer locations remain there until they are inserted into a tape device to begin a life cycle. A volume is removed from the buffer location when it has been unlabeled or overwritten.

- The use of buffer locations is optional.

Oracle Secure Backup ships with a predefined buffer location named `Media_Recycle_Bin`. You can also define additional buffer locations.

- If a buffer location is specified for a policy, then it must be specified in the last rule of the policy.

To add a rotation policy with the Oracle Secure Backup Web tool:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Media Life Cycle section, click **Rotation Policies**.

The Configure: Rotation Policies page appears.

This page displays a list of all currently configured rotation policies. If you are setting up a vaulting environment for the first time, then the list is empty because Oracle Secure Backup does not automatically generate any rotation policies.

4. Click **Add**.

The Configure: Rotation Policies > New Rotation Policy page appears.

5. Enter a name for your rotation policy in the **Rotation Policy** field and click **Apply**.

You must click **Apply** after entering the name of the rotation policy to add rotation rules to the rotation policy.

The name you enter must start with an alphanumeric character. It can contain only letters, numerals, dashes, underscores, and periods. The maximum character length that you can enter is 127 characters.

The Configure: Rotation Policy > *policy_name* page appears, letting you know that your additional rotation policy was created successfully.

6. Although your additional rotation policy exists, it cannot yet manage any volumes because it does not have any rotation rules. To add your first rotation rule:

- a. Select a location from the **Location** list.

The first rotation rule in a rotation policy must specify an active location.

- b. Select an event from the **Event** list.

The event you specify starts the retention clock for this volume. Your choices for an active location are:

- `firstwrite`

The time at which the first write to a volume occurs.

- `lastwrite`
The time at which the last write to a volume occurs. Each additional write to the volume resets the last write time for a volume.
- `nonwritable`
The volume is full, the write window is closed, or the media family is configured as nonappendable.
- `windowclosed`
The write window closes. The write window is the period for which a [volume set](#) remains open for updates, usually by appending another [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.

 **Note:**

The arrival and expiration events are valid only for storage locations. They are discussed in step 7.

- c. Enter a number in the **Duration** field and choose a unit of measure from the adjoining list.

The value you enter in the Duration field is the amount of time that must pass before a volume becomes eligible for a media movement job. The clock starts at the completion of the event you specify in the previous step.

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.
 - d. Select a position in the rotation policy for this rotation rule.

This field should be left at the default value 1, because this is your first rotation rule. The order of the rotation rules determines the order of movement of the volume from location to location.
 - e. Click **Add**.

The Configure: Rotation Policy > *policy_name* page is refreshed, and your additional rotation rule appears in the Rotation rule(s) field.
7. Optionally, specify additional rotation rules so that you can send volumes to a storage location when you are finished writing to them. To add additional rotation rules:
- a. Select a location from the **Location** list.
 - b. Select an event from the **Events** list.

The event you specify starts the retention clock for this location. If you specify an active location for this rotation rule, then your event choices are those described in step 6. If you specify a storage location for this rotation rule, then your choices are:
 - `arrival`

The time at which the volume arrives at this location. The arrival time is assumed to be the completion time for the media movement job that moved the volume to this location.
 - `expiration`

The time at which the volume expires.

- c. Enter a number in the **Duration** field and choose a unit of measure from the adjoining list.
- d. Select a position in the rotation policy for this rotation rule from the **Insert into position** list.

Select last to add a rotation rule at the end of the rotation policy or some number greater than one to add a rotation policy at an intermediate position. The first rotation rule in a rotation policy must specify an active location.

- e. Add a description of this rotation rule in the **Comments** field.

This step is optional.

- f. Click **Add**.

The Configure: Rotation Policy > *policy_name* page is refreshed, and your additional rotation rule appears in the Rotation rule(s) field.

8. Optionally, add a buffer location rotation rule.
9. When you are finished adding rotation rules, click **OK**.

The Configure: Rotation Policies page appears with your additional rotation policy in the Rotation Policies list.

Associating Rotation Policies with Media Families

A volume is associated with a rotation policy. The rotation policy for a volume is inherited from the media family for that volume. The movement of a volume through its life cycle is governed by the rotation policy in effect for its media family at the time the volume left its originating location.

Each media family can be assigned exactly one rotation policy, which applies to all volumes in the family. Associating a rotation policy with a media family is optional. If no rotation policy is associated with a media family, then Oracle Secure Backup does not manage the movement of the volumes created with that media family.

Changing the rotation policy of a media family changes the rotation policy of all volumes that are created with that media family *and* that are located in an active location at or after the time of the policy change. If a volume created with that media family is located in a storage location, then the rotation policy for that volume does not change. You cannot change the rotation policy of a media family that invalidates the active location of a volume made with that media family.

If a media family is associated with a constrained rotation policy, then backups using this family use only the tape device listed as the first location in the rotation policy. Although constrained rotation policies effectively restrict backups to one library, they do not impose restrictions on the choice of drives in a library. To restrict backups to specific drives, you must configure device restrictions for the schedule or backup. Note that Oracle Secure Backup does not permit configuration of device restrictions that can conflict with a constrained rotation policy.

If you use a constrained rotation policy to restrict media family mymf to tape library qualstar1, for example, then a volume in media family mymf cannot have any tape device other than qualstar1 as its originating location. If you subsequently attempt a backup specifying media family mymf and restricting the backup to tape library qualstar2, then the backup command conflicts with the constrained rotation policy, and the command fails with the following error:

```
Error: specified device restriction conflicts with media family device restriction.
```

To associate a rotation policy with a media family:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Basic section, click **Media Families**.
The Configure: Media Families page appears.
4. Select the media family you want to associate with a rotation policy and click **Edit**.
The Configure: Media Families > *family_name* page appears.
5. Select a rotation policy from the **Rotation policy** list and click **OK**.
The Configure: Media Families page displays a success message.

Adding a Vaulting Scan Schedule

During a vaulting scan, Oracle Secure Backup scans one or more locations to determine which volumes are eligible to be moved, based on the rotation policies associated with the volumes at those locations. When it finds one or more volumes eligible to be moved from a location, Oracle Secure Backup creates one media movement job for all eligible volumes at that location. The media movement job is then placed in a pending status until an operator explicitly runs it.

Volumes pending duplication are not considered for media movement. If you cancel a duplication job, then Oracle Secure Backup assumes that you do not want to create a duplicate for that volume and clears it for media movement.

If you use a rotation policy, then you must create either one vaulting scan schedule for the entire administrative domain or individual vaulting scan schedules for each location in the rotation policy. Without the vaulting scan, Oracle Secure Backup cannot select eligible volumes to be moved.



See Also:

["Running Volume Duplication Jobs"](#)

To schedule a vaulting scan:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Schedule Vaulting Scan**.
The Manage: Schedule Vaulting Scan page appears.
4. Click **Add**.
The Manage: Schedule Vaulting Scan > New Schedule Vaulting Scan page appears.
5. Enter a name for the vaulting scan schedule in the **Schedule Vaulting Scan** field.

Schedule names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods. They can contain at most 127 characters.

6. Enter a value in the **Priority** field.

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.

7. Optionally, select one or more locations from the **Restrictions** list.

You can use control-click to select multiple locations or shift-click to select a range of locations. If no locations are selected, then Oracle Secure Backup scans all locations.

8. Select the state in which the vaulting scan schedule is created:

- a. Select **Enabled** if you want the vaulting scan schedule to be in effect immediately. This is the default setting.
- b. Select **Disabled** if you do not want the vaulting schedule to be in effect immediately.

If you create a vaulting scan schedule in the Disabled state, then you can later change it to Enabled by returning to the Manage: Schedule Vaulting Scan page and editing the vaulting scan schedule.



See Also:

["Managing Vaulting Scan Schedules"](#)

9. In **Media family selections**, optionally select one or more media families.

If you select a media family, then Oracle Secure Backup scans only the selected media family. If no media families are selected, then Oracle Secure Backup scans all media families.

10. Click **Apply**.

The Manage: Schedule Vaulting Scan > *schedule_name* page appears.

11. Click **Triggers**.

The Manage: Schedule Vaulting Scan > *schedule_name* > Triggers page appears as shown in [Figure 11-2](#).

Figure 11-2 Triggers Page for Vaulting Scans

Manage: Schedule Vaulting Scan > vault_scan_1 > Triggers

Add Remove Cancel Preview

ID	Trigger
(Empty)	

Time 00 hours 00 minutes Expire after disabled

Trigger type Day

Select daily
 Select weekdays
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Select weekend
 Sunday
 Saturday

Week in month

All
 Selected
 First
 Second
 Third
 Fourth
 Fifth
 Last

Weekday exceptions

Except none Time none Specify day none none

12. In the Time section, select a trigger time from the **hours** and **minutes** lists.
13. Select a trigger type from the **Trigger type** list.
14. If you selected trigger type **Day**, then do the following:
 - a. Select the days you want the vaulting scan to run:
 - **Select daily**
This option produces a daily vaulting scan, seven days a week.
 - **Select weekdays**
This option produces a daily vaulting scan, Monday through Friday.
 - **Select weekend**
This option produces a vaulting scan only on Saturday and Sunday.
 - Select one or more days of the week
 - b. Select the week in the month you want the vaulting scan to run.
The default is all weeks.
 - c. In the Weekday exceptions section, you can specify days you do not want the vaulting scan to run by selecting except from the **Except** list, before or after from the **Time** list, and a particular weekday from the **Specify day** lists.
15. If you selected trigger type **Month**, then select an option in the **Day in month** section.
16. Click **Add**.

17. To add another trigger, go back to step 12.

When you are done adding triggers, click **Schedule Vaulting Scan** in the breadcrumbs at the top of the page.

The Manage: Schedule Vaulting Scans page appears with the additional vaulting scan schedule in the list of schedules.

Performing an On-Demand Vaulting Scan

You can use the Web tool to perform a one-time, on-demand vaulting scan without creating a scheduled scan.

To perform a one-time on-demand vaulting scan:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Web tool Home page, click **Manage**.

The Manage page appears.

3. In the Media Life Cycle section, click **Vault Now**.

The Manage: Vault Now page appears.

4. In **Priority**, enter a priority for the on-demand vaulting scan.

The priority for a job is a positive numeric value. The lower the value, the greater the importance assigned to the job by the scheduler. The scheduler gives preference to dispatching more important jobs over those with lesser importance.

This step is optional. The default priority is 100.

5. In **Expire after**, optionally enter a number and select a unit from the adjacent list.

If the on-demand vaulting scan cannot run immediately, then Oracle Secure Backup waits the specified amount of time before deleting the job. If no duration is specified, then Oracle Secure Backup waits forever to run the job.

6. In **Date** and **Time**, optionally enter a date and time for the scan.

By default, the current date and time are shown, which means that Oracle Secure Backup performs an immediate scan.

7. In **Media family selections**, optionally select a media family.

You can select multiple media families by shift-clicking. If you select one or more media families, then Oracle Secure Backup only checks volumes belonging to those media families. If no media family is selected, then the on-demand vaulting scan checks all volumes.

8. Select a location from the **Restrictions** list.

You can select multiple locations by shift-clicking. If you select one or more locations, then Oracle Secure Backup only checks those locations.

This step is optional. If no location is selected, then the on-demand vaulting scan checks all locations.

9. Click **Go**.

The Manage: Vault Now page is refreshed, and a message like the following appears:

```
Info: vaulting scan request 1 submitted; job id is admin/3
```

You can check the progress of the vaulting scan at the Manage: Jobs page.

Running Media Movement Jobs

Vaulting in a typical large organization could be organized something like this:

1. The Oracle Secure Backup administrator tells the backup operator on which days and at which times the operator is to check for scheduled media movement jobs on the Web tool Manage: Jobs page.
2. For each scheduled media movement job in the list, the backup operator prints any reports needed to accompany the volumes to be moved.

Pick and distribution reports are created for every media movement job.

Note:

You can set media movement jobs to start automatically with the `autorunmmjobs` policy, but manual intervention might still be required to *complete* a media movement job for a variety of reasons. See *Oracle Secure Backup Reference* for more information.

3. The backup operator runs the media movement jobs.
4. The operator removes ejected volumes from the containing libraries.
The ejection type for the library determines what the operator must actually do to eject the volumes. The operator can use the pick report to verify the volumes that are ejected.
5. The operator packs the ejected volumes for transport, including a copy of the distribution report with the volumes.

See Also:

["Ejecting Volumes from Libraries"](#)

Volumes that are scheduled to return to the local data center from a storage location are listed on a distribution report. The report can be provided to the storage location operator, who might be an off-site storage vendor, to identify which volumes to be shipped back to the data center. Returned volumes are placed directly into a tape library or into some buffer location until they are needed to restock a tape library.

Run the media movement job created for returning volumes when the job is created. The volumes that need to be returned are marked as in-transit until either of the following actions occur:

- The volume has been inserted into the destination library and an inventory is performed on the library.
- A `chvol --notintransit` command marks the volumes not in transit, which means that the volumes are located where they should be.

At smaller sites the Oracle Secure Backup administrator typically performs all of the preceding tasks.

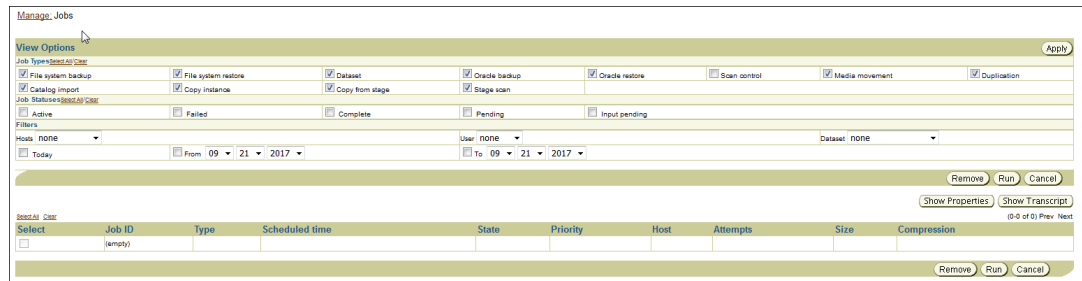
 **See Also:**

- "Viewing Pick and Distribution Reports" for more information about distribution and pick reports
- *Oracle Secure Backup Reference* to learn more about the `--notintransit` option of the `chvol` command

To run a media movement job using the Oracle Secure Backup Web tool:

1. Follow the steps in "Displaying the Oracle Secure Backup Web Tool Home Page".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Management section, click **Jobs**.
The Manage: Jobs page appears as shown in Figure 11-3.

Figure 11-3 Manage Jobs Page



4. By default, the Manage: Jobs page displays information about active jobs in the following categories:
 - File system backup
 - File system restore
 - Dataset
 - Oracle backup
 - Oracle restore
 - Media movement
 - Duplication

You can control what jobs are displayed on the Manage: Jobs page by deselecting any of the preselected options or by selecting any of the following additional options:

- Complete
- Pending
- Input pending
- Today
- Scheduled time

- From date
- To date
- Scan control

You can also control what jobs are displayed by choosing a host from the **Hosts** list, a user from the **Users** list, a dataset from the **Dataset** list, or any combination of these.

5. Select **Pending** in Job Statuses and click **Apply**.

The Manage: Jobs page is refreshed, and pending jobs appear in the list of jobs.

6. Select a media movement job and click **Run**.
7. Select the **Now** and **Media movement** options.
8. Leave the Devices list set to **none**.
9. Click **Apply**.

The Manage: Jobs page displays a success message, indicating that the media movement job was submitted.

The **State** column of the jobs list indicates either that the job completed successfully or that operator assistance is required. If operator assistance is required to complete the media movement job, then Oracle Secure Backup users configured for e-mailed job summaries receive a message similar to the following:

Dear reader:

```
Oracle Secure Backup job 3 is requesting assistance.
The job will resume when an operator responds.
```

```
If you'd like to view and optionally respond to this request, use --
. the Web tool's Manage/Jobs interface and its Show Transcript function, or
. obtool's transcript display command: obtool catxcr --tail 25 3
```

Thank you,
Oracle Secure Backup

If the preceding message appears, proceed to the next step. Otherwise, stop here.

10. Provide operator assistance by following these steps:
 - a. On the Manage: Jobs page, click **Show Transcript**.
 - b. Scroll to the end of the transcript to see why operator assistance is required.
 - c. Enter the appropriate command in the **Input Required!** field.
 - d. Click **Apply**.

In-Transit Flags

If a media movement job moves a volume from a library to a storage location, then Oracle Secure Backup knows when the volume is ejected from the library and immediately updates its catalog to show the volume in the specified location. Several days may go by before the volume exists in the storage location, but no harm is done by updating the catalog immediately.

If a media movement job moves a volume from a storage location to a library, however, Oracle Secure Backup cannot determine whether the volume is out of the storage location. If Oracle Secure Backup were to update its catalog immediately to show the volume in its changed location, then operations depending on this volume would be in a pending state until the volume arrived.

For example, suppose that a volume is recalled from a storage location for a restore operation. The media movement job for the recall runs and immediately marks that volume as back in the library. The restore job that was waiting for this volume starts immediately but cannot progress because it cannot find the volume in the library.

To avoid this problem, Oracle Secure Backup does not immediately show volumes in their changed locations when moving them from a storage location to another storage location or to a library. Instead, these volumes are tagged with *in-transit* flags. If the volumes are being moved from storage to a library, these flags are removed automatically when the volumes are loaded into their changed locations and an inventory is done. Any operation that causes Oracle Secure Backup to read the in-transit volume clears the in-transit flag and updates the current location.

If volumes are being moved from one storage location to another storage location, then the in-transit flags must be removed manually. In-transit flags can be removed from one or more volumes in a single operation using either the Manage: Volumes page in the Oracle Secure Backup Web tool or the `obtool chvol` command.

See Also:

- ["Recalling a Volume"](#)
- ["Changing Volume Properties"](#) for instructions on using the Oracle Secure Backup Web tool to remove in-transit flags
- *Oracle Secure Backup Reference* for full syntax and semantics for the `chvol` command

Minimum Writable Volumes

Specifying a minimum writable volumes for a tape library provides an automatic method for freeing up storage element slots in the library by rotating out non-writable volumes. The freed slots can then be filled with writable volumes. When Oracle Secure Backup scans a library for volumes to be moved, it also looks at the minimum writable volume threshold for each tape library. If the minimum writable volume threshold is nonzero, and if the number of writable volumes in that tape library has fallen to less than this threshold, then Oracle Secure Backup creates media movement jobs for the non-writable volumes. The non-writable volumes get media movement jobs even if their rotation policies do not yet require them to be moved. When this happens, Oracle Secure Backup notes in the vaulting scan job transcript that volumes have been moved early, as shown in the following example:

```
ob> catxcr -10 1
2008/09/05.20:42:44 _____
2008/09/05.20:42:44
2008/09/05.20:42:44 Transcript for job 1 running on stacr12
2008/09/05.20:42:44
2008/09/05.20:42:44 Processing location vlibminwrt
2008/09/05.20:42:44 Checking volume mf1-000001
2008/09/05.20:42:44 Volume mf1-000001 added to full volume list
2008/09/05.20:42:44 Checking volume mf1-000002
2008/09/05.20:42:44 Volume mf1-000002 added to full volume list
2008/09/05.20:42:44 Checking volume mf1-000003
2008/09/05.20:42:44 Volume mf1-000003 added to full volume list
2008/09/05.20:42:44 Checking volume mf1-000004
2008/09/05.20:42:44 Checking volume mf2-000001
2008/09/05.20:42:44 Full volume mf1-000001 added to volume movement list
```

```
2008/09/05.20:42:44 Full volume mf1-000002 added to volume movement list
2008/09/05.20:42:44 Full volume mf1-000003 added to volume movement list
2008/09/05.20:42:44 Created media movement request 1
2008/09/05.20:42:44 Done processing location vlibminwrt
2008/09/05.20:42:44 Media movement request 1 submitted; job id is 2
```

The vaulting scan job identified volumes mf1-000001, mf1-000002, mf1-000003 as non-writable volumes that can be moved to maintain the minimum writable volumes threshold. A media movement job for these volumes was created.

When a volume is rotated out of a tape library early, because the minimum writable volumes threshold has been reached, its duration at its next location is unchanged. For example, suppose a volume had a duration of four weeks after its write window closed in the tape library and six weeks after its arrival at Iron Mountain. If the volume is rotated early out of the tape library in its first week after its window closed, then its duration at Iron Mountain is still six weeks after arrival rather than nine weeks.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for instructions on setting a tape library minimum writable volumes threshold

Ejecting Volumes from Libraries

Operator assistance can be required in a media movement job, depending in part on the ejection type you specified when configuring a tape library for use with Oracle Secure Backup.

 **See Also:**

Oracle Secure Backup Installation and Configuration Guide for more information about configuring a tape library for use with Oracle Secure Backup

This section contains these topics:

- [Automatic Library Ejection](#)
- [On Demand Library Ejection](#)
- [Manual Library Ejection](#)

Automatic Library Ejection

This ejection type is necessary only for libraries with at least one import/export element or cartridge access port (CAP). ACSLS libraries have different export requirements compared to non-ACSLs libraries. In ACSLS, an export fails if the CAP has any volumes. In non-ACSLs libraries, an export fails only if there are no vacant export elements.

For libraries configured for automatic ejection type, Oracle Secure Backup performs the following steps:

1. Update library inventory.
2. Determine the number of volumes that can be moved out of the library.

- a. For an ACSLS library, the number of volumes that can be moved out depends on the CAP size. If a CAP name was not specified in the vaulting scan schedule, then Oracle Secure Backup picks the largest CAP available.
 - b. For a non-ACSLs library, the number of volumes that can be moved depends on the number of vacant export elements.
3. For each volume in the list of volumes to be moved, Oracle Secure Backup unloads the volume if it is in a drive and adds the volume to the list of volumes to be exported.

If the unload fails for a specific volume, then Oracle Secure Backup skips that volume and continues to process other volumes in the job. The skipped volume can be picked up by any subsequent media movement job for the same location.
 4. Oracle Secure Backup exports the volumes from ACSLS libraries when all volumes in the media movement job have been added to the list, or when the number of listed volumes equals the maximum number of volumes that can be moved.

For non-ACSLs libraries, Oracle Secure Backup exports the volumes one at a time.
 5. Any errors during this export are written to the media movement job transcript to be resolved by the Oracle Secure Backup operator.
 6. If an export fails, either because the CAP/IEE is full or because the ACSCS / `maxacsejectwaittime/` was reached, then Oracle Secure Backup retries the operation for a certain period and requests operator intervention if needed at the end of that time period.

On Demand Library Ejection

This ejection type is necessary only for libraries with at least one import/export element or cartridge access port (CAP). It is similar to the automatic ejection type, except that Oracle Secure Backup displays the following prompt once for each media movement job:

```
go - proceed with the volume movement
quit - give up and abort this media movement job
```

The Oracle Secure Backup operator must then use the `rpjjob` command to enter one of these options.

See Also:

Oracle Secure Backup Reference for complete syntax and semantics for the `rpjjob` command

Manual Library Ejection

No automation is used to eject volumes from the tape library. The backup operator determines which storage elements contain volumes ready to be ejected and manually removes them. This option can be useful when the library has no import/export slots.

Note:

If `automatic` or `ondemand` was specified, but Oracle Secure Backup detects that there are no iee slots, then the software automatically switches to manual ejection mode.

Oracle Secure Backup performs an initial library inventory during a media movement job and then shows the following prompt for each volume in the media movement job:

```
go - volume movement job completed, continue
goall - all volume movement completed for this job
quit - give up and abort this media movement job
```

The Oracle Secure Backup operator must then use the `rpymjob` command to enter one of these options.



See Also:

Oracle Secure Backup Reference for complete syntax and semantics for the `rpymjob` command

quit

If the Oracle Secure Backup operator selects the `quit` option, then the media movement job fails. Volumes whose catalog entries had been updated retain those updated entries. Volumes whose catalog entries had not been updated remain as-is until the next media movement job for the library. These unprocessed volumes are listed in the job transcript.

go

If the Oracle Secure Backup operator selects the `go` option, then Oracle Secure Backup does an inventory of the library to determine if the specified volume is still located in the library. If the volume is still in the library, then Oracle Secure Backup prompts the operator with a different set of options:

```
go - volume movement really completed, continue
goforce - volume movement completed, skip inventory check for this volume
skip - skip the movement of this volume
```

If the operator again selects the `go` option, then Oracle Secure Backup does another inventory of the library and presents the same prompt again if the volume is found. If the volume no longer appears in the library, however, then Oracle Secure Backup updates the volumes catalog to reflect the changed location of the volume.

If the operator chooses the `goforce` option, then Oracle Secure Backup does not recheck the library inventory and assumes the volume has been removed. Oracle Secure Backup updates the volumes catalog with the changed location of the volume. But Oracle Secure Backup also puts a warning in the job transcript that, according to its inventory the physical volume is still in the library.

If the operator chooses the `skip` option, then Oracle Secure Backup does not update the volumes catalog for this volume. It is processed again as part of the next media movement job for this library. The job transcript shows that the operator chose to skip movement of this volume.

If multiple volumes were included in the media movement job, then Oracle Secure Backup repeats the inventory and prompt until all volumes have been processed.

goall

If the Oracle Secure Backup operator selects the `goall` option, then the prompt is suppressed for all subsequent volumes in the media movement job.

Viewing Location Reports

Oracle Secure Backup provides three types of location reports:

- **Location report**
A location report displays a list of volumes at a particular location, ordered by volume ID. For each volume listed, it shows the next location it is expected to move to and the date that the volume is eligible to be moved to that next location. The next location and eligibility move date come from the rotation policy in effect for that volume.
- **Schedule report**
A schedule report contains the same information as a location report, but it is limited to volumes whose move-eligibility dates fall within a range that you specify.
- **Exception report**
An exception report shows the current and expected locations for all volumes whose current and expected locations are different. If a volume is recalled from a storage location back into a tape library, for example, then that volume appears in the exception report for that tape library.

A location report displays a list of volumes at a particular location. If a volume is associated with a rotation policy, then the next scheduled location and the move date are also displayed.

To view a location report:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Location Reports**.
The Manage: Location Reports page appears.
4. Select a location from the list of locations.
The location report page lists all configured locations within the administrative domain.
5. Select **location** from the Type list.
6. Click **View Report**.
A different page lists all volumes eligible for movement from that location. Each listing includes the volume name, next location, and move date.

Recalling a Volume

If an Oracle Secure Backup operator issues a `restore` command that requires one or more volumes that are not present in an active location, then Oracle Secure Backup automatically marks each required volume as being eligible for recall. A subsequent vaulting scan of the current location of each required volume results in a media movement job for recalling that volume.

When a volume is moving to an active location from a storage location, Oracle Secure Backup flags the volumes as `in-transit` and does not immediately update its volume catalog with the changed location of recalled volumes. The `in-transit` flag is necessary because Oracle Secure Backup cannot know whether the volume is still in the storage location or already moved from this location.

 **Note:**

When a volume is moving to a *storage* location from an *active* location, Oracle Secure Backup performs an inventory at the end of the media movement job to ensure that the volume is absent from the library. For this reason the `in-transit` flag is not necessary.

When volumes moved from storage arrive in the active location, they must be placed in their changed location. For a non-ACSLs library, volumes can be placed in a library slot or in an import/export slot. For an ACSLS library, volumes must be placed in a cartridge access port and injected into the ACSLS library from the ACSLS console.

You can update the Oracle Secure Backup volume catalog by selecting **Inventory** on the Libraries page. If a backup starts before the inventory has been updated, then Oracle Secure Backup updates it automatically. When the inventory is updated, the current location of any volume marked as *in-transit* is updated to contain the library location it resides in and the *in-transit* flag is removed from the volume record.

 **See Also:**

- ["In-Transit Flags"](#) for more information about in-transit flags
- ["Changing Volume Properties"](#) for instructions on using the Oracle Secure Backup Web tool to remove in-transit flags
- *Oracle Secure Backup Reference* for full syntax and semantics for the `chvol` command
- *Oracle Secure Backup Reference* for more information about the `autorunmmjobs` policy

Releasing a Volume

When the restore operation requiring a recalled volume is complete, Oracle Secure Backup can create a media movement job to return the recalled volume to the location from which it was recalled. This media movement job, also known as *releasing* a volume, can be generated automatically by Oracle Secure Backup or manually by the backup operator. If a recalled volume is not released, then it is outside its rotation policy and unmanaged by Oracle Secure Backup.

If the `autovolumerelease` policy is set to `yes`, then volumes automatically recalled by Oracle Secure Backup are automatically released when the backup operation is completed. If the policy is set to `no`, then the volumes must be released manually. You can configure the `autovolumerelease` policy at the Oracle Secure Backup Web tool Configure: Defaults and Policies > Vaulting page. The `autovolumerelease` policy has no effect on volumes manually recalled by the backup operator.

Oracle Secure Backup enables a backup operator to do an on-demand recall of a volume from its current storage location using the Oracle Secure Backup Web tool Manage: Volumes page. Oracle Secure Backup creates a media movement job for the recalled volume, which can run immediately if the operator specifies so. The recalled volume can be inserted into any tape device to perform the restore operation.

Volumes recalled by a backup operator are not automatically released when the restore operation is completed. The backup operator must release the volume from its current location and return the volume to the proper place in its rotation as specified by the rotation policy that applies to that volume. The backup operator can use the Oracle Secure Backup Web tool Manage: Volumes page for this purpose. The volume is frozen at its current point in its rotation policy until it is released.

If you have enabled volume duplication in your vaulting environment, then multiple copies of a backup volume might be available. Oracle Secure Backup first looks in its volumes catalog for duplicate volumes, determines their locations, and identifies the volume with the lowest recall time. If the identified volume is not at an active location, then Oracle Secure Backup schedules a media movement request.

 **See Also:**

- ["Volumes Outside Their Rotation Policies"](#)
- ["Running Media Movement Jobs"](#)
- *Oracle Secure Backup Reference* for more information about the `autovolumerelease` policy

Viewing Pick and Distribution Reports

The following two reports are generated automatically when you run a media movement job:

- Pick report

This is a list of all volumes to be picked for distribution to another location: a shopping list used to gather the volumes from a tape library or storage location to box and ship to their next location.

- Distribution report

This is a list of all volumes being sent to a particular location as the result of a media movement job: a packing list to be included in the shipment of volumes to a location.

In each case, the report name includes the media movement job number. Distribution and pick reports contain identical lists of volumes. In most cases, the only difference is that the distribution report also contains the customer ID (if any) assigned to the next location. However, the reports can differ when exceptions occur during media movement job processing. For example, if you skip the movement of a volume during job processing, then the pick report contains all volumes that should have been moved by the job, whereas the distribution report contains all volumes actually moved.

If you selected Iron Mountain FTP notification when you configured an off-site storage location, then whenever Oracle Secure Backup requests a volume be moved to or from that location, it creates additional pick and distribution reports in the format that Iron Mountain requires for handling electronic communication. These reports contain a list of barcodes for all volumes that are being requested from an off-site location.

You can send these reports by FTP to any vault vendor that supports the Iron Mountain FTP format. Pick and distribution reports are distinguished by a "P" or "D" in the report name. Both reports are placed in the `OSB_HOME/db/report` directory on all platforms.

 **Note:**

Oracle Secure Backup does not automatically send these reports to your vault vendor. You must send them by FTP yourself.

 **See Also:**

["Adding Locations"](#) for more information about Iron Mountain FTP notification

To view distribution and pick lists:

1. Follow the steps in ["Displaying the Oracle Secure Backup Web Tool Home Page"](#).
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Pick and Distribution Reports**.
The Manage: Pick and Distribution Reports page appears.
4. Select the report you want to view and click **View Report**.

Adding Volume Duplication Policies

Each media family can have at most one associated duplication policy. It defines for all volumes in the media family:

- At what point in their life cycles volumes are duplicated
- Whether the original volumes continue to exist or are replaced by duplicate volumes
- What media family the duplicates belong to (which can be different from the media family of the original volumes)
- How many duplicates are made
- Which tape devices are used for the duplications

Duplicate volumes cannot be reduplicated. If a duplication policy specifies that volume duplication uses a media family that itself has a volume duplication policy, then Oracle Secure Backup ignores requests for automatic duplication of volumes in that media family. Otherwise, it would be possible to configure policies that would require the endless duplication of volumes. To duplicate a duplicate volume, use on-demand duplication.

 **See Also:**

["On-Demand Volume Duplication"](#)

To add a duplication policy:

1. Follow the steps in ["Displaying the Oracle Secure Backup Web Tool Home Page"](#).
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Media Life Cycle section, click **Volume Duplication Policies**.

The Configure: Volume Duplication Policies page appears.

4. Click **Add**.

The Configure: Volume Duplication Policies > New Volume Duplication Policies page appears.

5. Enter a name for the volume duplication policy in the **Volume Duplication Policy** field.

The name you enter must start with an alphanumeric character. It can contain only letters, numerals, dashes, underscores, and periods. The maximum character length that you can enter is 128 characters.

6. In the Trigger section:

- a. Enter a number in the **Time** field and select a unit of measure from the adjoining list.
- b. Select a trigger event in the **after** list.

The event that causes duplication to occur can be one of these:

- `firstmove`

The time that a volume becomes eligible to be moved from its first active location. This is defined by the rotation policy for that volume.

- `firstwrite`

The first write to a volume occurs.

- `lastwrite`

The last write to a volume occurs.

- `nonwritable`

The volume is full, the [write window](#) is closed, or the media family is configured as nonappendable.

- `windowclosed`

The write window closes. The write window is the period for which a volume set remains open for updates, usually by appending another backup image instance. 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.

For example, if you selected `1 day` and `windowclosed`, then duplication could occur one day after the volume can no longer be written to. A duplication job is scheduled only if the event occurs at the first active location in the rotation policy.

7. In the Migration section, select **yes** or **no**.

Volume migration is the creation of a duplicate that replaces the original. If you select **yes**, then the original volume is deleted after it is successfully duplicated. You might want to do this when a volume has been in storage for an extended period or when the retention time required for a volume is longer than the expected lifetime of the physical media.

Volume migration is also recommended if you currently back up to a virtual tape library. A virtual tape library is not suitable for long time storage, because it has limited storage capacity. If you back up to a virtual tape library, then you can take advantage of its faster backup and use the volume migration feature of Oracle Secure Backup to migrate the data to tapes later. Migration copies the volume from the virtual tape library to a physical tape and unlabels the original volume on the virtual tape library. Unlabeling the original volume frees up memory used for that volume on the virtual tape library.

8. Select the media family you want to use for this duplication policy in the **Media family** list.
The media family you select in this step determines the rotation policy and retention period of the duplicate volume. Because this media family can be different from the media family of the original volume, duplicate volumes can have a different rotation policy and retention period than the original volume. But if the original volume has a content-managed expiration policy, then the duplicate volumes must be content-managed as well. Similarly, if the original volume has a time-managed expiration policy, then the duplicate volumes must be time-managed as well.
9. Enter the number of duplicates you want to make in the **Number of duplicates** field.
The default is one duplicate.
10. Select a restriction in the **Restrictions** field.
This step is optional. You can restrict volume duplication to specific tape devices. If you do not select a restriction, then volume duplications defined by the policy can use any available tape device on any media server, at the discretion of the Oracle Secure Backup scheduling system.
11. Enter a description of this duplication policy in the **Comments** field.
This step is optional.
12. Click **OK**.
The Configure: Volume Duplication Policies page displays a success message, and your additional duplication policy appears in the list.

Associating Volume Duplication Policies with Media Families

Oracle Secure Backup automatically duplicates a volume if a volume duplication policy is associated with that volume's media family. Each media family can be associated with at most one volume duplication policy. Associating a volume duplication policy with a media family is optional.

Duplicate volumes cannot be reduplicated. If a duplication policy specifies that duplicates are to be added to a media family, then Oracle Secure Backup ignores requests for automatic duplication of volumes in that media family. Otherwise, it would be possible to configure policies that would require the endless duplication of volumes. To duplicate a duplicate volume, use on-demand duplication.



See Also:

["On-Demand Volume Duplication"](#)

To associate a volume duplication policy with a media family:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Basic section, click **Media Families**.
The Configure: Media Families page appears.
4. Select the media family you want to associate with a volume duplication policy and click **Edit**.

The Configure: Media Families > *family_name* page appears.

5. Select a volume duplication policy from the **Volume duplication policy** list and click **OK**.
The Configure: Media Families page displays a success message.

 **See Also:**

"[Associating Rotation Policies with Media Families](#)" for screen shots of the Configure: Media Families and Configure: Media Families > *family_name* pages

Adding Volume Duplication Windows

A volume duplication window is the interval during which Oracle Secure Backup schedules duplication jobs to run. Oracle Secure Backup automatically generates a daily volume duplication window that begins at 10:00 and ends at 20:00. If this duplication window is sufficient to your needs, then no action is required.

It is recommended that you eliminate any overlap between your duplication window and your [backup window](#), so that a duplication job and a [backup job](#) do not contend for the same tape device. If your duplication window overlaps your backup window, then duplication jobs can get scheduled to run before backup jobs. If this happens, then some backup jobs might not have sufficient resources to run.

If a duplication job starts within a duplication window but does not finish within the window interval, then it is allowed to run until the duplication finishes. If subordinate or retry jobs are submitted by this job because of a duplication failure, then the newly created jobs are scheduled in the next duplication window.

To add a duplication window:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Advanced section, click **Volume Duplication Windows**.

The Configure: Volume Duplication Windows page appears.

4. This page displays the default volume duplication window that Oracle Secure Backup generates automatically.

If you want a different volume duplication window, then select the default and click **Remove**.

A confirmation page appears.

5. Click **Yes**.

The Configure: Volume Duplication Windows page displays a success message, and the default volume duplication window no longer appears in the duplication window list.

6. Click **Add**.

The Volume Duplication Window page appears.

7. Select a volume duplication window type from the **Type** list.

8. If you selected **Date** in step 7, then select a month, day, and year from the **Month**, **Day**, and **Year** lists.
9. If you selected **Day range** in step 7, then select a day range from the following options:
 - **Select daily**
This is equivalent to selecting all seven days in a week
 - **Select weekdays**
This is equivalent to selecting Monday through Friday
 - **Select weekend**
This is equivalent to selecting Sunday and Saturday.
 - Any combination of individual days of the week
10. Enter a time range in the **Time range** field.
The time range must be in 24-hour hh:mm-hh:mm format with no embedded spaces.
11. Click OK.
The Configure: Volume Duplication Windows page displays a success message, and your additional volume duplication window appears in the list of volume duplication windows.

Adding Volume Duplication Schedules

A volume duplication schedule determines where and when a volume duplication job is scheduled, what priority the volume duplication job has, and how long Oracle Secure Backup waits before expiring a duplication job that has not run.

Scheduling volume duplication is similar to scheduling a vaulting scan. Oracle Secure Backup scans its catalog to determine which volumes are eligible for duplication, according to the duplication policies of their respective media families. If Oracle Secure Backup finds a volume eligible for duplication, then it creates a volume duplication job for that volume. Volume duplication jobs are performed automatically during the volume duplication window.



See Also:

["Adding Volume Duplication Windows"](#)

To add a volume duplication schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Schedule Volume Duplication**.
The Manage: Schedule Volume Duplication page appears.
4. Click **Add**.
The Manage: Schedule Volume Duplication > New Schedule Volume Duplication page appears.
5. Enter a name for the volume duplication schedule in the **Schedule Volume Duplication** field.

6. Enter a value in the **Priority** field.

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.

7. Select at least one location in the **Locations** list.

You can use control-click to select multiple locations or shift-click to select a range of locations. Only active locations can be specified in a volume duplication schedule.

8. Click **Apply**.

The Manage: Schedule Volume Duplication > *schedule_name* page appears.

9. Click **Triggers**.

The Manage: Schedule Volume Duplication > *schedule_name* > Triggers page appears.

10. In the Time section, select a **trigger** time from the **hours** and **minutes** lists.

11. Select a trigger type from the **Trigger type** list.

12. If you selected trigger type **Day** in step 11, then do the following:

- a. Select the days you want the volume duplication scan to run:

- **Select daily**

This option produces a daily volume duplication scan, seven days a week.

- **Select weekdays**

This option produces a daily volume duplication scan, Monday through Friday.

- **Select weekend**

This option produces a volume duplication scan only on Saturday and Sunday.

- Select one or more days of the week

- b. Select the week in the month you want the volume duplication scan to run.

The default is all weeks.

- c. In the Weekday exceptions section, you can specify days you do not want the volume duplication scan to run by selecting except from the **Except** list, before or after from the **Time** list, and a particular weekday from the **Specify day** lists.

13. If you selected trigger type **Month** in step 11, then select an option in the **Day in month** section.

14. Click **Add**.

The Manage: Schedule Volume Duplication > *schedule_name* > Triggers page displays a success message, and the trigger appears in the Trigger list.

15. To add another trigger, go back to step 10.

When you are done adding triggers, click **Schedule Volume Duplication** in the breadcrumbs at the top of the page.

The Manage: Schedule Volume Duplication page appears with the additional volume duplication schedule in the list of schedules.

Running Volume Duplication Jobs

When a volume duplication job is scheduled to run within a duplication window, the Oracle Secure Backup scheduler reserves the required resources and dispatches the job to a media server. Oracle Secure Backup assigns a lower priority to a duplication job than to a backup job

by default. But you can use the `duplicationjobpriority` policy to specify the priority of volume duplication jobs relative to other jobs.

If a resource restriction has been specified for the volume duplication job, then the scheduler picks up the specified resources for running the job. If no restriction has been specified, then the scheduler tries to pick up the best set of tape devices to be used for the duplication. The scheduler initially looks for tape devices in the same media server. If tape devices are available in the same media server, then the volume duplication job runs on that media server.

 **Note:**

You must have multiple tape drives installed and configured in your Oracle Secure Backup administrative domain to duplicate a volume.

If tape devices are not available in the same media server and the `duplicateovernetwork` policy is enabled, then the scheduler tries to run the volume duplication job with tape devices in other media servers. In this case, the scheduler runs the job on the media server where the original volume is located. The component on the media server performing the volume duplication job sends the data over the network to another media server.

Duplication over a network slows duplication performance considerably and might use significant network bandwidth. Duplication over networked tape devices is not advisable. Oracle Secure Backup does not make use of tape devices over the network by default.

If the `duplicateovernetwork` policy is not enabled and a tape device restriction in the duplication policy specifies tape devices that are in a different media server than the original server, then the restriction takes precedence, and the duplication procedure uses the tape devices over the network.

If the original volume is located on a media server which does not run Oracle Secure Backup software, such as a NetApp filer, then the volume duplication job runs on the Oracle Secure Backup administrative server.

The volume duplication job transcript reports the number of archive files (backups) copied from the source volume. This number is off by one from the actual number of archive files present in the source volume, because it includes a count for the end of data (EOD) marker.

 **See Also:**

Oracle Secure Backup Reference for more information about the `duplicationjobpriority` policy

Volume Duplication Job Failures

Volume duplication jobs run automatically and do not ordinarily require the attention of a backup operator. If a volume duplication job fails, however, then the job is moved to a retry state so that it can be run at a later time. The backup operator must check the list of pending jobs on the Oracle Secure Backup Web tool Manage: Jobs page to see if any volume duplication jobs are pending or have failed and require corrective action.

 **See Also:**

"[Running Media Movement Jobs](#)" for instructions on running jobs from the Oracle Secure Backup Web tool Manage: Jobs page

The destination volume must have capacity at least equal to that of the original volume. If Oracle Secure Backup finds that the destination volume is smaller than the original volume, then it logs an error and fails the volume duplication job. An additional job is scheduled, which tries to find another eligible volume.

If duplication is attempted in a tape library with a robotic arm, then Oracle Secure Backup tries to find an eligible volume. If an eligible volume is found, then duplication proceeds. If an eligible volume is not found, then Oracle Secure Backup fails the volume duplication job.

An original volume cannot move from its originating location until all specified duplicates have been successfully created. If a backup operator uses the `exportvol` command to export an original volume, then Oracle Secure Backup checks to see if that volume is to be duplicated. If the specified duplicates have not yet been created, then Oracle Secure Backup gives a warning.

On-Demand Volume Duplication

In addition to automatic volume duplication, Oracle Secure Backup enables you to duplicate a volume manually at any time using any available tape devices.

Oracle Secure Backup does not consider manually created duplicate volumes when deciding if a volume's duplication requirements have been met. These duplication requirements are specified by the duplication policy associated with the volume.

Oracle Secure Backup does not allow a volume to move out of a tape library during vaulting even if you have manually created its required number of duplicates. To move a volume before its required number of duplicates have been created automatically, you must first remove the duplication policy for the volume.

 **See Also:**

- "[Duplicating Volumes](#)"
- "[Changing Volume Properties](#)"

Exporting Duplicate Volumes to Another Domain

A backup administrator can create a duplicate of a backup volume in one Oracle Secure Backup administrative domain and import the duplicate into another Oracle Secure Backup administrative domain using the `-G` option of `obtar`. Because the duplicate volume is the only source of restore information in the second administrative domain, Oracle Secure Backup imports it as an original volume.

If a backup administrator tries to import multiple duplicate volumes into another Oracle Secure Backup administrative domain, and if all of the duplicates were created from the same original volume, then the first duplicate volume is imported as an original volume and subsequent volumes are imported as duplicates.

If an original volume is imported into another Oracle Secure Backup administrative domain after a duplicate volume has been imported, then the original volume is imported as a duplicate volume in the second administrative domain.

NDMP Volume Duplication

Oracle Secure Backup uses NDMP volume duplication whenever the source and destination volumes both reside on the same NDMP copy-enabled VTL.



See Also:

["About NDMP Copy-Enabled Virtual Tape Library"](#)

Tracking Volumes Through a Vaulting Environment

This section describes a simple vaulting environment in terms of the volumes whose movements are being managed by Oracle Secure Backup. The administrative domain consists of a single host with a single tape library. The only volumes being managed are the Oracle Secure Backup catalog recovery volumes, and the only storage location is an on-site fire-resistant closet. [Table 11-1](#) describes how the vaulting environment progresses from its inauguration on day 1 to an unchanging routine 10 days later.

The vaulting environment is set up following the procedures in ["Setting Up a Vaulting Environment"](#). Briefly, the necessary steps are:

1. Add a storage location called `onsite_storage` corresponding to the fire-resistant closet.
2. Add a rotation policy called `catalog_recovery_rotation` with the following locations, events, and durations:

```
library : firstwrite : 4 hours
onsite_storage : arrival : 1 week
Media_Recycle_Bin : arrival : disabled
```

3. Associate rotation policy `catalog_recovery_rotation` with the default media family `OSB-CATALOG-MF`.
4. Schedule a daily vaulting scan for both `library` and `onsite_storage` at 0600.

Table 11-1 Inauguration of a Simple Vaulting Environment

Day	Time	Event
1	0000	An Oracle Secure Backup catalog recovery backup starts. The tape library moves a writable volume from a storage element to a tape drive and labels it <code>OSB-CATALOG-MF-000001</code> .
1	0600	An Oracle Secure Backup vaulting scan starts. Because 6 hours have elapsed since the first write to <code>OSB-CATALOG-MF-000001</code> , it is eligible to be moved. If that first write has completed, then a pending media movement job is created for the volume.
1	0800	The Oracle Secure Backup operator checks the Web tool Manage: Jobs page and finds a media movement job for <code>OSB-CATALOG-MF-000001</code> . The operator runs the job.
1	0815	The operator goes to the Web tool Manage: Pick and Distribution Reports page and reviews the distribution report for <code>OSB-CATALOG-MF-000001</code> .

Table 11-1 (Cont.) Inauguration of a Simple Vaulting Environment

Day	Time	Event
1	0830	The operator retrieves OSB-CATALOG-MF-000001 from the tape library import/export element, attaches the distribution report to it, and takes it to the fire-resistant closet (onsite_storage).
2-7	n/a	The events of days 2 through 7 are identical to the day 1 events, except that the volume being written to and moved from the library to storage increments from OSB-CATALOG-MF-000002 to OSB-CATALOG-MF-000007. The number of volumes at the storage location rises from 2 on day 2 to 7 on day 7.
8	0000	An Oracle Secure Backup catalog recovery backup starts. The tape library moves an unlabeled volume from a storage element to a tape drive and labels it OSB-CATALOG-MF-000008.
8	0600	An Oracle Secure Backup vaulting scan starts. A pending media movement job is created for OSB-CATALOG-MF-000008. OSB-CATALOG-MF-000001 has been in storage for 6 days and 22 hours. It is not quite eligible for rotation.
8	0800	The Oracle Secure Backup operator checks the Web tool Manage: Jobs page and finds a media movement jobs for OSB-CATALOG-MF-000008. The operator runs the job.
8	0815	The operator goes to the Web tool Manage: Pick and Distribution Reports page and prints a distribution report for OSB-CATALOG-MF-000008.
8	0830	The operator retrieves OSB-CATALOG-MF-000008 from the tape library import/export element, attaches the distribution report to it, and takes it to the fire-resistant closet (onsite_storage). The storage location now houses 8 volumes.
9	0000	An Oracle Secure Backup catalog recovery backup starts. The tape library moves an unlabeled volume from a storage element to a tape drive and labels it OSB-CATALOG-MF-000009.
9	0600	An Oracle Secure Backup vaulting scan starts. A pending media movement job is created for OSB-CATALOG-MF-000009. A second media movement job is created for OSB-CATALOG-MF-000001, because seven days have elapsed since its arrival at the fire-resistant closet (onsite_storage).
9	0800	The Oracle Secure Backup operator checks the Web tool Manage: Jobs page and finds media movement jobs for OSB-CATALOG-MF-000009 and OSB-CATALOG-MF-000001. The operator runs both jobs.
9	0815	The operator goes to the Web tool Manage: Pick and Distribution Reports page and prints a distribution report for OSB-CATALOG-MF-000009.
9	0830	The operator retrieves OSB-CATALOG-MF-000009 from the tape library import/export element, attaches the distribution report to it, and takes it to the fire-resistant closet (onsite_storage). The operator retrieves OSB-CATALOG-MF-000001 and imports it to the tape library. The number of volumes at the storage location remains at 8.
10+	n/a	By day 10, the vaulting environment has reached a steady state. Every day follows the same routine as day 9. The only change from day to day is a one-digit increment in the volume name.

Managing an Existing Vaulting Environment

This section provides step-by-step instructions for editing, renaming, and deleting objects in an existing Oracle Secure Backup vaulting environment.

This section contains these topics:

- [Managing Locations](#)

- [Managing Rotation Policies](#)
- [Managing Rotation Policy/Media Family Associations](#)
- [Managing Vaulting Scan Schedules](#)
- [Managing Volume Duplication Policies](#)
- [Managing Volume Duplication Policy and Media Family Associations](#)
- [Managing Volume Duplication Windows](#)
- [Managing Volume Duplication Schedules](#)
- [Changing Global Vaulting Policies](#)
- [Changing Global Volume Duplication Policies](#)



See Also:

"[Changing Volume Properties](#)" for instructions on moving a volume from one location to another or changing its rotation policy

Managing Locations

This section provides step-by-step instructions for editing, removing, and renaming an existing storage location.



See Also:

Oracle Secure Backup Installation and Configuration Guide for more information about editing an active location

This section contains these topics:

- [Editing or Viewing the Properties of a Storage Location](#)
- [Removing a Storage Location](#)
- [Renaming a Storage Location](#)

Editing or Viewing the Properties of a Storage Location

After you have set up a storage location, you might want to change one or more of its settings. For example, if a vaulting vendor adds support for Iron Mountain FTP notification, you could edit your storage location to change its notification type.

To edit or view storage location properties:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Locations**.
The Configure: Locations page appears.

4. Select a storage location whose properties you want to edit or view and click **Edit**.
The Configure: Locations > *location_name* page appears.
5. Make whatever changes you want.
6. Click **OK**.
The Configure: Locations page displays a success message.

Removing a Storage Location

You can use the Web tool to remove a storage location. A location referenced by a rotation policy cannot be deleted. The reference to the location from the rotation policy must be removed before the location can be deleted. Also, a location that contains volumes managed by Oracle Secure Backup cannot be deleted. Those volumes must be relocated before the location can be deleted.



See Also:

"[Managing Rotation Policies](#)" for instructions on removing a storage location from a rotation rule

To remove a storage location:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Locations**.
The Configure: Locations page appears.
4. Select the storage location you want to remove and click **Remove**.
A confirmation page appears.
5. Click **Yes**.
The Configure: Locations page displays a success message, and the selected storage location no longer appears in the list of locations.

Renaming a Storage Location

You can use the Web tool to rename a storage location. Note that renaming has consequences because Oracle Secure Backup assigns a **UUID** to each location object. All internal references use the UUID rather than the location name. If you change the name of a location, then all rotation policies that reference this name are updated.

To rename a storage location:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Locations**.
The Configure: Locations page appears.

4. Select a storage location whose name you want to change and click **Rename**.
A different page appears.
5. Enter the different name in the **Change *location_name* to** field and click **Yes**.
The Configure: Locations page displays a success message, and the storage location appears with its different name in the list of locations.

Managing Rotation Policies

This section provides step-by-step instructions for editing, removing, and renaming an existing rotation policy.

This section contains these topics:

- [Editing or Viewing the Properties of a Rotation Policy](#)
- [Removing a Rotation Policy](#)
- [Renaming a Rotation Policy](#)

Editing or Viewing the Properties of a Rotation Policy

You can use the Web tool to edit or view the properties of an existing rotation policy. You must have the `modify administrative domain's configuration` right to change the rotation policy.

To edit or view rotation policy properties:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Rotation Policies**.
The Configure: Rotation Policies page appears.
4. Select the rotation policy whose properties you want to view or edit and click **Edit**.
The Configure: Rotation Policy > *policy_name* page appears.
5. To add a rotation rule to the selected rotation policy:
 - a. Select a location from the **Location** list.
 - b. Select an event from the **Event** list.
 - c. Enter a number in the **Duration** field and select a unit of measurement from the adjoining list.
 - d. Select a position in the rotation policy for this rotation rule in the **Insert into position** list.
The first rotation rule in a rotation policy must specify an active location.
 - e. Click **Add**.



See Also:

["Adding Rotation Policies"](#) for more information about rotation rules

6. To remove a rotation rule from the selected rotation policy, select it in the list of rotation rules and click **Remove**.
A location can be removed from a rotation policy if no volumes are currently at that location.
7. To add a descriptive comment to the selected rotation policy, enter text in the **Comments** field and click **Apply**.

Removing a Rotation Policy

You can use the Web tool to remove an existing rotation policy. You must have the `modify administrative domain's configuration` right to remove a policy.

To remove a rotation policy:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Rotation Policies**.
The Configure: Rotation Policies page appears.
4. Select the rotation policy you want to remove and click **Remove**.
A confirmation page appears.
5. Click **Yes**.
The Configure: Rotation Policies page appears with a success message, and the selected rotation policy no longer appears in the Rotation Policies list.

Renaming a Rotation Policy

You can use the Web tool to rename an existing rotation policy. You must have the `modify administrative domain's configuration` right to rename the rotation policy.

To rename a rotation policy:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Rotation Policies**.
The Configure: Rotation Policies page appears.
4. Select the rotation policy you want to rename and click **Rename**.
A different page appears.
5. Enter the different name in the **Rename *policy_name* to** field and click **Yes**.
The Configure: Rotation Policies page displays a success message, and the selected rotation policy appears with its different name in the Rotation Policies list.

Managing Rotation Policy/Media Family Associations

You can remove the rotation policy associated with a media family or replace it with a different rotation policy. The rotation policy of volumes associated with the media family is changed as

well. Only those volumes still in their originating location have their rotation policy changed. The rotation policy of volumes that have moved out of their originating location is not changed.

To remove or change the rotation policy associated with a media family:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Basic section, click **Media Families**.
The Configure: Media Families page appears.
4. Select the media family whose rotation policy you want to remove or change and click **Edit**.
The Configure: Media Families > *family_name* page appears.
5. To remove the existing rotation policy, select none in the **Rotation policy** list and click **OK**.
The Configure: Media Families page displays a success message.
6. To replace the existing rotation policy, select a rotation policy from the **Rotation policy** list and click **OK**.
The Configure: Media Families page displays a success message.

Managing Vaulting Scan Schedules

This section provides step-by-step instructions for editing, removing, and renaming an existing vaulting scan schedule.

This section contains these topics:

- [Editing or Viewing the Properties of a Vaulting Scan Schedule](#)
- [Removing a Vaulting Scan Schedule](#)
- [Renaming a Vaulting Scan Schedule](#)

Editing or Viewing the Properties of a Vaulting Scan Schedule

You can use the Web tool to edit or view the properties of an existing vaulting scan schedule.

To edit or view the properties of a vaulting scan schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. Click **Schedule Vaulting Scan**.
The Manage: Schedule Vaulting Scan page appears.
4. Select the vaulting scan schedule you want to edit or view and click **Edit**.
The Manage: Schedule Vaulting Scan > *schedule_name* page appears.
5. Select **Disabled** to disable the vaulting scan schedule without deleting it. You might want to do this when removing a host from service for an extended period.
Select **Enabled** to enable a previously disabled vaulting scan schedule.

6. Make whatever other changes you want to the vaulting scan schedule priority, locations, media families, or comments.
Click **Triggers** to add or remove a vaulting scan schedule trigger.
7. Click **OK** to accept the changes.
The Manage: Schedule Vaulting Scan page displays a success message, and the edited schedule appears in the list of schedules.
8. Click **Cancel** to return to the Manage: Schedule Vaulting Scan page without changing anything.

Removing a Vaulting Scan Schedule

You can use the Web tool to remove an existing vaulting scan schedule.

To remove a vaulting scan schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. Click **Schedule Vaulting Scan**.
The Manage: Schedule Vaulting Scan page appears.
4. Select the vaulting scan schedule you want to remove and click **Remove**.
A confirmation page appears.
5. Click **Yes**.
The Manage: Schedule Vaulting Scan page displays a success message. The selected schedule no longer appears in the list of schedules.

Renaming a Vaulting Scan Schedule

You can use the Web tool to rename an existing vaulting scan schedule.

To rename a vaulting scan schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. Click **Schedule Vaulting Scan**.
The Manage: Schedule Vaulting Scan page appears.
4. Select the vaulting scan schedule you want to rename and click **Rename**.
A different page appears.
5. Enter the different name for the schedule in the **Rename *schedule_name* to** field and click **Yes**.
The Manage: Schedule Vaulting Scan page displays a success message, and the selected schedule appears in the list of schedules with its different name.

Managing Volume Duplication Policies

This section provides step-by-step instructions for editing, removing, and renaming an existing duplication policy.

This section contains these topics:

- [Editing or Viewing the Properties of a Volume Duplication Policy](#)
- [Removing a Volume Duplication Policy](#)
- [Renaming a Volume Duplication Policy](#)

Editing or Viewing the Properties of a Volume Duplication Policy

If a duplication policy is modified, then the policy settings that apply to a duplication job are the settings at the time the job runs, not the time when the job was created. The change in policy does not apply to existing duplicates.

To edit or view the properties of an existing volume duplication policy:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Volume Duplication Policies**.
The Configure: Volume Duplication Policies page appears.
4. Select the volume duplication policy you want to edit or view and click **Edit**.
The Configure: Volume Duplication Policies > *policy_name* page appears.
5. Make whatever changes you want to the duplication policy and click **OK**.
 - a. To remove an existing duplication rule, select it in the **Duplication rule(s)** list and click **Remove**.
 - b. To add a duplication rule, select a media family from the **Media family** list, enter a value in the **Number of duplicates** field, and click **Add**.

The Configure: Volume Duplication Policies page displays a success message, and the edited duplication policy appears in the list.

Removing a Volume Duplication Policy

A duplication policy that is associated with one or more media families cannot be removed. The media families must first be updated to remove the references to the duplication policy.

To remove an existing volume duplication policy:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Media Life Cycle section, click **Volume Duplication Policies**.
The Configure: Volume Duplication Policies page appears.
4. Select the duplication policy you want to remove and click **Remove**.

A confirmation page appears.

5. Click **Yes**.

The Configure: Volume Duplication Policies page displays a success message, and the selected duplication policy no longer appears in the list of duplication policies.

Renaming a Volume Duplication Policy

You can use the Web tool to rename an existing volume duplication policy.

To rename a volume duplication policy:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Media Life Cycle section, click **Volume Duplication Policies**.

The Configure: Volume Duplication Policies page appears.

4. Select the duplication policy you want to rename and click **Rename**.

A different page appears.

5. Enter the different name in the **Rename *policy_name* to** field and click **Yes**.

The Configure: Volume Duplication Policies page displays a success message. The selected duplication policy appears in the list of policies with its different name.

Managing Volume Duplication Policy and Media Family Associations

You can use the Web tool to remove or change the rotation policy associated with a media family.

To manage duplication and media family associations:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Basic section, click **Media Families**.

The Configure: Media Families page appears.

4. Select the media family whose volume duplication policy you want to remove or change and click **Edit**.

The Configure: Media Families > *family_name* page appears.

5. To remove the existing volume duplication policy, select none in the **Volume duplication policy** list and click **OK**.

The Configure: Media Families page displays a success message.

6. To replace the existing volume duplication policy, select a different volume duplication policy from the **Rotation policy** list and click **OK**.

The Configure: Media Families page displays a success message.

Managing Volume Duplication Windows

This section provides step-by-step instructions for removing a volume duplication window. You cannot edit an existing volume duplication window. If you want a longer volume duplication window, you can either remove and replace the existing window or simply add a second window with the extra hours you want. If you want a shorter volume duplication window, however, you must remove and replace the existing duplication window. For instructions on adding a volume duplication window, see "[Adding Volume Duplication Windows](#)".

Note:

If you add a volume duplication window that is identical to an existing window except for its time range, then the Configure: Volume Duplication Windows page displays only the additional time range appended to the existing volume duplication window.

To remove a volume duplication window:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.

The Configure page appears.

3. In the Advanced section, click **Volume Duplication Windows**.

The Configure: Volume Duplication Windows page appears.

4. Select the volume duplication window you want to remove and click **Remove**.

A confirmation page appears.

5. Click **Yes**.

The Configure: Volume Duplication Windows page displays a success message, and the selected volume duplication window no longer appears in the list of windows.

Note:

If you have two or more duplication windows that differ only in their time ranges, then you cannot remove just one of them. You must remove all of them and then re-create the duplication windows you want to keep.

Managing Volume Duplication Schedules

This section provides step-by-step instructions for editing, removing, and renaming an existing volume duplication schedule.

This section contains these topics:

- [Editing or Viewing the Properties of a Volume Duplication Schedule](#)
- [Removing a Volume Duplication Schedule](#)
- [Renaming a Volume Duplication Schedule](#)

Editing or Viewing the Properties of a Volume Duplication Schedule

You can use the Web tool to edit or view the properties of a volume duplication schedule.

To edit or view the properties:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Schedule Volume Duplication**.
The Manage: Schedule Volume Duplication page appears.
4. Select the volume duplication schedule you want to edit or view and click **Edit**.
The Manage: Schedule Volume Duplication > *schedule_name* page appears.
5. Make whatever changes you want to the volume duplication policy and click **OK**.
The Manage: Schedule Volume Duplication page displays a success message. The edited volume duplication schedule appears in the list.

Removing a Volume Duplication Schedule

You can use the Web tool to remove a volume duplication schedule.

To remove a volume duplication schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Schedule Volume Duplication**.
The Manage: Schedule Volume Duplication page appears.
4. Select the volume duplication schedule you want to remove and click **Remove**.
A confirmation page appears.
5. Click **Yes**.
The Manage: Schedule Volume Duplication page displays a success message, and the selected volume duplication schedule no longer appears in the list of schedules.

Renaming a Volume Duplication Schedule

You can use the Web tool to rename a volume duplication schedule.

To rename a duplication schedule:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Schedule Volume Duplication**.
The Manage: Schedule Volume Duplication page appears.

4. Select the volume duplication schedule you want to rename and click **Rename**.

A different page appears.

5. Enter the different name for the volume duplication schedule in the **Rename *schedule_name* to** field and click **Yes**.

The Manage: Schedule Volume Duplication page displays a success message, and the selected volume duplication schedule appears with its different name in the list of schedules.

Changing Global Vaulting Policies

You can use the following global policies to control how Oracle Secure Backup performs vaulting:

- `autovolumerelease`
Set the `autovolumerelease` policy to `yes` to automatically release recalled volumes when restore jobs requiring those volumes have completed. Only volumes automatically recalled by Oracle Secure Backup are released. The default value is `no`.
- `customeridstring`
Use the `customeridstring` 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.
- `invretrydelay`
Use the `invretrydelay` policy to dictate the duration that Oracle Secure Backup waits before retrying an export operation or inventory operation (to verify that a volume has been physically removed from a library). This policy has a default value of 2 minutes.
- `maxinvretrytime`
Use the `maxinvretrytime` policy to define the maximum duration for which the media movement job will continue retrying the export or inventory operation. This policy has a default of 15 minutes. After this duration is completed, Oracle Secure Backup places the job in an "input required" state. The job waits for user intervention. Oracle Secure Backup sends an alert email to the email recipients in the location object.
As an example, suppose that the `invretrydelay` and `maxinvretrytime` policies are set to their default values. The Oracle Secure Backup media manager attempts to export a volume to an `iee` slot according to the automatic ejection mode, but does not find a vacant slot. Oracle Secure Backup retries the export every 2 minutes. Oracle Secure Backup continues trying for 15 minutes, at which time the job requires user input to progress further.
- `minwritablevolumes`
Use the `minwritablevolumes` policy to specify the minimum number of writable volumes that must always be available in each tape library. 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.
- `reportretaintime`
Use the `reportretaintime` policy to define how long vaulting reports (`pick/distribution`) are retained. The default value is `7days`.

To change global vaulting policies:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.
3. In the Advanced section, click **Defaults and Policies**.
The Configure: Defaults and Policies page appears.
4. In the Policy column, click **vaulting**.
The Configure: Defaults and Policies > Vaulting page appears as shown in [Figure 11-4](#).

Figure 11-4 Vaulting Policies

Name	Current Value	Reset to Default Value
Auto run media movement jobs	no	
Auto volume release	no	
Inv retry delay	2 minutes	
Max inv retry time	15 minutes	
Offsite customer ID		
Minimum writable volumes	0	
Report retain time	7 days	

5. Make whatever vaulting policy changes you want and click **OK**.
6. If you later want to reset a policy to its default value, select the option in the **Reset to Default Value** column for that policy.

Changing Global Volume Duplication Policies

You can use the following global policies to control how Oracle Secure Backup performs volume duplication:

- `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.
- `duplicationjobpriority`
Use the `duplicationjobpriority` policy to specify the priority of volume duplication jobs relative to other jobs. The default value is 200.

To change global volume duplication policies:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Web tool Home page, click **Configure**.
The Configure page appears.

3. In the Advanced section, click **Defaults and Policies**.
The Configure: Defaults and Policies page appears.
4. In the Policy column, click **duplication**.
The Configure: Defaults and Policies > Duplication page appears.
5. Make whatever volume duplication policy changes you want and click **OK**.
6. If you later want to reset a policy to its default value, select the option in the **Reset to Default Value** column for that policy.

Recovery Manager and Vaulting

Oracle Secure Backup vaulting is closely integrated with the Oracle Database 10g release 2 (10.2) and later [Recovery Manager \(RMAN\)](#) `restore database preview` and `restore database preview recall` commands. In Oracle Database 10g release 2 (10.2) and later, an RMAN restore fails immediately if it is determined that any needed volume is located at a storage location. You can use `restore database preview` to get the status of all volumes required for a restore, including volumes that are `AVAILABLE` but located remotely. You can use information from `restore database preview` to direct RMAN to avoid a restore if the volumes needed for the restore are at a storage location, as shown in the following example.

```

RMAN> startup force mount pfile=/jfersten_tstvw1/oracle/work/t_init1.ora ;
2> restore database preview;
3>

RMAN-06378: List of Backup Sets
RMAN-06379: =====
RMAN-06389: BS Key   Type LV Size          Device Type Elapsed Time Completion Time
RMAN-06390: -----
RMAN-06391: 5       Full   340.95M   SBT_TAPE    00:01:48    10-AUG-07
RMAN-06392:          BP Key: 5   Status: AVAILABLE Compressed: NO Tag: TAG20080810T150035
RMAN-06355:          Handle: 05ipls0j_1_1 Media: rmanvltfam-001,rmanvltfam-002,rmanvltfam-003,
RMAN-06335: List of Datafiles in backup set 5
RMAN-06336: File LV Type Ckp SCN    Ckp Time Name
RMAN-06337: ---- --
RMAN-06338: 1       Full 308037   10-AUG-07 /jfersten_tstvw1/oracle/dbs/t_dbl.f
RMAN-06338: 2       Full 308037   10-AUG-07 /jfersten_tstvw1/oracle/dbs/t_ax1.f

RMAN-08607: List of remote backup files
RMAN-06320: =====
RMAN-06355:          Handle: 05ipls0j_1_1 Media:
rmanvltfam-001,rmanvltfam-002,rmanvltfam-003,rmanvltfam-004RMAN-03091: Finished restore at 10-AUG-07

Recovery Manager complete.=====

```

The volumes `rmanvltfam-001`, `rmanvltfam-002`, `rmanvltfam-003`, and `rmanvltfam-004` are required for the restore but are not located in a library. They are remotely located and must be recalled.

You can use `restore database preview recall` to start a recall for all volumes needed for a restore that are currently at a storage location. This RMAN command translates into an Oracle Secure Backup media movement job. When the volumes have been recalled from storage, the `restore database preview` output for the same restore indicates that these volumes are now available on-site. A restore can be completed successfully at this point.

 **Note:**

The volumes recalled by `restore database preview recall` must be manually released to return to their rotation schedules even if the `autovolumerelease` policy is set to `yes`.

 **See Also:**

- ["Recalling a Volume"](#)
- *Oracle Secure Backup Reference* for more information about the `autovolumerelease` policy

The following example shows the output from a `restore database preview recall`, and `obtool` commands showing the results of the resulting media movement job.

```

RMAN> startup force mount pfile=/jfersten_tstvw1/oracle/work/t_init1.ora ;
2> restore database preview recall ;
3>
RMAN-06196: Oracle instance started
RMAN-06199: database mounted

Total System Global Area      134217728 bytes

Fixed Size                     1259552 bytes
Variable Size                  121636832 bytes
Database Buffers               8388608 bytes
Redo Buffers                   2932736 bytes

RMAN-03090: Starting restore at 10-AUG-07
RMAN-08030: allocated channel: ORA_SBT_TAPE_1
RMAN-08500: channel ORA_SBT_TAPE_1: sid=92 devtype=SBT_TAPE
RMAN-08526: channel ORA_SBT_TAPE_1: Oracle Secure Backup
RMAN-08030: allocated channel: ORA_DISK_1
RMAN-08500: channel ORA_DISK_1: sid=90 devtype=DISK

RMAN-06178: datafile 3 not processed because file is offline
RMAN-06378: List of Backup Sets
RMAN-06379: =====
RMAN-06389: BS Key   Type LV Size          Device Type Elapsed Time Completion Time
RMAN-06390: ----- -- -- -
RMAN-06391: 5           Full    340.95M    SBT_TAPE   00:01:48    10-AUG-07
RMAN-06392:          BP Key: 5   Status: AVAILABLE Compressed: NO Tag: TAG20080
810T150035
RMAN-06355:          Handle: 05ipls0j_1_1  Media: rmanvltfam-001,rmanvltfam-002,rmanvltfam-003,
RMAN-06335: List of Datafiles in backup set 5
RMAN-06336: File LV Type Ckp SCN      Ckp Time Name
RMAN-06337: ---- -- -- -
RMAN-06338: 1           Full 308037    10-AUG-07 /jfersten_tstvw1/oracle/dbs/t_db1.f
RMAN-06338: 2           Full 308037    10-AUG-07 /jfersten_tstvw1/oracle/dbs/t_ax1.f
RMAN-12016: using channel ORA_SBT_TAPE_1
RMAN-12016: using channel ORA_DISK_1

RMAN-05035: archive logs generated after SCN 308037 not found in repository
RMAN-05033: Media recovery start SCN is 308037

```

```

RMAN-05034: Recovery must be done beyond SCN 308037 to clear data files fuzzines
s
RMAN-08608: Initiated recall for the following list of remote backup files
RMAN-07524: =====
RMAN-06355:          Handle: 05ip1s0j_1_1   Media:
rmanvltfam-001,rmanvltfam-002,rmanvltfam-003,rmanvltfam-004
RMAN-03091: Finished restore at 10-AUG-07
=====

```

RMAN has completed the `restore database preview recall` command. Oracle Secure Backup has created a media movement job for the remote volumes requested by RMAN. If the `autorunmmjobs` policy is set to `no`, then that job is in a pending state and must be started by the Oracle Secure Backup operator. An `lsjob` command returns the following information about this media movement job:



See Also:

Oracle Secure Backup Reference for more information about the `autorunmmjobs` policy

```

ob> lsjob --long --type mm
17:
Type:                media movement for TrustyVaultsInc
Volumes:             rmanvltfam-001 rmanvltfam-002 rmanvltfam-003 rmanvltfam-004
Scheduled time:     none
State:              pending enable by operator
Priority:           100
Run on host:       (administrative server)
Attempts:          0

```

A `catrpt` command displays the distribution report for this media movement job:

```

ob> catrpt --type dist 17
                Oracle Secure Backup Distribution List Report
                Location - TrustyVaultsInc

Volume ID      Barcode                               Move Date      Next Loc
-----
rmanvltfam-001 b1ee571429f5102ad52000cf1ce8d3a 2008/8/10      vlibrman
rmanvltfam-002 b22b696a29f5102ad52000cf1ce8d3a 2008/8/10      vlibrman
rmanvltfam-003 b26873be29f5102ad52000cf1ce8d3a 2008/8/10      vlibrman
rmanvltfam-004 b39fbf9429f5102a9f0000cf1ce8d3a 2008/8/10      vlibrman

```

The media movement job is in a pending state. The operator can run the media movement job with a `runjob` command:

```
ob> runjob --mediamovement --now 17
```

In releases before Oracle Database 10g release 2 (10.2), an RMAN restore operation requiring volumes currently at a storage location results in a corresponding Oracle Secure Backup restore job. The Oracle Secure Backup scheduler also starts a media movement job to recall the volumes from storage. The restore job waits in a `pending` state until all the required volumes have been successfully recalled.

Each storage location can be associated with a recall time. This is the time taken to recall a volume from this location. If this recall time exceeds the resource wait time configured for this restore job, then the recall operation is not started and the restore job fails.

You can also recall stored volumes needed for an RMAN restore with the `recallvol` command in `obtool` or with the Oracle Secure Backup Web tool, as described in "Recalling a Volume".

 **See Also:**

- "Adding Locations" for instructions on setting a recall time for a storage location
- *Oracle Secure Backup Reference* for complete `recallvol` syntax and semantics

Troubleshooting Vaulting

This section discusses two problems that can surface in a vaulting environment. It also suggests what to do if you encounter these problems.

Misplaced Volumes

There are any number of reasons a volume might not be at the location currently recorded for it in the Oracle Secure Backup catalog:

- The wrong volume is removed from a tape library for transportation to a storage location
- The wrong volume is returned from a storage location
- Two or more media movement jobs are occurring simultaneously, their distribution lists are interchanged, and they are transported to the wrong locations
- A volume is lost or destroyed en route to or returning from a storage location

If a volume is manually removed from an active or storage location and misplaced, then Oracle Secure Backup does not flag it as misplaced. The Oracle Secure Backup catalog still shows it as residing in its former location. Its misplaced status is not discovered until it next becomes eligible for inclusion in a media movement job. In this case the volume is misplaced, but it is still somewhere in your administrative domain. Finding it might require a complete volumes inventory or physical search.

If the wrong volume is returned from a storage location, then two volumes are misplaced simultaneously. For example, suppose Oracle Secure Backup creates a media movement job to move `vol000001` from storage to its `Media_Recycle_Bin`. But if `vol000002` gets moved instead, then the Oracle Secure Backup catalog shows `vol000001` in the `Media_Recycle_Bin` when it is really still at the storage location. Worse, it shows `vol000002` at the storage location when it is really in the `Media_Recycle_Bin`. In this case the volumes are still somewhere in your administrative domain, but one of them (`vol000002` in this example) is in danger of being overwritten by mistake. You can guard against this by requiring that all volumes be accompanied by distribution reports when moving between locations.

A volume misplaced en route to a storage location is arguably the worst case. The volume is no longer in your administrative domain, and you do not know it has been misplaced until Oracle Secure Backup generates the next media movement job for it. This next media movement job might be months after the volume is misplaced. You can guard against this case by generating two distribution reports for each media movement job: one distribution report accompanies the volume to the storage location, while the other is transmitted by itself to the storage location operator. If the storage location operator receives a distribution report but not a matching volume, then the operator knows immediately that a volume has been misplaced en route.

**See Also:**

["Viewing Pick and Distribution Reports"](#)

Volumes Outside Their Rotation Policies

Volumes are associated with rotation policies. Volumes inherit rotation policies from their media families. If you change the rotation policy associated with a media family, then the different policy applies to all volumes that belong to the media family and have not left their originating locations. The different rotation policy does not apply to volumes that belong to the media family but are not at their originating location.

**Note:**

A volume can also be assigned to a different rotation policy with the `chvol --rotationpolicy` command.

If the different rotation policy includes all locations included in the old policy, then there is no problem with volumes that have left their originating locations. But if the different rotation policy omits one or more locations, then all volumes in the newly omitted locations at the time of the policy change are stranded. Oracle Secure Backup does not create media movement jobs for these volumes, because it does not look for them in the omitted locations.

Stranded volumes must be moved to a location specified in the different rotation policy with the Oracle Secure Backup Web tool Manage: Volumes page. These stranded volumes appear in the volume exception report.

**See Also:**

["Associating Rotation Policies with Media Families"](#)

Viewing Exception Reports

An exception report lists the 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.

To generate an exception report:

1. Follow the steps in ["Displaying the Oracle Secure Backup Web Tool Home Page"](#).
2. From the Oracle Secure Backup Web tool Home page, click **Manage**.
The Manage page appears.
3. In the Media Life Cycle section, click **Location Reports**.
The Manage: Location Reports page appears as shown in [Figure 11-5](#).

Figure 11-5 Location Reports Page

Home Configure **Manage** Backup Restore

Manage: Location Reports

View Report Type location In Transit

Location	Comment
Media_Recycle_Bin	OSB-generated location
lib1	OSB-generated location for library lib1

4. Select exception in the **Type** list and click **View Report**.

This report identifies volumes that are not in the locations currently recorded in the Oracle Secure Backup catalog. This includes volumes whose location is unknown, volumes in the wrong tape library, and expired volumes still in rotation.

Managing Backup Encryption

Backup Encryption is an optional and easily configurable mechanism which ensures that all client data that Oracle Secure Backup writes to a backup container is encrypted. Backup encryption can be performed for both file-system data and [Recovery Manager \(RMAN\)](#) generated backups.

**Note:**

Encryption is not supported during volume duplication or volume migration. Unencrypted backup sections on a volume cannot be encrypted during a volume duplication or volume migration operation. For more information about volume duplication and volume migration, see [Vaulting](#) .

This chapter contains these sections:

- [Overview of Backup Encryption](#)
- [Overview of Software-Based Encryption](#)
- [Overview of Hardware-Based Encryption](#)
- [Example: Performing a One-Time Unencrypted Backup](#)
- [Example: Performing Day-to-Day Backup Encryption](#)
- [Example: Performing Transient Backup Encryption](#)
- [Enabling Backup Encryption](#)

Overview of Backup Encryption

Data is vital to an organization and it must be guarded against malicious intent while it is in an active state, on production servers, or in preserved state, on backup tapes. Data center security policies enable you to restrict physical access to active data. To ensure security of backup data stored on tapes, Oracle Secure Backup provides backup encryption.

You can encrypt data at the global level, client level, and job level by setting appropriate encryption policies. You can select the required algorithm and encryption options to complete the encryption process.

This section consists of the following topics, that explain backup encryption in detail:

- [Types of Backup Encryption](#)
- [About Backup Encryption Policies](#)
- [About Backup Encryption Setting Levels](#)
- [About Backup Encryption Options](#)
- [About Backup Encryption Algorithms](#)
- [About Backup Encryption Security Control](#)

- [About Backup Encryption Key Management](#)
- [About Backup Encryption for File-System Backups](#)
- [About Backup Encryption for Oracle Database Backups](#)

Types of Backup Encryption

Oracle Secure Backup enables you to perform the following types of encryption:

- Software encryption

Software encryption is supported for hosts that have the Oracle Secure Backup software installed. It is not supported for NDMP hosts or NAS filers. The data that is backed up is encrypted before it is sent over the network to the backup storage media.

When you use software encryption for a backup, all backup image instances associated with this backup are encrypted. If software encryption is not enabled at the time the backup is created, you can encrypt a backup image instance created using the original unencrypted backup if this backup image instance is being stored in a tape device that supports hardware encryption.

See Also:

Oracle Secure Backup Reference for more information about backup encryption when copying backup image instances

- Hardware encryption

Hardware encryption is supported only for tape devices that support encryption such as the LTO5 tape drive. The tape device hardware performs the required data encryption.

If a backup that uses hardware encryption is copied to a disk pool, the backup image instance on the disk pool is unencrypted. However, if a backup is created using software encryption, you cannot use hardware encryption for backup image instances created using this backup.

See Also:

["Overview of Hardware-Based Encryption"](#)

About Backup Encryption Policies

Backup encryption is designed to be easy to implement. In the simplest scenario, you change one global policy to ensure that all data from each client is encrypted. Backup encryption also offers a large degree of configuration flexibility.

To set encryption at the global level or for a specific client, set the encryption policy to one of the following values:

- `required`

All data coming from this backup domain or client must be encrypted.

- `allowed`

All data coming from this backup domain or client may be encrypted. The decision to encrypt is deferred to the next lower priority level. This is the default setting.

About Backup Encryption Setting Levels

You can specify encryption settings at the following levels, from highest to lowest precedence. The encryption policies are explained under "[About Backup Encryption Policies](#)"

1. Global

If backup encryption is set to `required` at the global level, then all backup operations within the administrative domain will be encrypted. This global policy is defined using Oracle Secure Backup defaults and policies.

2. Client

If the host encryption setting is `required`, then all backup operations on the host will be encrypted regardless of whether or not encryption was configured at the backup level. If the host encrypted setting is `allowed`, then backups on the host will not be encrypted unless configured as part of the backup job itself or if the global encryption policy is set to `required`.

3. Job

If the host and global encryption policies are set to `allowed`, then backup encryption will only be performed if it is configured at the backup level.

An encryption setting specified at a higher level always takes precedence over a setting made at a lower level. For example, if you enable backup encryption at the global level, and your file-system backup job disables encryption, then the backup is still encrypted because the setting at the higher level (global level) takes precedence.

About Backup Encryption Options

While enabling encryption for backups, you can select one of the following options:

- **yes**
This option specifies that the backup is encrypted.
- **no**
This option specifies that the backup is not encrypted. This is the default setting.
- **forced off**
This option specifies that the backup is not encrypted, overriding the host-required encryption setting
- **transient**
This option specifies a backup encrypted by Oracle Secure Backup with a user-supplied one-time passphrase. If you select this option, then you must also select an encryption algorithm option and enter a passphrase in the **specify passphrase** field.

A client `rekeyfrequency` policy defines when a different key is generated. For example, the policy might require that a different set of keys be generated every 30 days. Older keys are retained in a wallet-protected key store. This ensures that if a key or `wallet` and the associated backup tape are compromised, then only older data could be unencrypted. The default `rekeyfrequency` policy for a client is inherited from the global `rekeyfrequency` policy.

About Backup Encryption Algorithms

The encryption algorithm is inherited from the global default policy and can be overridden at the client level. Each client can use a different encryption algorithm. For example, a payroll computer can use a higher level of encryption than a test lab computer. The supported encryption algorithms are:

- AES128
- AES192
- AES256



See Also:

"[About Hardware Encryption Algorithm](#)" for more information about hardware encryption options

About Backup Encryption Security Control

Oracle Secure Backup provides an interwoven encryption security model that mainly controls user-level access, host authentication, and key management. Once backup encryption is enabled, all data is encrypted using the defined encryption algorithm. The data is encrypted before it leaves the client. The encryption keys are stored in a mechanism that is protected by the Oracle Secure Backup [wallet](#).

The administrative server is considered a secure host. All keys and wallet-protected key stores for all clients are stored on this protected computer. When a backup or restore job is started, the encryption key is passed over a [SSL](#) connection to the client that is encrypting or decrypting data. The encryption keys are retained in memory only so long as needed to perform the encryption or decryption.

The encrypted key stores are extremely valuable, because they enable encryption and decryption of all tapes. If the key stores are lost, then all data would also be lost. Best practise is to schedule frequent catalog backups of your Oracle Secure Backup administrative server using the `OSB-CATALOG-DS` dataset provided as this includes a backup of you key stores. The encrypted key store format is platform independent.

Backups of Oracle Secure Backup administrative data must not be encrypted with an automatically generated key. If they were, and if the administrative server were destroyed, then recovering the decryption key used to encrypt the encryption keys would be difficult. For this reason, making a transient backup of the administrative server tree is better.

About Backup Encryption Key Management

Keys can be generated either randomly, also called transparent keys, or with a passphrase. The suggested mode of operation and default value is automatic generation. Each newly created [client](#) gets an automatically generated key during the `mkhost` phase. This transparent key is added to the wallet-protected key store that is specific for this client, and it remains valid for encryption until:

- A key renewal event occurs
- The backup administrator manually renews an automatically generated key

- The backup administrator changes the key to a passphrase while providing a different passphrase

The passphrase is never stored anywhere. The hash of the passphrase and the key generated from the passphrase are stored in the encrypted store. Oracle Secure Backup does not enforce a minimum length for a passphrase.

Once the new key is created, it is added to the wallet-protected key store and marked as the active encryption key. Old encryption keys are left in the key store and used for automatic and seamless decryption of data. If clients are removed from the backup domain, then their key stores are still retained on the administrative server. This ensures that the backup administrator can always restore data no matter the age of the encrypted backup [volume set](#).

 **Note:**

There is one exception where a key is not automatically added to the key store. Keys for transient backups are effectively one-use keys and are not usually stored in the key store. You can override this behavior through a command line option. See "[About Transient Backup Encryption](#)" to learn more about transient backups.

When a key expires, a different key is automatically generated. For passphrase generated keys, however, there is some overhead for the backup administrator, who must type in a passphrase for each client that is using passphrase-generated keys. When a passphrase-generated key expires, Oracle Secure Backup generates a warning message stating that the backup administrator must update the passphrase for the stated client. This message is placed in the Oracle Secure Backup log files, the display output, and an email to the backup administrator.

About Backup Encryption for File-System Backups

For file-system backups, you can select encryption for the entire administrative domain, a specific client, or a specific backup job. To define encryption for a particular file-system backup job, you specify the encryption policy in the backup schedule that is associated with your file-system backup job. You can also configure encryption for on-demand backups of file-system data.

 **See Also:**

- "[Enabling Backup Encryption](#)"
- "[Adding an On-Demand Backup Request](#)"

About Backup Encryption for Oracle Database Backups

For Oracle Database backups, encryption can be specified for the administrative domain, a specific client, or a specific backup job. You specify encryption for a specific Oracle Database backup job using database backup storage selectors or through the Recovery Manager (RMAN) media management parameter `OB_ENCRYPTION`. The encryption algorithm that Oracle Secure Backup uses depends on the algorithm configured for the Oracle Secure Backup host.

 **See Also:**

"[Adding a Database Backup Storage Selector](#)" for information about defining backup storage selectors

For a particular Oracle Database backup job, settings made using the `OB_ENCRYPTION` parameter override the settings made using the database storage selector associated with the backup job.

If the RMAN data from the SBT is encrypted, then Oracle Secure Backup performs no further encryption. RMAN encryption satisfies a host or global `required` encryption setting within Oracle Secure Backup. For example, if a host is configured with encryption `required` and the backup was encrypted by RMAN, then Oracle Secure Backup does not re-encrypt the backup because the host encryption `required` configuration has been met. For RMAN encrypted backups, the encryption keys are managed by the database so the host encryption key settings configured within Oracle Secure Backup would not apply.

If a host is configured for encryption `required`, and if RMAN backup encryption is disabled, then Oracle Secure Backup encrypts the RMAN backups using Oracle Secure Backup encryption based on the host encryption configuration.

Values for RMAN Parameter `OB_ENCRYPTION`

You can set the following values for the `OB_ENCRYPTION` parameter:

- `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`. Setting `OB_ENCRYPTION` to `OFF` is equivalent to specifying no value for it.
- `FORCEDOFF`
Oracle Secure Backup does not encrypt the database backup, overriding any host or domain encryption settings that are set to `required`. 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.

 **See Also:**

Oracle Database Backup and Recovery User's Guide for more information

Overview of Software-Based Encryption

Oracle Secure Backup provides policy-based backup encryption securing the backup data on tape whether the tapes are onsite, offsite, or lost. This section explains backup encryption for different types of backups monitored by encryption policies.

About Transient Backup Encryption

In some cases you may need to back up a set of data from backup domain Site A and restore it at backup domain Site B. The backup set might contain backup files for several clients. Each client backup file is encrypted to a client-specific encryption key, which was probably used in recent backups at Site A. For Site B to decrypt the data, you would have to collect all keys used in encrypting the data at Site A and then ship those keys to Site B.

This scenario would be a serious threat to security because these keys were used in other recent backups. Oracle Secure Backup enables cross-site backup encryption without this security threat by encrypting data at the volume set level for a given backup job. The key for volume set encryption is based on a passphrase. The data is encrypted against this passphrase-generated key for all clients that are part of this backup job. The backup administrator of Site A gives the passphrase and encryption algorithm used to Site B. The passphrase and encryption algorithm are provided when Site B does the restore operation, and the data can be decrypted.

In all other cases, the encryption keys for backup encryption are automatically added to the appropriate wallet-protected key store. A transient key, however, is a one-time key used mainly for moving data to a remote location. Transient encryption keys, therefore, are not stored in the protected key stores by default. Oracle Secure Backup does provide an option to the backup administrator to store the transient encryption key in the key store.

Oracle Secure Backup supports transient passphrase encryption only for file-system backups. For Oracle Databases, use RMAN to create and restore transient passphrase encrypted backups.

See Also:

- ["Enabling Transient Backup Encryption"](#) for information about the steps to encrypt transient backups
- *Oracle Database Backup and Recovery Reference* for information about creating encrypted backups of Oracle Database by using password-based encryption

Overview of Hardware-Based Encryption

Oracle Secure Backup supports encryption of backup data using its commands or through RMAN but that can affect the system performance.

For encryption without performance impact, Oracle Secure Backup provides hardware-based encryption on select LTO and T10000 tape drive formats.

The LTO and T10000 interface to hardware encryption is implemented through the SCSI specification for hardware encryption. Other vendors offer similar hardware, and their products are certified for use with Oracle Secure Backup as they are tested and approved by Oracle.

Information about every tape device supported by Oracle Secure Backup is available at the following URL:

<http://www.oracle.com/technetwork/database/database-technologies/secure-backup/learnmore/index.html>

Hardware-based encryption brings no changes to the existing Oracle Secure Backup encryption model. You can enable hardware-based encryption at the policy, host, or backup job level within Oracle Secure Backup. The decisions, policies, key management, and settings for hardware-based encryption are similar to software-based encryption.

You select hardware-based encryption either by selecting the tape drive for a backup or by having nothing but the select tape drives in your Oracle Secure Backup administrative domain. Oracle Secure Backup turns on the encryption feature within the tape drive with SCSI commands and sends the encryption key to the tape drive. Encryption is performed by the LTO and T10000 drive formats in hardware instead of in software by Oracle Secure Backup. If a drive that supports hardware encryption is not found, or if there is no compatible tape in the drive, then the existing Oracle Secure Backup software encryption model is used.

 **Note:**

For drives in IBM libraries, you can use hardware-based encryption after you enable Application-Managed Encryption (AME), which is an IBM-specific protocol. For further details, contact your library vendor. If a drive is already configured to use another encryption method, such as Library-managed encryption or a key management system, then AME is not required for that drive.

If a drive that supports hardware encryption contains a compatible tape but needs an additional compatible tape to complete a backup, then Oracle Secure Backup looks for an additional LTO or T10000 tape. If it finds one, it mounts the supporting tape and continues with the backup. If Oracle Secure Backup cannot mount an additional compatible tape, then the job state shows as `Running` and requires the backup operator to intervene.

 **Note:**

If you perform a backup using hardware-based encryption, then you cannot restore using software-based encryption. Similarly, you cannot restore using hardware-based encryption, if you have performed the backup using software-based encryption.

About Hardware-Encrypted Transient Backups

You can disable hardware-based encryption on transient backups with the `--disablehardwareencryption` option of the `backup` command. This option forces Oracle Secure Backup to use software-based encryption for the backup.

You can also disable hardware encryption by setting the `enablehardwareencryption` backup encryption policy to `no`.

 **See Also:**

- *Oracle Secure Backup Reference* for complete syntax and semantics for the `backup` command
- ["About Transient Backup Encryption"](#)
- ["About Defaults and Policies"](#)

About Hardware Encryption Reports and Logging

Hardware-based encryption generates no additional reports or logs, but it does affect the following existing reports and logs:

- In any transcript, log, or report where Oracle Secure Backup shows encryption settings `on/off/forcedoff/rman`, hardware-based encryption adds `hardware` and `transient_hardware` settings for data that was encrypted by the selected tape drive.
- Job transcripts show encryption type and algorithm.
- Output of the `lssection --long` command includes encryption type.

Following is an example of the output of the `lssection` command:

```
ob> lssection --long
Backup section OID: 114
  Containing volume: passphrase-mf-000001
  Containing volume OID: 119
  File: 2
  Section: 1
  Backup level: 0
  Client: storabck34
  Encryption: hardware
  Algorithm: aes256
  Created: 2014/02/25.15:30
  Size: 1.9 MB
```

- Output of the `lsvol --long` command shows if a volume can be encrypted in a *Tape Attributes* field. Possible values are `unknown`, `hw encryptable`, and `not hw encryptable`. The `unknown` value persists until a tape is mounted and Oracle Secure Backup can determine if it supports hardware encryption.
- The `lsdev --long --geometry` command reports on the availability of hardware encryption.

About Hardware Encryption Algorithm

Oracle Secure Backup supports encryption algorithms AES128, AES192, and AES256 for software-based encryption. In addition to host-based software encryption, Oracle Secure Backup also supports tape drive hardware encryption for compatible tape formats like LTO and T10000 as listed on the Oracle Secure Backup tape drive compatibility device matrix. Oracle Secure Backup automatically chooses the AES256 algorithm while performing tape drive encryption. Oracle Secure Backup encryption key management is identical whether performing host-based software encryption or tape drive encryption.

When a hardware-encrypted backup job completes, the job transcript and all other reports display the AES256 encryption algorithm. The archive section database and the tape header also show that the AES256 algorithm was used for the encryption.

This behavior matters only when you do a hardware-encrypted transient backup and do not store the key. In this situation, you must supply the AES256 algorithm when doing a restore. If the `backup --store` option was used on a hardware-encrypted transient backup, then the algorithm is not needed.

See Also:

- *Oracle Secure Backup Reference* for complete syntax and semantics for the `backup` command
- "[About Transient Backup Encryption](#)"

About Hardware Encryption Policies

Hardware-based encryption in Oracle Secure Backup is controlled by two backup encryption policies:

- `enablehardwareencryption`

By default, Oracle Secure Backup automatically leverages tape drive encryption over host-based encryption. If the policy value is changed to `no`, then Oracle Secure Backup does software-based encryption instead of hardware based encryption.

- `requireencryptablemedia`

If this policy is set to its default value `no`, then Oracle Secure Backup first attempts to mount a tape capable of hardware encryption. If that is not possible, then Oracle Secure Backup falls back to software encryption. If the policy value is changed to `yes`, then Oracle Secure Backup puts the job into a pending state until a hardware-encryptable tape is made available.

This policy is ignored if the tape drive is incapable of hardware encryption or cannot identify encryption-capable tapes.

See Also:

"[Enabling Hardware Encryption](#)" for detailed information on the steps to enable hardware encryption.

Example: Performing a One-Time Unencrypted Backup

Oracle Secure Backup enables the backup administrator to do a one-time unencrypted backup without changing global or client encryption settings.

Suppose the backup administrator is planning to move all home directories from one host to another and does not want to copy files directly between these two hosts. The backup administrator wants instead to back up a [dataset](#) worth of data to a tape, restore it to another host, and immediately destroy the tapes or the contents of the tapes after the transfer. The backup administrator does not want to use encryption because of the processing overhead that occurs.

In this special case, the backup administrator can use the `backup --encryption forcedoff` command. This command overrides global and client encryption settings and performs an unencrypted backup. Transcripts and all other reports for this job then state that encryption was forcibly disabled for this backup set. There is a similar mechanism available to RMAN backups using the `OB_ENCRYPTION` variable from within RMAN.

See Also:

Oracle Secure Backup Reference for complete syntax and semantics of the `backup` command in `obtool`

Example: Performing Day-to-Day Backup Encryption

Encryption keys are generated automatically with a default AES256 encryption algorithm. The default initial global and client backup encryption policy settings are set as `allowed`.

If the backup administrator decides that the default configuration is sufficient for the enterprise, then no configuration is required. This section describes the configuration of a more complicated case.

The following depicts three classes of hosts namely, Developers, Payroll, and CEO. Each of these host requires a different type and amount of encryption.

- **Developers**
These clients require encryption only for source code backup operations in a dataset called `SourceCode`.
- **Payroll**
This client requires AES256 encryption with a different encryption key each week.
- **CEO**
This client requires all data to be encrypted using a passphrase-generated key.

The Developer clients require no changes in the setup. The backup administrator instead updates the backup job for the `SourceCode` dataset that is used to back up the developer computers. If a [backup schedule](#) does not exist, then the backup administrator creates a backup schedule with a `mksched` command:

```
mksched --dataset sourcecode --type backup --encryption yes SourceCode
```

If the backup schedule exists, then the backup administrator uses the `chsched` command with the same options specified.

The Payroll host requires changes to the default client policies and settings for the encryption algorithm, key regeneration time, and client encryption flags. The backup administrator makes these changes with a `chhost` command:

```
chhost -algorithm aes256 -encryption required -rekeyfrequency 1week Payroll
```

This ensures that all data from the payroll client is always encrypted to the AES256 algorithm with a different key encryption key each week.

For the CEO client, the default encryption is sufficient but the encryption key type required is passphrase-generated. To do this, the backup administrator runs the `chhost` command:


```
chhost --keytype passphrase TheBoss
```

The system prompts to enter the passphrase. After performing the initial configuration, there is minimal additional overhead managing backup encryption.

Since the keys are managed in the keystore internal to Oracle Secure Backup, do not enter the passphrase on the command line while restoring a backup. The `restore` command does not make any reference to this passphrase and the key management is transparent.

Host-based passphrase and transparent encryption do not differ in the way encryption is handled. The only difference is the manner in which the encryption keys were created.

The encryption state is displayed as part of the job transcript during a backup operation for both file system and RMAN backups.

Example: Performing Transient Backup Encryption

Oracle Secure Backup enables you to restore encrypted backups on different domains. For example, you encrypt a backup on domain A, you can restore this backup on domain B.

```
ob> backup --level full --at 2013/09/17.21:00 --priority 10 --privileged --encryption  
transient --algorithm aes128 --passphrase transient --dataset mydatasets1/test.ds --go  
Info: backup request 1 (dataset mydatasets1/test.ds) submitted; job id is admin/3.
```

Enabling Backup Encryption

Data is encrypted at the client level. Each client has its own set of keys. One key is the active key used for encrypting backups. Older keys are used to seamlessly restore older backups that were created with those keys.

Note:

Oracle Secure Backup does not encrypt backups of [NAS](#) devices. Oracle Secure Backup encryption is performed on the client host where Oracle Secure Backup software has been installed. Because backup software cannot be installed directly on NAS devices, [NDMP](#) is used for backup and restore operations.

See Also:

["About Catalog Import Encryption"](#) for more information about encrypting backup catalog data

Enabling Encryption for the Administrative Domain

To enable backup encryption at the global level, for the entire administrative domain:

1. Follow the steps in ["Displaying the Oracle Secure Backup Web Tool Home Page"](#).
2. From the Oracle Secure Backup Home page, click **Configure**.
The Configure page appears.
3. In the Advanced section, click **Defaults and Policies**.

The Configure: Defaults and Policies page appears.

4. In the Policy column, click **backupencryption**.

The Configure: Defaults and Policies: Backupencryption page appears.

5. For the Encryption property, select **required**.
6. For the Algorithm property, select one of the following options: aes128, aes192, or aes256.

 **See Also:**

"[About Backup Encryption Algorithms](#)" for information about the backup encryption algorithms

7. For the Key Type property, select one of the following: transparent or use passphrase.

 **See Also:**

"[About Backup Encryption Key Management](#)" for information about backup encryption key settings

Enabling Encryption for a Client

To enable backup encryption at the host level:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".
2. From the Oracle Secure Backup Home page, click **Configure**.

The Configure page appears.

3. In the Basic section, click **Hosts**.

The Configure: Hosts page appears.

4. Select the host for which you want to configure backup encryption and click **Edit**.
5. For the Encryption property, select **required**.
6. For the Algorithm property, select one of the following options: aes128, aes192, or aes256.

 **See Also:**

"[About Backup Encryption Algorithms](#)" for information about the backup encryption algorithms

7. For the Key Type property, select one of the following: transparent or use passphrase.

 **See Also:**

"[About Backup Encryption Key Management](#)" for information about backup encryption key settings

Encrypting Data for Backups

You can enable encryption at the backup level. The encryption settings at the backup level override the global encryption policy settings.

Enabling Encryption for a Scheduled Backup

1. Perform steps 1 to 5 under "[Adding a Backup Schedule](#)".
2. For **Encryption**, select Yes.
3. Perform steps 6 to 8 under "[Adding a Backup Schedule](#)".
4. Click **Apply** and then click **OK**.

Enabling Encryption for an On-Demand Backup

1. Perform steps 1 to 10 under "[Adding an On-Demand Backup Request](#)".
2. Select the suitable encryption option for this backup.



See:

"[About Backup Encryption Options](#)" for detailed information on backup encryption options

3. Click **Apply** and then click **OK**.

Enabling Transient Backup Encryption

To enable encryption for transient backups:

1. Perform steps 1 to 10 under "[Adding an On-Demand Backup Request](#)".
2. For **Encryption**, select transient.
3. Enter a passphrase for secure encryption, in the specify passphrase field. Re-enter the passphrase in the verify field.
4. Select an algorithm for this backup encryption.
5. Click **OK**.



See Also:

"[About Transient Backup Encryption](#)" for detailed information on encrypting transient backups

Enabling Hardware Encryption

To change the values of hardware encryption policies:

1. Follow the steps in "[Displaying the Oracle Secure Backup Web Tool Home Page](#)".

2. From the Oracle Secure Backup Home page, click **Configure**.
The Configure page appears.
3. In the Advanced section, click **Defaults and Policies**.
The Configure: Defaults and Policies page appears.
4. In the Policy column, click **backupencryption**.
The Configure: Defaults and Policies > backupencryption page appears as shown in [Figure 12-1](#).

Figure 12-1 Encryption Policies

[Configure: Defaults and Policies](#) > Backupencryption

Apply OK Cancel

Name	Current Value	Reset to Default Value
Algorithm	<input type="radio"/> aes256 <input checked="" type="radio"/> aes192 <input type="radio"/> aes128	
Encryption	<input type="radio"/> required <input checked="" type="radio"/> allowed	
Key type	<input checked="" type="radio"/> transparent <input type="radio"/> passphrase	
Rekey frequency	<input checked="" type="radio"/> duration <input type="text" value="1"/> <input type="text" value="month"/> <input type="button" value="v"/> <input type="radio"/> per backup	
Enable Hardware Encryption	<input type="text" value="yes"/> <input type="button" value="v"/>	
Require encryptable media	<input type="text" value="no"/> <input type="button" value="v"/>	

5. To put backup jobs in a pending state if an encryptable tape is not loaded in the compatible tape drive, select **yes** in the **Require encryptable media** list.
6. Click **OK**.
The Configure: Defaults and Policies page displays a success message.

Disaster Recovery of Oracle Secure Backup Administrative Data

To guard against the loss of data on a computer used to make backups, Oracle Secure Backup protects its own [catalog](#) and settings data. Without this metadata the backups that Oracle Secure Backup has made are just so many assorted tapes. If the real-time Oracle Secure Backup catalog data is lost, then you can use the metadata from an Oracle Secure Backup catalog backup to restore Oracle Secure Backup to the state that it was in at the time of its last catalog backup.

Data which defines an Oracle Secure Backup administrative domain resides on the administrative host in the `$OSB_HOME/admin` directory and `usr/etc/ob` directory. During an Oracle Secure Backup installation, a dataset description file `OSB-CATALOG-DS` is automatically generated to back up these critical directories. Ideally, you must perform a backup of these directories daily, after completing all other backups so that the latest state of the administrative host can be captured for restore, in case of a hardware failure on the administrative host.

Oracle Secure Backup catalog recovery protects only the catalog and settings on an administrative server. The operating system and other installed software are not automatically backed up.

This chapter contains these sections:

- [Overview of Catalog Recovery Concepts](#)
- [Overview of Catalog Backup Jobs](#)
- [Recovering the Oracle Secure Backup Administrative Domain](#)

Overview of Catalog Recovery Concepts

The following Catalog Recovery objects are created during an initial Oracle Secure Backup install. These objects are reserved for Oracle Secure Backup Catalog Backups for the purpose of disaster recovery.

- [About Catalog Recovery Schedule Object](#)
- [About Catalog Recovery Media Family Object](#)
- [About Catalog Recovery Dataset Object](#)
- [About Catalog Recovery Summary Object](#)

All reserved catalog recovery objects are instances of the usual Oracle Secure Backup objects with some added restrictions. The restrictions are meant to prevent you from accidentally disabling the catalog backup or changing the backup settings to something that does not perform correctly.

Catalog Recovery Objects are similar to standard Oracle Secure Backup objects but they have some restrictions to prevent them from being changed, disabled, or accidentally deleted. The Oracle Secure Backup Web Tool, `obtool`, or Oracle Enterprise Manager can be used to make changes to these objects using the commands `chsched`, `chmf`, `chsum`, and `edds` in the same way their regular equivalents can be modified.

About Catalog Recovery Schedule Object

This object is associated with a catalog recovery [dataset](#) object, which specifies the data to be backed up, and a catalog recovery [media family](#) object, which specifies characteristics of the tape [volume](#).

The catalog recovery schedule object is created by the Oracle Secure Backup installer to perform a [full backup](#) at midnight each day. The priority is set at 50, rather than the default 100. A suitably-privileged [Oracle Secure Backup user](#) can:

- Add or remove a [trigger](#)
- Modify the priority
- Change [tape drive](#) restrictions
- Add or remove comments

By default, catalog backups are disabled after you install Oracle Secure Backup. You must explicitly set the trigger date to enable the scheduled backups of the catalog.

The associated dataset of the catalog object cannot be changed. Only unencrypted full backups are permitted. An [incremental backup](#) of the catalog data is disallowed because it would add complexity to the restore operation, which must be kept simple because it is performed without catalog data.



Note:

A backup using an automatically generated encryption key would be useless without the key store on disk, which would be lost if the administrative server were destroyed.

About Catalog Recovery Media Family Object

A catalog recovery media family object defines the tape volumes that result from a catalog recovery backup. The Oracle Secure Backup installer creates a catalog recovery media family object with a [write window](#) of 7 days, and a [retention period](#) of 14 days. It is recommended that backups be rotated between two volume sets.

A suitably privileged Oracle Secure Backup user can:

- Alter the write window
- Alter the retention time
- Modify the [volume ID](#) generation parameters
- Modify volume duplication attributes
- Associate a [rotation policy](#) with the media family
- Add or remove comments

The catalog recovery media family object must have a [time-managed expiration policy](#). Oracle Secure Backup does not allow the catalog recovery media family object to be content-managed, because backups are comprised of file-system data which cannot be content-managed.

About Catalog Recovery Dataset Object

A catalog recovery dataset object specifies what data is to be backed up. It incorporates an `include catalog` dataset directive to specify catalog data. This directive is expanded by Oracle Secure Backup to a definition of all files and databases that must be included in a catalog recovery backup. The catalog data itself is always backed up unencrypted regardless of any local encryption policies.

Other files and hosts can be added to the catalog recovery dataset object. To add files and paths on the administrative server to the catalog backup, enclose them within block delimiters beneath the `include catalog` directive in a dataset. You can add the following directives to an `include catalog` block:

- `include path`
- `exclude path`
- `exclude name`

No other directives are allowed within the `include catalog` block. The following example directive would cause the files in `/usr/local/bin` on the administrative host to be included in every catalog backup:

```
include catalog {  
    include path "/usr/local/bin"  
}
```

Note:

The `include catalog` directive cannot be added within an `include host` block, because it implicitly applies only to the administrative server. The dataset parser reports an error in this case.

You can add the `include catalog` directive to other datasets as well. There is no restriction on what else might be backed up by a dataset that includes it. The expanded catalog directive and its children, however, are handled as a separate job by the [scheduler](#).

A suitably-privileged Oracle Secure Backup user can modify the catalog recovery dataset object using the standard dataset language. But Oracle Secure Backup does not allow you to remove the `include catalog` directive from the catalog recovery dataset object.

See Also:

Oracle Secure Backup Reference for more information on Oracle Secure Backup dataset language

About Catalog Recovery Summary Object

A catalog recovery summary object causes Oracle Secure Backup to generate a summary report detailing each backup operation within the last 24 hours. This report is generated with a `--catalog` option that causes Oracle Secure Backup to include extended information about

catalog recovery backups. When a summary report is generated with `--catalog`, Oracle Secure Backup also checks for catalog backup failures and generates an e-mail to the backup administrator if any are found.

 **Note:**

The Oracle Secure Backup installer asks for the e-mail address of the `admin` user. On Windows, the installer also asks for an e-mail server. If no e-mail address is specified, or if no e-mail server is specified on Windows, then e-mail notifications are not sent.

A report generated with the `--catalog` option set includes:

- The volume ID and [barcode](#) for the catalog backup
- The file number for the catalog backup
- Results of the verification step

Catalog backups also appear in summary reports that include information on each [backup job](#), but they are not flagged as catalog backups, and they are mixed with the other backup jobs. The `--catalog` option is intended to help a backup administrator to check the status of catalog backups separately from other backup jobs.

Overview of Catalog Backup Jobs

Catalog recovery backup jobs always include a catalog backup, and they can include other files as well. Catalog backup jobs use the `include catalog` dataset extension to specify that all catalog data for the administrative server is included in the backup. Every catalog backup job is a [full backup](#). Oracle Secure Backup is configured on installation to perform regular catalog backup jobs.

Storage encryption is disabled for all catalog backup jobs. You cannot recover encrypted backup data without the encryption [wallet](#). But in a disaster scenario the encryption wallet would be lost, because it is part of the catalog data. So if the catalog backup data were encrypted, there would be no way to decipher it. Catalog backups can use transient passphrase encryption, because this does not require a wallet. Transient passphrase encryption is not enabled for catalog backup by default, but it can be added following the standard procedure.

 **See Also:**

"[About Transient Backup Encryption](#)" for more information about transient passphrase encryption

Recovering the Oracle Secure Backup Administrative Domain

If the Oracle Secure Backup administrative server fails or important directories are inadvertently deleted or damaged, then the administrative domain can be recovered by performing a restore of the Oracle Secure Backup Catalog. The dataset used for this backup is included in the default install of an Oracle Secure Backup administrative role and is called `OSB-`

CATALOG-DS. This section describes the procedure for restoring the `admin` and `ob` (on *nix or db on windows) directories which contain the information necessary to recover your administrative domain. Oracle strongly recommends that you perform regular backups of the `OSB-CATALOG-DS` dataset and also maintain a record of your Oracle Secure Backup device attachments, especially for devices you intend to use during disaster recovery. Having the following information readily available will facilitate the speed of the operation:

- A copy of the `lsdevice --long` output from `obtool`.
- The attachment information.
- A copy of your most recent e-mail of the job summary report for a catalog backup. The job summary for a catalog backup provides the information required to identify the volume and file number that holds the latest catalog backup.

This section contains the following topics:

- [Restoring the Oracle Secure Backup Catalog in a Tape Domain](#)
- [Restoring the Oracle Secure Backup Catalog in a Disk Pool Domain](#)

Restoring the Oracle Secure Backup Catalog in a Tape Domain

This section assumes that you are using a remote media server. If you are using a locally attached tape drive on your administrative server, then you can substitute the steps for locally attached drives for the steps for remote tape drives. The procedure points out these steps where appropriate.

To restore the Oracle Secure Backup catalog, perform the following tasks in order:

1. [Preparing to Restore the Oracle Secure Backup Catalog](#)
2. [Making the Administrative Domain Operational](#)

Preparing to Restore the Oracle Secure Backup Catalog

Before restoring the catalog data, perform a clean Oracle Secure Backup install on the machine selected to be the substitute or replacement Oracle Secure Backup administrative server. The easiest approach is to attach a tape drive to the administrative server. However, this option is not always available. If the administrative server does not have an attached tape device, then a remote media server needs to be reconfigured or added to the domain. This section lists the steps for adding a remote media server to the newly installed administrative host.

To prepare to restore the Oracle Secure Backup catalog:

1. Choose one of the following options:
 - If the tape drive is *locally* attached to the administrative server, skip to Step 3.
 - If the tape drive is attached to a *remote* media server, and if this remote host does *not* run Oracle Secure Backup software, skip to Step 3.
 - If the tape drive is attached to a *remote* media server, and if this remote host *does* run Oracle Secure Backup software, then perform the tasks described in Step 2:
2. Perform the following steps:
 - a. On the remote media server, stop the Oracle Secure Backup processes.
See *Oracle Secure Backup Reference* for the operating system-specific command syntax to startup and shutdown Oracle Secure Backup services.

- b. Move the `/usr/etc/ob` directory to an alternate location to save it.

On Unix/Linux, use the following command:

```
# mv /usr/etc/ob /usr/etc/ob.save
```

On Windows, use the following commands:

```
C:\> cd C:\Program Files\Oracle\Backup
C:\Program Files\Oracle\Backup > move /Y db db-save
```

- c. Restart the Oracle Secure Backup processes on the remote media server.
3. On the administrative server host, do the following:
 - a. Install Oracle Secure Backup and choose the administrative server option.
 - b. If you are installing on Windows, and if the tape device is attached locally, then in the Select the Program Features dialog box select **Configure locally attached media devices**.

See *Oracle Secure Backup Reference* for more information on `obtool` commands.

4. On the administrative server, log in to `obtool` as a user with administrative privileges and list the hosts in the domain.

The following example logs in to Oracle Secure Backup on host `brhost1`:

```
$ obtool
Oracle Secure Backup 12.2.0.1.0
login: admin
ob> lshost
brhost1          admin,client          (via OB)   in service
```

5. Choose one of the following options depending on whether your media server is separate from your administrative server:

- If the administrative server is acting as the media server, then add the media server role to the administrative server.

For example, enter the following command to add the media server role to administrative server `brhost1`:

```
ob> chost --addrole mediaserver brhost1
```

- If the remote media server already has Oracle Secure Backup installed, then do the following:
 - a. Stop the Oracle Secure Backup processes.
 - b. Save the `ob` directory (in *nix) or `db` directory (on Windows) which contains data identifying it as a member of the original administrative domain to an alternate location.
 - c. On Unix/Linux, use the following command:


```
# mv /usr/etc/ob /usr/etc/ob.save
```
 - d. On Windows, use the following commands:


```
C:\> cd C:\Program Files\Oracle\Backup
C:\Program Files\Oracle\Backup > move /Y db db-save
```
 - e. Restart the Oracle Secure Backup processes on the remote media server.
- If a remote media server is being used, then create the media server host using the `mkhost` command.

Do one of the following:

- If the remote host is *not* an NDMP media server, then install the Oracle Secure Backup package and add it to the administrative domain using the syntax shown in the following example:

```
ob> mkhost --role mediaserver brhost2
Info: waiting for host to update certification status...
```

- If the remote host *is* an NDMP media server, do not install Oracle Secure Backup on it, just add it to the administrative domain and ping it using the syntax shown in the following example:

```
ob> mkhost -r mediaserver -u root --ndmppass passwd -a ndmp brhost2
ob> pinghost brhost2
```

6. Run the `discoverdev` command to automatically discover and configure tape devices.

The following example discovers the tape devices on NDMP tape server `brhost2`:

```
ob> discoverdev -ic -h brhost2
Device-Type Device-Model Serial-Number Attachpoint
Library SL3000 571020201053 brhost2:/dev/scsi/changer/c0t500104F000AFE4F7d0
create device object brhost2_lib_1? (a, n, q, y, ?) [y]: y
Tape T10000C 576004000570 brhost2:/dev/rmt/0bn
create device object brhost2_tape_1? (a, n, q, y, ?) [y]: y
Tape Ultrium 5-SCSI HU1113FT2L brhost2:/dev/rmt/10bn
create device object brhost2_tape_2? (a, n, q, y, ?) [y]: y
Tape Ultrium 5-SCSI HU1113FT2P brhost2:/dev/rmt/11bn
create device object brhost2_tape_3? (a, n, q, y, ?) [y]: y
Tape Ultrium 5-SCSI HU1113FT0L brhost2:/dev/rmt/12bn
create device object brhost2_tape_4? (a, n, q, y, ?) [y]: y
Tape Ultrium 5-SCSI HU1113FT0T brhost2:/dev/rmt/13bn
```

The following example discovers the tape devices on a Linux media server, `storabck06`:

```
ob> discoverdev -ic -h storabck06
Device-Type Device-Model Serial-Number Attachpoint
create device object storabck06_lib_3? (a, n, q, y, ?) [y]: y
Library STK SL500 559000101874 storabck06:/dev/sg30
create device object storabck06_tape_1? (a, n, q, y, ?) [y]: y
Tape HP Ultrium 5-SCSI HU19487T7J storabck06:/dev/sg11
create device object storabck06_tape_2? (a, n, q, y, ?) [y]: y
Tape STK T10000C 576004000570 storabck06:/dev/sg12
create device object storabck06_tape_3? (a, n, q, y, ?) [y]: y
Tape HP Ultrium 5-SCSI HU1113FT0K storabck06:/dev/sg13
create device object storabck06_tape_4? (a, n, q, y, ?) [y]: y
Tape STK T10000C 576004000554 storabck06:/dev/sg14
create device object storabck06_tape_5? (a, n, q, y, ?) [y]: y
Tape IBM ULTRIUM-TD2 1110349363 storabck06:/dev/sg15
```

The following example shows `discoverdev` on a Windows media server:

```
ob> discoverdev -ic -h STORABCK56
Device-Type Device-Model Serial-Number Attachpoint
Library STK SL150 464970G+1333SY1401 STORABCK56://./ob10
create device object STORABCK56_lib_1? (a, n, q, y, ?) [y]: y
Tape HP Ultrium 5-SCSI HU1327WEYJ STORABCK56://./obt0
create device object STORABCK56_tape_1? (a, n, q, y, ?) [y]: y
Tape HP Ultrium 5-SCSI HU1328WGF6 STORABCK56://./obt1
create device object STORABCK56_tape_2? (a, n, q, y, ?) [y]: y
```

Associating discovered drives to libraries...

```
*** th0_warning: number of storage elements default (42) differs from current (30)
```

```
*** th0_warning: number of import export elements default (5) differs from current
(4)
no. of DTEs in library STORABCK56_lib_1 are: 2
drive serial number at dte: 1 for STORABCK56_lib_1 library is: HU1328WGF6
drive serial number at dte: 2 for STORABCK56_lib_1 library is: HU1327WEYJ
```

7. Ping the tape library to ensure that it is accessible.

For example, enter the following commands to ping library `brhost2_lib_1`:

```
ob> pingdev brhost2_lib_1
Info: library brhost2_lib_1 accessible.
Info: drive 1 tapel accessible.
```

8. Perform an initial inventory on the library containing the volume before using it for the first time.

For example, run the following command on library `brhost2_lib_1`:

```
ob> inventory --force -L brhost2_lib_1
```

This step is required even if you know which volume contains the `OSB_CATALOG` backup.

9. List the volumes in the tape library.

For example, enter the following command to list the volumes in library `brhost2_lib_1`:

```
ob> lsvol -L brhost2_lib_1
Inventory of library brhost2_lib_1:
  in  1:      occupied
  in  2:      occupied
  in  3:      occupied
  in  4:      unlabeled
  in  5:      unlabeled
  in  6:      unlabeled
  in  7:      unlabeled
  in  8:      unlabeled
  in  9:      unlabeled
```

10. Identify the volume that contains the catalog backup.

Choose one of the following options:

- If you have a job summary for a catalog backup, then obtain the volume ID, bar code, and file number for the catalog backup from the summary.

The following example shows a job summary for a catalog backup:

```
III. Successful jobs.
      Sceduled or          Content or          Backup
Job ID *Introduced at Completed at *Catalog Backup  Size  # (Barcodes)
-----
1      2014/06/25.01:05 2014/06/25.15:26  dataset OSB-CATALOG-DS  \
1.1    2014/06/25.01:05 2014/06/25.15:26  *catalog brhost1 17.9 MB 1
VOL000001                                     (000268)
admin/5 *2014/06/25.17:41 2014/06/25.17:42 dataset OSB-CATALOG-DS
admin/5.1*2014/06/25.17:41 2014/06/25.17:42  *catalog brhost1 18.5
MB                                             OSB-CATALOG-MF-000001(000016)
```

- If the volume containing your catalog backup is in the tape library, but if you do not know which volume contains the backup, then run the `identifyvol` and `lsvol` commands to find the volume. If you have a barcode reader this won't be necessary, just run `identifyvol -import` on the tape with the barcode label you need to use for the catalog restore

The following example shows how to identify a catalog volume:

```
ob> identifyvol --import -D brhost2_tape_1 1-2
```

Seq #	Volume ID	Volume Tag	Archive File	Archive Sect	Client Host	Backup Level	Archive Create Date & Time
1	VOL000001	000268	1	1	brhost1	0	2014/06/25 15:25:58

```
End of volume set.
```

Seq #	Volume ID	Volume Tag	Archive File	Archive Sect	Client Host	Backup Level	Archive Create Date & Time
1	OSB-CATALOG-MF-000001	000016	1	1	brhost1	0	2014/06/25 17:42:16

```
End of volume set.
```

- If the volume containing your catalog backup is *not* in the tape library, and if you do not know which volume contains the backup, then you must perform additional work. You must perform the following steps until you locate the correct volume:
 - Unload the volumes in the library.
 - Load new volumes
 - Run the `inventory` command from Step 8
 - Run the `identifyvol` command for each volume until you find a likely candidate, then you can move on to Step 11.

11. Once you have identified the tape containing the most recent OSB-CATALOG-BACKUP, you can generate a browsable index for it using the `catalog` command. To do this, perform the following commands:

```
ob> identifyvol -import -D <drive> <storage element number>
```

(Skip this step if you've performed it earlier. This step is necessary to get the volume ID for use in the `catalog` command)

```
ob> catalog -v OSB-CATALOG-MF-000001 -D brhost2_tape_1
Info: catalog import request 1 submitted; job id is admin/1
```

12. Restore the catalog data to alternate directories to stage it for recovering the administrative server, this example is for *nix and uses the default Oracle Secure Backup paths, but the equivalent can be done on Windows as well:

```
ob> set host brhost1
ob> cd /usr/local/oracle/backup
ob> restore admin --aspath /usr/local/oracle/backup/admin-restored -h brhost1 --go
Info: 1 catalog restore request item submitted; job id is admin/7.
ob>
```

```
ob> cd /usr/etc/
ob> ls
ob/
ob> pwd
/usr/etc on host brhost1 (browsing catalog data)
ob> restore ob --aspath /usr/etc/ob-restored --go
Info: 1 catalog restore request item submitted; job id is admin/8.
ob>
```

The following example shows the Windows case for a restore of the catalog data using the default Oracle Secure Backup paths:

```
ob> set host brhost1
ob> cd "C:\Program Files\Oracle\Backup"
ob> restore admin --aspath C:\admin-restored -h brhost1 --go
```

```
Info: 1 catalog restore request item submitted; job id is admin/1.
ob>
```

```
ob> cd "C:\Program Files\Oracle\Backup"
ob> restore db --aspath C:\db-restored --go
Info: 1 catalog restore request item submitted; job id is admin/2
```

13. On the administrative server, stop all Oracle Secure Backup services.

See *Oracle Secure Backup Reference* for the operating system-specific command syntax to startup and shutdown Oracle Secure Backup services.

14. On the media server, stop all Oracle Secure Backup services.

See *Oracle Secure Backup Reference* for the operating system-specific command syntax to startup and shutdown Oracle Secure Backup services.

15. Confirm that catalog files have been restored properly by listing the contents of the restored directories.

The following Linux and UNIX example lists the restored `ob` and `admin` directories:

```
$ ls /usr/local/oracle/backup/admin-restored
config encryption history log security state
$ ls /usr/etc/ob-restored
osbdevs report wallet xcr
```

The following Windows example lists the restored `db` and `admin` directories:

```
C:\>dir /w c:\admin-restored
Volume in drive C has no label.
Volume Serial Number is 240F-6921
Directory of c:\admin-restored
[.] [..] [config] [encryption]
[history] [log] [security] [state]
0 File(s) 0 bytes
8 Dir(s) 254,307,901,952 bytes free
C:\>dir /w c:\db-restored
Volume in drive C has no label.
Volume Serial Number is 240F-6921
Directory of c:\db-restored
[.] [..] .hostid obconfig.txt
[report] [wallet] [xcr]
2 File(s) 488 bytes
5 Dir(s) 254,307,901,952 bytes free
```

16. On the administrative server, remove the following directories from the Oracle Secure Backup home:

- `ob` (Linux and UNIX) or `db` (Windows) directory
- `admin` directory

The following Linux and UNIX example deletes the `/usr/etc/ob` and `/usr/local/oracle/backup/admin` directories:

```
$ rm -rf /usr/etc/ob
$ rm -rf /usr/local/oracle/backup/admin
```

The following Windows example deletes the `C:\Program`

```
Files\Oracle\Backup\admin and C:\Program
Files\Oracle\Backup\db directories.
C:\>cd C:\Program Files\Oracle\Backup
C:\Program Files\Oracle\Backup>del /S admin
C:\Program Files\Oracle\Backup>del /S db
```

17. Move the restored Oracle Secure Backup directories to their original locations on the administrative domain.

The following Linux and UNIX example renames the restored directories:

```
$ mv /usr/local/oracle/backup/admin-restored /usr/local/oracle/backup/admin
$ mv /usr/etc/ob-restored /usr/etc/ob
```

The following Windows example renames the restored directories:

```
C:\>cd C:\Program Files\Oracle\Backup
C:\Program Files\Oracle\Backup>move /Y C:\db-restored db
C:\Program Files\Oracle\Backup>move /Y C:\admin-restored admin
```

Making the Administrative Domain Operational

After you have restored the catalog files, the administrative domain is not yet ready for normal operation. This section explains how to return the domain for normal use.

To make the administrative domain operational:

1. Choose one of the following options:
 - If the tape drive is *locally* attached to the administrative server, skip to Step 3.
 - If the tape drive is attached to a *remote* media server, and if this remote host does *not* run Oracle Secure Backup software, skip to Step 3.
 - If the tape drive is attached to a *remote* media server, and if this remote host *does* run Oracle Secure Backup software, then perform the tasks in Step 2.
2. Perform the following steps:
 - a. On the remote media server, stop the Oracle Secure Backup services.
See *Oracle Secure Backup Reference* for operating system-specific command syntax.
 - b. Move the original `/usr/etc/ob` directory back into place:
On Unix, use the following command:

```
# mv /usr/etc/ob.sav /usr/etc/ob
```


On Windows, use the following command:

```
C:\>cd C:\Program Files\Oracle\Backup
C:\Program Files\Oracle\Backup>del /S db
C:\ Program Files\Oracle\Backup> move /Y db-save db
```
 - c. On the remote media server, start the Oracle Secure Backup services.
3. On the administrative server, re-create the obfuscated encryption wallet.

Although Oracle Secure Backup restores the password-protected encryption wallet to the administrative server, for security reasons the obfuscated encryption wallet is not backed up. You must re-create it manually after a restore operation, specifying the password used to create the original encryption wallet.

Note:

You must know your original encryption wallet password to accomplish this task.

The following example uses the `obcm` command to re-create the wallet:

```
obcm mkow --keywallet
```

When prompted, enter the wallet password.

After you run the above command, when you attempt to run `obtool`, you may encounter the following error:

```
obtool: Error: can't connect to administrative observed - Network is unreachable
```

You can resolve this error by stopping and restarting the Oracle Secure Backup services.

4. On the administrative server, stop and restart the Oracle Secure Backup services. See *Oracle Secure Backup Reference* for operating system-specific command syntax.

See Also:

["Managing Daemons"](#)

5. If the catalog restore was performed using a *remote* media server, cycle the Oracle Secure Backup daemons on that server.

If the daemons have not been cycled, the following error message may be displayed indicating that you must first cycle daemons before your administrative domain will be operational:

```
Error: can't connect to Oracle Secure Backup service daemon on brhost2 - observed not running
```

```
brhost2: no services are available
```

6. On the administrative server, perform an initial inventory on the library before using it for the first time.

For example, run the following command on library `brhost2_lib_1`:

```
ob> inventory -L brhost2_lib_1
```

7. Confirm that the recovered Oracle Secure Backup administrative domain is intact. Check devices, datasets, volumes, jobs, media families, and other associated Oracle Secure Backup objects to confirm they are present and working as expected in the domain.

Restoring the Oracle Secure Backup Catalog in a Disk Pool Domain

If an Oracle Secure Backup domain does not contain tape devices, a disk pool device can be used for catalog backups. It is recommended that a separate disk pool device be created exclusively for use by catalog backups. In the event of a catastrophic failure involving the administrative server, having a separate disk pool device reserved for this purpose will simplify and expedite restoring the Oracle Secure Backup domain.

For example:

```
ob> mkdev --type disk --attach <AdminHost>:<disk-pool-storage-location-path>
CatalogDiskPool
```


The storage location selected for the disk pool should be on a remote disk, physically separate from the Oracle Secure Backup administrative server but easily accessible by NFS or another mounting protocol. The disk should be selected so that a failure of the administrative server does not impact the accessibility of the `<disk-pool-storage-location-path>` by a substitute server on the network.

In order to automate the process, the `OSB-CATALOG-SCHED` should be modified to restrict the catalog backup to the disk pool.

For example:

```
ob> chsched --restrict <CatalogDiskPool> OSB-CATALOG-SCHED
```

The following procedure describes an example of a disaster recovery of an Oracle Secure Backup administrative domain on a Linux administrative server. The steps for accessing the Oracle Secure Backup catalog backup data from a diskpool device are the same for all platforms, although the particulars of disaster recovery will differ slightly.

See Also:

[Restoring the Oracle Secure Backup Catalog in a Tape Domain](#) for more information on the restore details associated with a tape environment

To restore the Oracle Secure Backup Catalog, complete the following steps:

1. Keep a record of the attachment associated with your diskpool device, for example:

```
[root@storabck102 backup]# obtool
ob> lsd -l cloud-diskpool
cloud-diskpool:
Device type:          disk pool
In service:          yes
Debug mode:          no
Capacity:            (not set)
Consumption:         489.0 GB
Free space goal:     (system default)
Concurrent jobs:     1
Blocking factor:     (default)
Max blocking factor: (default)
UUID:                9f8b6c26-54d3-1033-8188-0021288e4464
Attachment 1:
  Host:               storabck102
  Directory:          /mount-cloud-bucket/diskpool
ob>
```

2. Perform a fresh install on your administrative server. In this example, it is assumed that the name and IP address will remain the same as the previous administrative server.

See Also:

Oracle Secure Backup Installation and Configuration Guide for more information on the installation procedure

- To create the original disk pool device by using the same attachment, run the following commands:

```
ob> chhost --addrole mediaserver storabck102
ob> mkdev -t disk -a storabck102:/mount-cloud-bucket/diskpool --force
diskpool
```

 **Note:**

The `-force` option is necessary or else you will not be able to use an existing diskpool attachment directory in the newly installed Oracle Secure Backup administrative domain.

- Catalog the diskpool to import it into the Oracle Secure Backup administrative domain:

```
ob> catalog -d diskpool
```

- Confirm that the import succeeded

```
ob> lsj --long --log admin/1
admin/1:
Type:                catalog import for diskpool
Scheduled time:      none
State:               completed successfully at 2015/10/27.10:53
Priority:             100
Run on host:         (administrative server)
Attempts:            1
Log:
 2015/10/27.10:53:45 Dispatching job to run on administrative
server.
 2015/10/27.10:53:56 Catalog import completed with no error.
 2015/10/27.10:53:56 Job completed successfully.
```

- To restore the original `$OSB_HOME/admin` and `/usr/etc/ob` directories to alternate names, run the following commands:

```
ob> restore /usr/local/oracle/backup/admin --aspath /usr/local/oracle/
backup/admin-restored --go
ob> restore /usr/etc/ob --aspath /usr/etc/ob-restored --go
```

- Run the `ls` command to confirm that the restores completed successfully.
- Stop the Oracle Secure Backup daemons and place the restored directories appropriately:

```
[root@storabck102 backup]# /etc/init.d/observed stop
[root@storabck102 backup]# ps -ef | grep ob
[root@storabck102 backup]#
[root@storabck102 backup]# ls
admin-newinstall apache device etc install man templates
admin-restored bin drv help lib samples tools
[root@storabck102 backup]# mv admin admin-newinstall
[root@storabck102 backup]# mv admin-restored admin
[root@storabck102 backup]# ls
admin apache device etc install man templates
```

```
admin-newinstall bin    drv    help lib    samples tools
[root@storabck102 backup]#
[root@storabck102 etc]# ls
ob ob-restored
[root@storabck102 etc]# mv ob ob-newinstall
[root@storabck102 etc]# mv ob-restored ob
[root@storabck102 etc]#
```

9. Restart the Oracle Secure Backup Daemons.
10. Use `obcm` to update the wallet after the restore using the original keywallet password:

```
# obcm chpass --keywallet
Old wallet password:
New wallet password:
New wallet password (again):
Wallet password has been reset
```

11. Use the `lsh` to confirm that the previous administrative domain is intact.
12. Check the continuity with clients and devices by pinging them, browsing the catalog for clients, and performing test restores.

14

Staging

This chapter describes the Oracle Secure Backup staging feature which lets you store one or more backup image instances in a container in preparation for automatically copying or moving the backup image instances to another container.

This chapter contains the following sections:

- [About Staging](#)
- [About the Oracle Secure Backup Default Stage Rule](#)
- [Setting Up Staging](#)

About Staging

Staging lets you store one or more backup image instances in a container in preparation for automatically copying or moving the backup image instances to another container.

For Oracle Secure Backup, the staging container can be a disk pool or a cloud device. In a typical staging scenario, the backup instance would be moved from a disk pool to a tape drive.

Staging can involve multiple backup image instances and can be configured to run at scheduled times and based on certain conditions. Examples of conditions include the size of a set of backup images, the client hosts in the backup, and database information.

Staging can also be done on-demand.

Benefits of Staging

- Disks have much faster random access of backup files than tapes. Tapes can be moved offsite for long-term storage. Staging allows a backup to be automatically contained on both disk and tape, thus allowing both fast restores and the benefits of being on tape.
- Staging allows the use of multiple streams, in parallel, during backup and restore operations. In the case of backups, the data is copied to a single tape drive at a later time.
- Staging can minimize the stop-and-reposition issue that occurs when slow clients are backed up to tape because when staging is used, slow clients can be concurrently backed up to a disk pool and then copied to tape in a single high-speed data stream.
- Staging allows backup instances to remain on disk after they are also written to tape. Each instance can have a different expiration time so the backup could remain on the disk to restore more quickly while also being on tape for long term protection.
- Staging can be used to create additional copies of backup image instances at an offsite location using a remote Oracle Secure Backup media server to provide additional data protection through redundancy.

Staging Concepts

The following terms describe the concepts of staging:

Staging

Staging is the temporary use of a disk pool as an interim container for a backup image that is ultimately destined to be written to another container, usually tape. The backup is first written to a disk pool device in order to improve efficiency by reducing the time a physical tape drive is assigned for exclusive use by a given backup job. Backup images staged to a disk pool are scheduled for movement to tape based on either a schedule, or based on the amount of data in the disk pool device. After the backup image instance in the disk pool is copied to another container, it can optionally be deleted.

Stage source job

A stage source job (usually referred to as simply a source job) is the initial backup job that writes backup images to the stage pool. A source job can be an on-demand backup job, a backup schedule, a cpinstance job, or even another copyfromstage job that writes backup image instances to another stage disk pool device.

Copy-from-stage

Copy-from-stage refers to automatically copying backup image instances to a destination container.

copyfromstage job

A copyfromstage job is the job that copies the backup image instances created by a stage source job to a destination container.

stagescan job

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. A stagescan job is typically launched by a stagescan schedule, but can also be launched on-demand using the `obtool stagescan` command.

 **Note:**

All copyfromstage jobs have system job ID numbers, starting at 1 and increasing. Scheduled stagescan jobs also have a system job ID. In the output of the `obtool lsjob` command, system jobs always appear first in the job listing and so could appear at the top of a very long job listing. To view both copyfromstage jobs and stagescan jobs, specify them as job types when you issue the `lsjob` command. See *Oracle Secure Backup Reference* for information about the `lsjob` command.

Staged

A backup image instance is said to be staged if the instance is to be stage-copied either immediately or at some future time.

Migrate

To migrate a backup image instance refers to doing a stage copy of a backup image instance from the source container to the destination container and, upon a successful copy, deleting the backup image instance in the source container. The term migrate, in the context of staging, is synonymous with the word move.

On-demand staging

On-demand staging refers to issuing an `obtool` command to create an immediate stagescan job that copies all backup images instances that match a specific stage device and a specific set of stage rules.

Source container

The staging disk pool device that contains one or more backup image instances.

Destination container

The target device to which a copyfromstage job copies backup images from the staging disk pool. The destination container can be a tape device or another disk pool.

About the Oracle Secure Backup Default Stage Rule

Stage rules control which backup images are copied, and when they are copied. They can also be used to control the minimum time a backup image is guaranteed to remain on a stage device.

Oracle Secure Backup provides a default stage rule that matches all instances. For a scheduled stagescan job, if no other stage rule in a device matches a backup image instance, then the instance is always copied by the default stage rule. The purpose of having a default stage rule is to guarantee that all instances in a stage disk pool are copied. Copying all instances ensures that if you make a configuration error, and an instance you expected to be copied is not copied, then backup image instances that expire in the source disk pool are not permanently lost.

A "match" to a stage rule means that an instance matches the media family name and one or more places (database ID, database name, or file-system host name). If the stage rule restriction list contains a cloud device, then the instance also must be encrypted to match the rule. If those conditions match, then the default stage rule is not invoked for the instance. In the following situations it is possible that even in the case of a match, an instance still might not be copied:

- There is a stagescan schedule listed in the stage rule that does not match the current stagescan schedule that invoked the stagescan job. The instance is copied by that rule later when the other schedule runs.
- The value of a matching stage rule's minimum age filter, or minimum copy size filter, could be set to values so large that an instance is never copied. The instance will then never be deleted even if the instance expiration time is exceeded. Caution should always be used when setting values for those filters.

The device in the restriction list of the default stage rule should be considered an "error" device so that any instances copied there by the default stage rule are considered mistakes. These mistakes can then be corrected by adding additional stage rules that match these backup image instances stored in the source disk pool device.

Note:

A stage-enabled Oracle Secure Backup Cloud Storage Device does not support the default stage rule. A backup instance that is stored within the stage-enabled Oracle Secure Backup Cloud Storage Device and not picked up by the stage rule may be purged when it expires. Such an instance may be deleted if it has not been staged. To ensure that all backup instances are staged, you can add a "catch all" stage rule at the end of the device's list of staging rules.

Stage Loops

Oracle Secure Backup prevents a copyfromstage job from using the same disk pool as both the source and destination. However, when more than a single pool has staging enabled, it is

possible for instances to be copied back to the original pool if a stage loop occurs. For example, the following situations result in stage loops:

- A stagescan schedule in a copyfromstage job copies an instance from source disk pool A to destination disk pool B which also has staging enabled. Later, another stagescan schedule creates a copyfromstage job that copies the new instance in the destination pool B back to the original source disk pool A.
- An instance is copied from pool A to pool B, then from pool B to pool C, and then from pool C back to the original pool A.

Stage loops must be prevented because they could easily result in the same instance being replicated many times until a disk pool runs out of space.

To prevent stage loops, Oracle Secure Backup does the following when a stage rule is added to a device or a change is made to a stage rule restriction list:

1. Scans the stage rule list on the source device and assumes that the instance might be copied to any disk pool that is in each stage rule restriction list.
2. Scans the restriction list for each stage rule in each of the potential destination disk pool devices and assumes that the instance might be copied to any of these disk pools.

If any of these disk pools are the original disk pool, or any other disk pool that has already been assumed as a destination for the instance, then the configuration command fails, and an error message is displayed. For example:

```
ob> chstage --restrict pool1 srule2
Error: stage loop - pool1 -> srule2:pool0 -> srule1:pool1
Error: restriction list not changed
ob>
```

Limitations of Stage Loop Detection

- There is no check to see if the instance matches any stage rule, or even if staging is enabled in the disk pools. Creating a stage loop by changing a stage rule restriction list is prohibited.
- Oracle Secure Backup usually only searches four disk pools deep to detect stage loops. If there are many disk pools and stage rules, then the search can potentially time out after 10 seconds. Oracle Secure Backup is always guaranteed to search two disk pool levels deep, regardless of how long it takes, so the case shown in the previous example will always be detected.
- If a disk pool has any stage rules with a disk pool device in the stage rules restriction list, then the disk pool device cannot be added to the restriction list of the default stage rule because this would cause a stage loop.
- Stage rules with a disk pool in the restriction list cannot be added to a disk pool device that is already in the restriction list of the default stage rule.

Setting Up Staging

The following are some concepts and guidelines to be aware of when you set up staging.

- When staging is used, it is assumed that all backup image instances copied into a stage disk pool device will be copied elsewhere. This assumption prevents incorrect configurations in which an instance is expected to be copied but is not, and then the instance expires and is deleted, leaving no backup to restore. To prevent this, an instance

in a staging disk pool is never automatically deleted until it has been copied, even if the instance has expired. (However, if desired, you can explicitly delete the instance using the `rminstance` command.)

Do not use the default stage rule to intentionally cause backup image instances to be copied. Instead, use it with an "error" disk pool as the target device so that instances that don't match any other stage rule can be identified when they appear in the error disk pool.

The default stage rule can be used to copy instances in a staging design, but be aware that doing so can make it harder to detect that instances are not going where expected because the default rule always copies anything that does not match any rule. Therefore, if you expect a rule to lead to an instance being copied, but the instance does not match the rule, then that instance gets mixed in with everything else that is copied by the default stage rule.

- Use the minimum number of stage rules necessary so that stagescan jobs run as fast as possible.
- To avoid having too many instances in a `copyfromstage` job, do not use an existing disk pool as a staging device when you first upgrade to use staging. You can ignore this guideline if the existing disk pool has relatively few instances in it.
- Do not leave the restriction list in a stage rule empty. Explicitly list the destinations device(s).

There are many ways to set up staging. The following describes one example.

To set up staging:

1. Use the `mkdev` command to create a target disk pool device.

```
ob> mkdev --type disk --initialize --attach somehost:/somepath/pooltarget
pooltarget
```

2. Use the `mksched` command to create two stagescan schedules.

```
ob> mksched --type stagescan --day daily --time 6:00 scheda
ob> mksched --type stagescan --day daily --time 12:00 schedb
```

3. Create three stage rules. The `--dbid`, `--dbname`, and `--fshost` options are not specified in these examples, so they all default to the asterisk (*) wildcard character.

```
mkstage --schedule scheda --matchfamily mfa --targetfamily mftarget --
restrict pooltarget rulea
mkstage --schedule schedb --matchfamily mfb --targetfamily mftarget --
restrict pooltarget ruleb
mkstage --matchfamily mfc --targetfamily mftarget --restrict pooltarget
rulec
```

The first stage rule, `rulea`, matches media family `mfa` and uses schedule `scheda`.

The second stage rule, `ruleb`, matches media family `mfb` and uses schedule `schedb`.

The first stage rule, `rulec`, matches media family `mfc` and has no schedule.

4. Set the default state rule target media family and restrictions.

Staging cannot be enabled on any stage disk pool device using the `--staging yes`, until after the target media family and the restriction list are set in the default stage rule. This

only needs to be done one time. (The following example assumes there is a tape device named `vt1`.)

```
ob> chstage --targetfamily mftarget --restrict vt1 OSB-DEFAULT-STAGE-RULE
```

5. Create a staging disk pool device.

```
ob> mkdev --type disk --initialize --stagerule rulea,ruleb,rulec --staging  
yes  
--attach somehost:/somepath/poolstage poolstage
```

When schedule `scheda` is triggered, instances that match stage rule `stagea` (that is, instances that are backed up using media family `mfa`) will be copied to disk pool `poolstage` using media family `mftarget`. Instances that match stage rule `rulec` (that is, instances backed up using media family `mfc`) will be copied. Because `rulec` has no schedule, it will match all schedules.

When schedule `schedb` is triggered, instances that match stage rule `stageb` (that is, instances that are backed up using media family `mfb`) will be copied to disk pool `poolstage` using media family `mftarget`. Instances that match stage rule `rulec` (that is, instances backed up using media family `mfc`) will be copied.

A

NDMP Special Characteristics

As an [Oracle Secure Backup user](#), you do not have to be aware of [NDMP](#) in any substantive way unless you use third-party NDMP-enabled appliances. If you use Windows, Linux, or UNIX hosts with secondary storage connected through [SCSI](#) or [Fibre Channel](#), then NDMP is basically invisible. There might be some cases, however, in which you must be aware of special NDMP characteristics.

NDMP and IPv6

Oracle Secure Backup supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6. But NDMP filers and tape systems that are not running Oracle Secure Backup software must be assigned IPv4 addresses. If NDMP filers or tape system are accessed during a backup or restore operation, then the Oracle Secure Backup NDMP counterpart must also be assigned an IPv4 address.

NDMP and Constrained Error Reporting

NDMP specifies no programmatic means for a [data service](#) to report many common errors. This restriction applies to the common `pathname not found` condition, which NDMP data services typically report as `internal error`. Oracle Secure Backup notes all such errors in the job transcript.

Most NDMP implementations make use of the LOG interface, which provides servers a means to report text messages to the backup application. Oracle Secure Backup records all LOG messages it receives in the job transcript.

Limitations Using Network Appliances Data ONTAP

The NDMP [data service](#) of Data ONTAP provides for backup of directories and their contents only. You cannot explicitly back up individual files. You can restore both individual files and directory trees.

During restore operations, the Data ONTAP NDMP data service does not report the names of files and directories restored from the [backup image](#). As a result, Oracle Secure Backup warns you that the NDMP data service did not identify whether files you requested were found.

Glossary

active location

A [location](#) in a [disk pool](#), [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 clients
- One or more media servers

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 through which data travels) of a [tape device](#) or a [disk pool](#) to a host in the [administrative domain](#).

backup catalog data

This is the metadata that is stored on tape and the disk pool in the `/osbmeta` directory, following the backup image instance, as a part of the backup. Backup catalog data provides information that rebuilds that backup image instance within the [Oracle Secure Backup catalog file](#) during the [import catalog](#) process.

backup container

The physical storage media on which a backup is stored. Backup containers can be [tape devices](#) or [disk pools](#).

backup image

The product of a [backup operation](#). It stores the metadata related to the backup operation. The actual data this is backed up is stored in the [backup image instance](#).

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 instance

The product of a [backup operation](#). It stores the actual data that is backed up. There can be more than one backup image instances for a single [backup image](#).

A single backup image instance 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 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 can back up any file 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 or disk pool.

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 the backup requests become backup jobs and are 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

The 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 window

A time frame in which a [backup operation](#) can be run.

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.

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](#).

class

A named set of [rights](#) for an [Oracle Secure Backup user](#). A class can have multiple users, but each Oracle Secure Backup user can belong to one and only one class.

client

Any computer or server whose files Oracle Secure Backup backs up or restores.

Common Internet File System (CIFS)

An Internet file-system protocol that runs on top of [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#).

content-managed expiration policy

A [volume](#) with this type of [expiration policy](#) expires when every [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 block

The amount of data written to a [volume](#) in each write operation.

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.

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.

dataset

The contents of a [file-system backup](#). A [dataset file](#) describes a 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 at least one [dataset file](#). 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.

DBID

An internal, uniquely generated number that differentiates databases. Oracle creates this number automatically when you create the database.

defaults and policies

A set of configuration data that specifies how Oracle Secure Backup runs in an [administrative domain](#).

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 data, and

ownership data. An [attachment](#) consists of a host name and the device special file name by which that tape 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 NAS devices such as a Network Appliance [filer](#).

disk pool

A file-system directory that stores backups. Disk pools can be accessed concurrently by multiple backup or restore jobs.

DMA

See [data management application \(DMA\)](#)

domain

A group of computers and tape 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. Every host or device sharing a common part of the IP address is said to be in the same domain.

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](#).

Fibre Channel

A protocol used primarily by a [tape device](#) 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.

host

An addressable computer in the network that has been assigned a specific set of roles.

host authentication

The initialization phase of a connection between two hosts in the [administrative domain](#). After the hosts authenticate themselves to each other with [identity certificates](#), communications between the hosts are encrypted by [SSL](#). Almost all connections are two-way authenticated; exceptions include initial host invitation to join an administrative domain and interaction with hosts that use [NDMP access mode](#).

identity certificate

An X.509 [certificate](#) signed by the [Certification Authority \(CA\)](#) that uniquely identifies a host in an Oracle Secure Backup [administrative domain](#).

import catalog

The process through which an Oracle Secure Backup user imports and catalogs a volume set from tape to the Oracle Secure Backup domain. The function reads the backup catalog data from the tape and inserts necessary information into the [Oracle Secure Backup catalog file](#).

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 a [file-system backup](#). 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 each past, current, and pending [backup job](#).

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 might be the name of a [tape library](#), a [disk pool](#), a data center, or an off-site storage facility.

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](#) or [disk pool](#) connected to it. A media server is responsible for transferring data to or from the 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 \(NAS\)](#)

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 NFS and CIFS.

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 a file server direct to a [tape drive](#)—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.

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

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 or disk. `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 Oracle Secure Backup [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 Oracle Secure Backup [Web tool](#).

off-site backup

A backup that is equivalent to a [full backup](#) except that it does not affect the full or incremental [backup schedule](#). An off-site backup is useful when you want to create a [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 [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.

Oracle Secure Backup catalog file

This is the `indices.cur` file. This file contains complete information about all backed up files, including the name, path, and statistical information. There is one catalog file per host.

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 tape device, whereas the Oracle Secure Backup logical unit number is part of the name of the [device special file](#).

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

The [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](#) 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](#) password is valid.

password reuse time

The length of time which must elapse before a previously-used [Oracle Secure Backup user](#) password may be reused.

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 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.

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 or disk pool.

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.

RMAN client

The [Recovery Manager \(RMAN\)](#) client program, which is installed automatically with Oracle Database software, initiates database backup and recovery. The RMAN client can back up and

recover any Oracle Database files accessible locally or through Oracle Net so long as it meets compatibility requirements.

RMAN recovery catalog

The recovery catalog is an optional database schema that serves as a secondary repository of [Recovery Manager \(RMAN\)](#) metadata. You can create a centralized recovery catalog in a database to store the metadata for multiple target databases. The recovery catalog is managed by RMAN and is independent of the Oracle Secure Backup [catalog](#).

RMAN target database

The target is the database that [Recovery Manager \(RMAN\)](#) backs up or restores. The RMAN repository, which is the metadata that RMAN uses to manage backup and recovery, is stored in the control file of the target database.

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, to 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. A [file-system backup](#) is triggered by a schedule, which you can create with the `mksched` command in [obtool](#). In contrast, an [on-demand backup](#) is a one-time-only backup 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](#) containing each [backup job](#) 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 multiple tape devices to use 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 [host authentication](#) using 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.

SSL

See [Secure Sockets Layer \(SSL\)](#)

Storage Area Network (SAN)

A high-speed storage device subnetwork. 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 element

A physical location within a [tape library](#) where a [volume](#) can be stored and retrieved by a tape 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 a [file-system backup](#) that contains all files and directories saved from the top-most file-system level.

tape device

A [tape library](#) or [tape drive](#) 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 a [storage element](#) and a [tape drive](#).

tape service

An [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 all volumes 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.

trusted certificate

A [certificate](#) that is considered valid without the need for validation testing. Trusted certificates build the foundation of the system of trust. Typically, they are certificates from a trusted [Certification Authority \(CA\)](#).

unprivileged backup

A [file-system backup](#) 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 associate with Oracle Secure Backup user who initiates the backup.

UUID

Universal Unique Identifier. An identifier used for tagging objects across an Oracle Secure Backup [administrative domain](#).

virtual tape library

One or more large-capacity disk drives partitioned into virtual physical tape volumes. To Oracle Secure Backup the virtual tape library appears to be a physical library with tape volumes and at least one [tape drive](#). The volumes and drives in the virtual tape library can be configured to match common physical tapes and drives.

volume

A volume is a unit of media, such as the LTO5 tape drive. 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 order of the [volume](#) 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 X.509 [certificates](#) and their 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](#).

write window

The period for which a [volume set](#) remains open for updates, usually by appending additional [backup images](#). 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

A

adding

- backup schedules, [5-16](#)
- backup windows, [5-14](#)
- classes, [2-16](#)
- dataset files, [5-11](#)
- dataset files in OSB catalog recovery, [13-3](#)
- duplication policies page, [11-29](#)
- duplication windows, [11-32](#)
- media families, [3-3](#)
- one-time backup request, [5-30](#), [5-32](#)
- rotation policies, [11-11](#)
- storage locations, [11-9](#)
- users, [2-8](#)
- vaulting scan schedules, [11-15](#)
- volume duplication schedules, [11-33](#)

admin class, [2-5](#)

administrative data

- and OSB backup encryption, [12-4](#)

administrative domain

- about, [1-3](#)
- multiple-host, [4-9](#)
- Oracle RAC environment, [4-24](#)
- single-host, [4-9](#)

algorithms

- hardware-based, [12-9](#)
- OSB encryption, [12-4](#)

AME encryption

- hardware-based, [12-7](#)

Apache Web server daemon

- about, [1-15](#)

autovolumerelease policy, [11-49](#)

B

backup

- statistics, [9-6](#)

backup catalog

- browsing, [6-9](#)
- displaying, [6-9](#)
- recovery, [13-1](#)

backup containers

- about, [1-20](#)
- default, [1-20](#)
- disk pools, [1-25](#)

backup containers (*continued*)

- types, [1-20](#)

backup dataset files

- about, [5-2](#)
- location, [5-3](#)

backup encryption

- about, [12-1](#)
- administrative data, [12-4](#)
- algorithms, [12-4](#)
- client level, [12-12](#)
- example, [12-11](#)
- hardware-based, [12-7](#)
- keys, [12-4](#)
- levels, [12-3](#)
- one-time unencrypted backups, [12-10](#)
- options, [12-4](#)
- OSB catalog recovery, [13-4](#)
- policy values, [12-2](#)
- rekey frequency, [12-3](#)
- security, [12-4](#)

backup encryption and RMAN, [12-6](#)

backup encryption levels

- precedence, [12-3](#)

backup image instances

- catalog data, [1-19](#)
- deleting, [7-5](#)
- deleting expired, [8-20](#)
- deleting expired from cloud storage devices, [8-22](#)
- displaying, [7-4](#)
- editing, [7-4](#)

backup images

- and sections, [1-27](#)
- displaying, [7-1](#)
- file numbers, [6-15](#), [6-16](#)
- labels, [1-22](#)
- managing, [7-1](#)
- renaming, [7-2](#)

backup jobs

- canceling, [9-10](#)
- displaying job transcripts, [9-4](#)
- file-system, [1-10](#)
- managing, [9-1](#)
- OSB catalog recovery, [13-4](#)
- removing, [9-8](#)
- resuming, [10-15](#)

- backup jobs (*continued*)
 - running, 9-9
 - suspending, 10-15
 - viewing properties, 9-4
- backup requests
 - about, 1-9
 - adding one-time request, 5-30, 5-32
 - displaying, 5-30
 - removing, 5-30, 5-33
 - sending to scheduler, 5-33
- backup schedules
 - about, 5-7, 5-27
 - adding, 5-16
 - configuring, 5-16
 - displaying, 5-16
 - editing, 5-17
 - removing, 5-18, 5-19
 - renaming, 5-18
- backup sections
 - about, 1-21
- backup statistics, 9-6
 - backup_time, 9-7
 - dev_iorate, 9-8
 - dev_iosecs, 9-7
 - dev_kbytes, 9-7
 - devices, 9-6
 - directories, 9-7
 - encryption, 9-7
 - end_time, 9-7
 - entries_excluded, 9-7
 - entries_scanned, 9-7
 - entries_skipped, 9-7
 - error_rate, 9-8
 - file, 9-6
 - file_kbytes, 9-7
 - files, 9-7
 - filesystem_errors, 9-7
 - hardlinks, 9-7
 - host, 9-6
 - kbytes_scanned, 9-7
 - mount_points_skipped, 9-7
 - path, 9-8
 - physical_blks_read, 9-8
 - physical_blks_written, 9-8
 - read_errors, 9-8
 - sparse_files, 9-7
 - start_time, 9-7
 - status, 9-6
 - symlinks, 9-7
 - unknown_type, 9-7
 - voltags, 9-6
 - volumes, 9-6
 - write_errors, 9-8
 - wrt_iorate, 9-8
 - wrt_iosecs, 9-8
- backup strategy
 - about, 5-6
 - restore frequency, 5-7
 - typical, 5-7
- backup triggers
 - configuring, 5-19
 - creating daily backup triggers, 5-21
 - creating monthly triggers, 5-23
 - creating quarterly triggers, 5-24
 - creating yearly triggers, 5-25
 - displaying a trigger schedule, 5-27
 - displaying the triggers page, 5-19
 - editing, 5-26
 - removing, 5-26
- backup windows
 - adding, 5-14
 - configuring, 5-13
 - displaying, 5-14
 - removing, 5-15
- backups
 - critical data, 5-34
 - displaying metadata, 4-20
 - full and incremental compared, 5-1
 - listing, 6-14
 - off-site, 5-2
 - on-demand, 5-28
 - privileged, 2-2
 - RMAN and file-system compared, 4-3
 - scheduled, 5-4
 - transient encryption keys, 12-7
 - unprivileged, 2-2
 - validating, 1-28
- barcode
 - extracting a volume, 8-10
 - inserting a volume, 8-9
 - labeling a volume, 8-13
 - loading a volume, 8-12
 - moving a volume, 8-11
- barcode readers
 - about, 1-22
- block size
 - about, 1-29
 - and restore operations, 1-30
- blocking factor
 - about, 1-29
 - and restore operations, 1-30
- borrowing a tape drive, 8-14
- browsing
 - backup catalog, 6-9
 - OSB catalog, 1-5
 - OSB catalog with data selectors, 6-2
 - volumes, 10-1

C

canceling

jobs, [9-10](#)

catalog

about, [1-4](#)

browsing, [1-5](#)

location, [1-4](#), [6-2](#)

Oracle Secure Backup, [1-5](#)

restore operations based on, [6-1](#)

super-directory, [1-5](#)

catalog data

about, [1-3](#)

backup image instances, [1-19](#)

catalog import

cataloging backup catalog data, [1-6](#)

managing catalog imports, [10-10](#)

catalog recovery

about, [13-1](#)

adding files, [13-3](#)

backup jobs, [13-4](#)

datasets, [13-3](#)

disabling backups, [13-2](#)

encryption, [13-4](#)

media families, [13-2](#)

modifying, [13-1](#)

objects, [13-2](#)

summary, [13-3](#)

checking

dataset files, [5-12](#)

checkpoints

about, [5-5](#)

defined, [10-12](#)

displaying, [10-12](#)

removing, [10-12](#)

checksum validation, [1-28](#)

classes

about, [2-5](#)

adding, [2-16](#)

admin, [2-5](#)

configuring, [2-15](#)

definition, [2-1](#)

displaying, [2-15](#)

editing properties, [2-16](#)

operator, [2-5](#)

oracle, [2-5](#)

reader, [2-6](#)

removing, [2-17](#)

renaming, [2-17](#)

user, [2-5](#)

cleaning tape drives, [8-14](#)

client direct to cloud, [1-39](#)

about, [1-39](#)

enabling, [8-21](#), [8-23](#)

closing tape library door, [8-11](#)

cloud storage devices

about, [1-37](#)

displaying properties, [8-21](#)

monitoring and managing, [8-21](#)

monitoring space usage, [8-22](#)

compression

and volume duplication, [11-6](#)

configuration files

about, [1-3](#)

accessing, [1-6](#)

configuring

backup schedules, [5-16](#)

backup triggers, [5-19](#)

backup windows, [5-13](#)

classes, [2-15](#)

database backup storage selectors, [3-6](#)

job summaries, [3-10](#)

media families, [3-1](#)

media families for RMAN, [4-16](#)

RMAN, [4-12](#)

RMAN access to SBT library, [4-13](#)

constrained rotation policy, [11-11](#)

content-managed expiration policies

about, [1-35](#)

creating

backup image instances, [7-3](#)

catalog-based restore request, [6-11](#)

daily backup triggers, [5-21](#)

monthly backup triggers, [5-23](#)

quarterly backup triggers, [5-24](#)

raw restore request, [6-15](#)

yearly backup triggers, [5-25](#)

critical data

backups, [5-34](#)

CROSSCHECK command, [1-36](#), [4-21](#)

customeridstring policy, [11-49](#)

D

daemons

about, [1-13](#)

displaying, [10-13](#)

interaction, [1-16](#)

managing, [10-14](#)

obhttpd, [1-15](#)

obixd, [1-15](#)

obndmpd, [1-15](#)

obpoolmgr, [1-15](#)

obproxyd, [1-16](#)

obrobotd, [1-15](#)

obscheduled, [1-14](#)

observed, [1-14](#)

types, [1-13](#)

viewing properties, [10-15](#)

daily backup

creating triggers, [5-21](#)

- Data ONTAP operating system, [5-5](#)
 - data selectors
 - browsing, [6-2](#)
 - database backup storage selectors
 - configuring, [3-6](#)
 - creating with Oracle Cloud Control, [4-17](#)
 - parameters, [4-4](#)
 - removing, [3-10](#)
 - database recovery
 - with RMAN and OSB, [4-19](#)
 - databases
 - backing up with RMAN and OSB, [4-18](#)
 - recovering with RMAN and OSB, [4-19](#)
 - dataset files
 - about, [5-2](#)
 - adding, [5-11](#)
 - checking, [5-12](#)
 - displaying, [5-11](#)
 - editing, [5-12](#)
 - examples, [5-9](#)
 - location, [5-3](#)
 - OSB catalog recovery, [13-3](#)
 - removing, [5-13](#)
 - renaming, [5-13](#)
 - defaults and policies
 - about, [1-7](#), [2-18](#)
 - autovolumerelease, [11-49](#)
 - classes, [1-7](#)
 - customeridstring, [11-49](#)
 - duplicateovernetwork, [11-50](#)
 - duplicationjobpriority, [11-50](#)
 - minwritablevolumes, [11-49](#)
 - reportretaintime, [11-49](#)
 - vaulting policies, [11-49](#), [11-50](#)
 - viewing, [2-18](#)
 - DELETE command, [4-21](#)
 - deleting
 - backup image instances, [7-5](#)
 - expired backup image instances, [8-20](#), [8-22](#)
 - disabling
 - NUMA awareness, [4-13](#)
 - vaulting scan schedules, [11-43](#)
 - disk pools
 - about, [1-25](#)
 - displaying properties, [8-16](#)
 - managing, [8-16](#)
 - monitoring space usage, [8-16](#)
 - displaying
 - backup catalog, [6-9](#)
 - backup image instances, [7-4](#)
 - backup images, [7-1](#)
 - backup requests, [5-30](#)
 - backup schedules, [5-16](#)
 - backup windows, [5-14](#)
 - checkpoints page, [10-12](#)
 - cloud storage devices, [8-21](#)
 - displaying (*continued*)
 - daemons page, [10-13](#)
 - dataset files, [5-11](#)
 - disk pools, [8-16](#)
 - job summaries, [3-11](#)
 - job transcripts, [9-4](#)
 - libraries page, [8-5](#)
 - media families, [3-3](#)
 - raw media, [6-15](#)
 - trigger schedule, [5-27](#)
 - triggers page, [5-19](#)
 - distribution report
 - defined, [11-4](#), [11-28](#)
 - duplexed backups in Oracle RAC environments, [4-6](#)
 - duplicateovernetwork policy, [11-50](#)
 - duplication
 - adding policies, [11-29](#)
 - adding windows, [11-32](#)
 - and NDMP copy-enabled VTL, [11-8](#)
 - duplicateovernetwork policy, [11-50](#)
 - duplicationjobpriority policy, [11-50](#)
 - editing policies, [11-45](#)
 - exporting duplicate volumes, [11-36](#)
 - failures, [11-35](#)
 - jobs, [11-7](#)
 - original and duplicate volumes, [11-6](#)
 - over network, [11-35](#)
 - priority, [11-34](#)
 - removing policies, [11-45](#)
 - removing windows, [11-47](#)
 - renaming policies, [11-46](#)
 - restore using duplicate volumes, [11-28](#)
 - schedules, [11-7](#)
 - using NDMP copy-enabled VTL, [11-37](#)
 - volume migration, [11-30](#)
 - volumes, [11-6](#)
 - volumes on-demand, [11-7](#)
 - volumes over network, [11-35](#)
 - windows, [11-8](#), [11-32](#)
 - duplication policies
 - duplicateovernetwork, [11-50](#)
 - duplicationjobpriority, [11-50](#)
 - duplicationjobpriority policy, [11-50](#)
- ## E
-
- editing
 - backup image instances, [7-4](#)
 - backup schedules, [5-17](#)
 - backup triggers, [5-26](#)
 - class properties, [2-16](#)
 - dataset files, [5-12](#)
 - job summary schedules, [3-14](#)
 - media family properties, [3-5](#)
 - rotation policies, [11-41](#)

- editing (*continued*)
 - storage locations, [11-39](#)
 - user properties, [2-10](#)
 - encryption
 - about OSB backup encryption, [12-1](#)
 - client level, [12-12](#)
 - example, [12-11](#)
 - file-system backups, [12-5](#)
 - hardware-based, [12-7](#)
 - one-time unencrypted backups, [12-10](#)
 - Oracle Database backups, [12-5](#)
 - OSB administrative data, [12-4](#)
 - OSB catalog recovery, [13-4](#)
 - OSB encryption algorithms, [12-4](#)
 - OSB encryption keys, [12-4](#)
 - OSB encryption options, [12-4](#)
 - OSB encryption rekey frequency, [12-3](#)
 - OSB encryption security, [12-4](#)
 - RMAN and OSB compared, [4-6](#)
 - EOD labels, [1-22](#)
 - EOV labels, [1-23](#)
 - error log
 - tape library, [8-15](#)
 - events
 - rotation policies, [11-12](#)
 - example
 - vaulting environment, [11-37](#)
 - exception report
 - defined, [11-5](#), [11-26](#)
 - expiration date
 - extending, [10-6](#)
 - expiration policies
 - and RMAN, [4-21](#)
 - content-managed, [1-35](#)
 - time-managed, [1-36](#)
 - exporting
 - duplicate volumes, [11-36](#)
 - volumes, [8-8](#)
 - extracting volumes, [8-10](#)
- ## F
-
- failure
 - duplication jobs, [11-35](#)
 - file-system backup catalog
 - browsing, [6-9](#)
 - displaying, [6-9](#)
 - file-system backup jobs
 - about, [1-10](#)
 - file-system backup requests
 - adding one-time request, [5-30](#), [5-32](#)
 - removing, [5-30](#), [5-33](#)
 - file-system backups
 - about scheduled backups, [5-4](#)
 - creating one-time schedule, [5-20](#)
 - critical data, [5-34](#)
 - file-system backups (*continued*)
 - displaying requests, [5-30](#)
 - encryption, [12-5](#)
 - full and incremental compared, [5-1](#)
 - listing, [6-14](#)
 - off-site, [5-2](#)
 - on-demand, [5-28](#)
 - restartable, [5-5](#)
 - file-system restore jobs
 - about, [1-10](#)
 - file-system restore operations
 - about, [6-1](#)
 - catalog-based, [6-1](#)
 - creating a catalog-based request, [6-11](#)
 - creating a raw restore request, [6-15](#)
 - displaying raw media, [6-15](#)
 - raw, [6-1](#)
 - removing a raw restore request, [6-19](#)
 - sending raw restore request to scheduler, [6-19](#)
 - using obtar, [6-2](#)
 - file-system restore requests
 - removing catalog-based request, [6-13](#)
 - sending catalog-based requests to scheduler, [6-14](#)
 - full backups
 - and incremental backups compared, [5-7](#)
- ## H
-
- hardware-based encryption, [12-7](#)
 - logging, [12-9](#)
 - reports, [12-9](#)
- ## I
-
- IBM drive encryption
 - hardware-based, [12-7](#)
 - identifying volumes, [8-11](#)
 - immutable buckets
 - about, [1-40](#), [8-27](#)
 - using, [8-21](#)
 - incremental backups
 - and full backups compared, [5-7](#)
 - index daemon
 - about, [1-15](#)
 - inserting
 - volumes, [8-9](#)
 - Internet Protocol v6
 - and NDMP, [A-1](#)
- ## J
-
- job summaries
 - about, [1-12](#)
 - configuring, [3-10](#)

job summaries (*continued*)displaying, [3-11](#)

job summary schedules

about, [1-12](#)editing, [3-14](#)removing, [3-14](#)

job transcript

backup statistics, [9-6](#)

job transcripts

about, [1-12](#)

jobs

about, [1-9](#)canceling, [9-10](#)dataset, [1-11](#)displaying job transcripts, [9-4](#)duplication job failure, [11-35](#)identifiers, [1-11](#)logs, [1-12](#)managing, [9-1](#)media movement, [11-19](#)priority, [1-11](#)removing, [9-8](#)restore, [1-11](#)resuming, [10-15](#)running, [9-9](#)subordinate, [1-11](#)suspending, [10-15](#)transcripts, [1-12](#)viewing properties, [9-4](#)volume duplication, [11-7](#)

K

keys

OSB backup encryption, [12-4](#)

Llabeling, volumes, [8-13](#)

labels

EOD, [1-22](#)EOV, [1-23](#)

levels

backup encryption, [12-3](#)

library commands

descriptions, [8-6](#)running, [8-5](#)

library page

displaying, [8-5](#)

listing

tape library volumes, [8-5](#)

loading

volumes, [8-12](#)

local backups

and networked backups compared, [4-25](#)

location report

defined, [11-4](#)

locations

about, [11-2](#)adding, [11-9](#)editing, [11-39](#)removing, [11-40](#)renaming, [11-40](#)LTO4 tape drive, [12-7](#)

Mmanaged volumes, [11-1](#)

managing

backup and restore jobs, [9-1](#)backup images, [7-1](#)daemons, [10-14](#)disk pools, [8-16](#)

maximum blocking factor

about, [1-29](#)

media families

about, [1-31](#)adding, [3-3](#)associating with rotation policies, [11-14](#)associating with volume duplication policies,
[11-31](#)configuring, [3-1](#)configuring for RMAN, [4-16](#)default volume sequence files, [1-33](#)displaying with Web tool, [3-3](#)editing properties, [3-5](#)OSB catalog recovery, [13-2](#)removing, [3-6](#)RMAN-DEFAULT, [1-36](#)rotation policy, [1-32](#)user-specified volume ID, [1-34](#)user-specified volume sequence file, [1-33](#)volume expiration policy, [1-31](#)volume identification sequence, [1-31](#)

media life cycle

autovolumerelease policy, [11-49](#)customeridstring policy, [11-49](#)duplicateovernetwork policy, [11-50](#)duplicationjobpriority policy, [11-50](#)minwritablevolumes policy, [11-49](#)reportretaintime, [11-49](#)

media life cycle management

overview, [11-1](#)

media management

adding duplication policies, [11-29](#)adding duplication windows, [11-32](#)adding rotation policies, [11-11](#)adding storage locations, [11-9](#)adding vaulting scan schedules, [11-15](#)adding volume duplication schedules, [11-33](#)and RMAN, [11-51](#)

- media management (*continued*)
 - associating rotation policies with media
 - families, [11-14](#)
 - associating volume duplication policies with
 - media families, [11-31](#)
 - constrained rotation policies, [11-11](#)
 - disabling vaulting scan schedules, [11-43](#)
 - distribution reports, [11-4](#), [11-28](#)
 - duplication job failure, [11-35](#)
 - editing duplication policies, [11-45](#)
 - editing rotation policies, [11-41](#)
 - editing storage locations, [11-39](#)
 - exception reports, [11-5](#), [11-26](#)
 - exporting duplicate volumes, [11-36](#)
 - location reports, [11-4](#)
 - locations, [11-2](#)
 - managed and unmanaged volumes, [11-1](#)
 - media movement jobs, [11-19](#)
 - minimum writeable volumes, [11-22](#)
 - missing volume reports, [11-5](#)
 - network volume duplication, [11-35](#)
 - on-demand duplication, [11-7](#)
 - original and duplicate volumes, [11-6](#)
 - pick and distribution reports, [11-28](#)
 - pick reports, [11-4](#), [11-28](#)
 - removing duplication policies, [11-45](#)
 - removing duplication windows, [11-47](#)
 - removing rotation policies, [11-42](#)
 - removing storage locations, [11-40](#)
 - removing volume duplication schedules,
 - [11-48](#)
 - renaming duplication policies, [11-46](#)
 - renaming rotation policies, [11-42](#)
 - renaming storage locations, [11-40](#)
 - reports, [11-3](#)
 - restore using duplicate volumes, [11-28](#)
 - rotation policies, [11-11](#)
 - rotation policy events, [11-12](#)
 - running media movement jobs, [11-19](#)
 - schedule reports, [11-4](#)
 - storage locations, [11-9](#)
 - tape volume recall, [11-27](#)
 - unconstrained rotation policies, [11-11](#)
 - vaulting environment example, [11-37](#)
 - vaulting scan schedules, [11-15](#)
 - vaulting scans, [11-3](#)
 - volume duplication, [11-6](#)
 - volume duplication jobs, [11-7](#)
 - volume duplication policies, [11-29](#)
 - volume duplication priority, [11-34](#)
 - volume duplication schedules, [11-7](#), [11-33](#)
 - volume duplication windows, [11-8](#), [11-32](#)
 - volume migration, [11-30](#)
 - media management parameters
 - SBT_LIBRARY, [4-14](#)
 - setting in RMAN, [4-18](#)
 - media movement
 - pick and distribution reports, [11-28](#)
 - media movement jobs
 - about, [11-19](#)
 - running, [11-19](#)
 - metadata
 - displaying, [4-20](#)
 - migration
 - volumes, [11-30](#)
 - minimum writeable volumes, [11-22](#)
 - minimumwriteablevolumes policy, [11-49](#)
 - missing volumes report
 - defined, [11-5](#)
 - modifying
 - OSB catalog recovery, [13-1](#)
 - mounting volumes, [8-2](#)
 - moving
 - volumes, [8-10](#)
- ## N
-
- naming
 - users, [2-8](#)
 - NDMP
 - and Internet Protocol v6, [A-1](#)
 - daemon, [1-15](#)
 - hosts, [2-2](#)
 - incremental restore operation, [6-12](#)
 - NDMP copy-enabled VTL
 - about, [11-8](#)
 - NDMP volume duplication
 - using, [11-37](#)
 - network
 - volume duplication over, [11-35](#)
 - networked backups
 - and local backups compared, [4-25](#)
 - NUMA
 - disabling, [4-13](#)
 - NUMA support, [4-12](#)
- ## O
-
- OB_ENCRYPTION parameter settings, [12-5](#)
 - observed
 - about, [1-14](#)
 - obtar
 - restoring files with, [6-2](#)
 - off-site backups, [5-2](#)
 - on-demand
 - backups, [5-28](#)
 - duplication, [11-7](#)
 - opening
 - tape library door, [8-11](#)
 - operator class
 - about, [2-5](#)

- oracle class
 - about, [2-5](#)
 - Oracle Database backups
 - encryption, [12-5](#)
 - Oracle RAC
 - duplexed backups, [4-6](#)
 - installing OSB in an Oracle RAC environment, [4-24](#)
 - networked and local backups compared, [4-25](#)
 - using Oracle Secure Backup with, [4-24](#)
 - Oracle Secure Backup
 - features, [1-1](#)
 - Oracle Secure Backup catalog
 - about, [1-5](#)
 - accessing, [1-6](#)
 - Oracle Secure Backup daemons
 - about, [1-13](#)
 - interaction, [1-16](#)
 - obhttpd, [1-15](#)
 - obixd, [1-15](#)
 - obndmpd, [1-15](#)
 - obpoolmgr, [1-15](#)
 - obproxyd, [1-16](#)
 - obrobotd, [1-15](#)
 - obscheduled, [1-14](#)
 - observed, [1-14](#)
 - types, [1-13](#)
 - oracle secure backup using multipart upload
 - about, [1-38](#)
 - OSB backup encryption
 - about, [12-1](#)
 - administrative data, [12-4](#)
 - algorithms, [12-4](#)
 - client level, [12-12](#)
 - example, [12-11](#)
 - hardware-based, [12-7](#)
 - keys, [12-4](#)
 - one-time unencrypted backups, [12-10](#)
 - options, [12-4](#)
 - rekey frequency, [12-3](#)
 - security, [12-4](#)
 - OSB catalog
 - about, [1-4](#)
 - and RMAN catalog compared, [4-11](#)
 - browsing, [1-5](#)
 - browsing with data selectors, [6-2](#)
 - location, [1-4](#), [6-2](#)
 - super-directory, [1-5](#)
 - view modes, [6-4](#)
 - OSB catalog recovery
 - about, [13-1](#)
 - adding files, [13-3](#)
 - backup jobs, [13-4](#)
 - datasets, [13-3](#)
 - disabling backups, [13-2](#)
 - encryption, [13-4](#)
 - OSB catalog recovery (*continued*)
 - media families, [13-2](#)
 - modifying, [13-1](#)
 - objects, [13-2](#)
 - summary, [13-3](#)
 - OSB dataset files
 - about, [5-2](#)
 - adding, [5-11](#)
 - checking, [5-12](#)
 - editing, [5-12](#)
 - location, [5-3](#)
 - removing, [5-13](#)
 - renaming, [5-13](#)
 - OSB encryption
 - and RMAN encryption compared, [4-6](#)
 - catalog recovery, [13-4](#)
 - hardware-based, [12-7](#)
 - OSB users
 - about, [2-1](#)
 - adding, [2-8](#)
 - and operating system accounts, [2-2](#)
 - assigning preauthorized access, [2-13](#)
 - assigning Windows account information, [2-12](#)
 - changing passwords, [2-10](#)
 - configuring, [2-6](#)
 - configuring preauthorized for RMAN, [4-16](#)
 - creating preauthorized for RMAN, [4-14](#)
 - definition, [2-1](#)
 - displaying in Web tool, [2-7](#)
 - editing properties, [2-10](#)
 - illustrated preauthorized for RMAN, [4-14](#)
 - naming, [2-8](#)
 - passwords, [2-8](#)
 - preauthorization, [2-2](#)
 - removing, [2-14](#)
 - removing preauthorized access, [2-14](#)
 - removing Windows account information, [2-12](#)
 - renaming, [2-14](#)
 - rights, [2-5](#)
- ## P
-
- passwords
 - changing, [2-10](#)
 - forcing password change, [2-4](#)
 - security policies, [2-3](#)
 - setting, [2-8](#)
 - setting grace time, [2-4](#), [2-9](#)
 - setting lifetime, [2-4](#), [2-9](#)
 - setting reuse time, [2-4](#), [2-9](#)
 - pick report
 - defined, [11-4](#), [11-28](#)
 - policies
 - about, [2-18](#)
 - adding duplication policies, [11-29](#)
 - backup encryption, [12-2](#)

- policies (*continued*)
 - editing duplication policies, [11-45](#)
 - hardware-based encryption, [12-10](#)
 - removing duplication policies, [11-45](#)
 - renaming duplication policies, [11-46](#)
 - resetting to default, [2-19](#)
 - setting, [2-19](#)
 - viewing, [2-18](#)
 - volume duplication, [11-29](#)
 - pool manager daemon
 - about, [1-15](#)
 - preauthorized access
 - assigning to users, [2-13](#)
 - removing, [2-14](#)
 - preauthorized users
 - configuring for RMAN, [4-16](#)
 - creating for RMAN, [4-14](#)
 - illustrated for RMAN, [4-14](#)
 - priority
 - volume duplication, [11-34](#)
 - privileged backups, [2-2](#)
 - properties
 - daemons, [10-15](#)
 - jobs, [9-4](#)
 - proxy daemon
 - about, [1-16](#)
- ## R
-
- raw restore operations
 - creating a request, [6-15](#)
 - removing a request, [6-19](#)
 - reader class, [2-6](#)
 - recall volumes, [11-27](#)
 - recovering a database
 - with RMAN and OSB, [4-19](#)
 - rekey frequency
 - OSB backup encryption, [12-3](#)
 - removing
 - backup requests, [5-30](#), [5-33](#)
 - backup schedules, [5-18](#), [5-19](#)
 - backup windows, [5-15](#)
 - catalog-based restore request, [6-13](#)
 - checkpoints, [10-12](#)
 - classes, [2-17](#)
 - database backup storage selectors, [3-10](#)
 - dataset files, [5-13](#)
 - duplication windows, [11-47](#)
 - job summary schedules, [3-14](#)
 - jobs, [9-8](#)
 - media families, [3-6](#)
 - raw restore request, [6-19](#)
 - rotation policies, [11-42](#)
 - storage locations, [11-40](#)
 - triggers, [5-26](#)
 - users, [2-14](#)
 - removing (*continued*)
 - volume duplication schedules, [11-48](#)
 - renaming
 - backup images, [7-2](#)
 - backup schedules, [5-18](#)
 - classes, [2-17](#)
 - dataset files, [5-13](#)
 - rotation policies, [11-42](#)
 - storage locations, [11-40](#)
 - users, [2-14](#)
 - reports
 - customeridstring policy, [11-49](#)
 - hardware-based encryption, [12-9](#)
 - media management, [11-3](#)
 - reportretaintime policy, [11-49](#)
 - reservations
 - managing tape library reservations, [8-21](#)
 - tape library, [8-21](#)
 - restartable backups
 - about, [5-5](#)
 - checkpoints, [5-5](#)
 - restore
 - using duplicate volumes, [11-28](#)
 - restore frequency
 - backup strategy, [5-7](#)
 - restore jobs
 - about, [1-11](#)
 - canceling, [9-10](#)
 - displaying job transcripts, [9-4](#)
 - file-system, [1-10](#)
 - managing, [9-1](#)
 - multiple, [1-11](#)
 - removing, [9-8](#)
 - resuming, [10-15](#)
 - running, [9-9](#)
 - suspending, [10-15](#)
 - viewing properties, [9-4](#)
 - restore operations
 - about, [6-1](#)
 - catalog-based, [6-1](#)
 - creating a raw restore request, [6-15](#)
 - displaying raw media, [6-15](#)
 - raw, [6-1](#)
 - removing a raw restore request, [6-19](#)
 - sending raw restore request to scheduler, [6-19](#)
 - using obtar, [6-2](#)
 - using wildcard pattern matching, [6-1](#)
 - restore request
 - creating a catalog-based request, [6-11](#)
 - removing catalog-based request, [6-13](#)
 - restore requests
 - about, [1-9](#)
 - sending catalog-based requests to scheduler, [6-14](#)

resuming
 backup and restore jobs, [10-15](#)
 retention rule
 compliance rule, [1-40](#), [8-27](#)
 legal hold, [1-40](#), [8-27](#)
 returning a tape drive, [8-15](#)
 reusing volumes, [8-15](#)
 rights
 about, [2-5](#)
 RMAN
 and media management, [11-51](#)
 and Oracle Secure Backup, [4-1](#)
 and vaulting, [11-51](#)
 communication with Oracle Secure Backup,
 [4-10](#)
 configuring access to SBT library, [4-13](#)
 configuring media families, [4-16](#)
 displaying backup piece information, [4-23](#)
 expiration policy, [4-21](#)
 performing backups with OSB, [4-18](#)
 recovering a database with OSB, [4-19](#)
 setting media management parameters, [4-18](#)
 using with Oracle Secure Backup, [4-12](#)
 RMAN and backup encryption, [12-6](#)
 RMAN backup sets
 and OSB backup images compared, [4-3](#)
 RMAN backups
 crosschecking, [4-21](#)
 displaying information about, [4-21](#)
 RMAN catalog
 and OSB catalog compared, [4-11](#)
 RMAN commands
 CROSSCHECK, [1-36](#), [4-21](#)
 DELETE, [4-21](#)
 RMAN encryption
 and OSB encryption compared, [4-6](#)
 RMAN-DEFAULT media family
 about, [1-36](#)
 robot daemon
 about, [1-15](#)
 rotation policies
 about, [11-11](#)
 adding, [11-11](#)
 associating with media families, [11-14](#)
 constrained and unconstrained compared,
 [11-11](#)
 editing, [11-41](#)
 events, [11-12](#)
 minimum writeable volumes, [11-22](#)
 removing, [11-42](#)
 renaming, [11-42](#)
 rotation policy
 and media family, [1-32](#)
 running jobs, [9-9](#)

S

SBT errors, displaying, [4-23](#)
 SBT interface
 about, [4-1](#)
 SBT library
 configuring RMAN access, [4-13](#)
 SBT_LIBRARY parameter, [4-14](#)
 schedule daemon
 about, [1-14](#)
 schedule report
 defined, [11-4](#)
 scheduled backups
 about, [5-4](#)
 scheduler
 catalog-based restore requests, [6-14](#)
 job priority, [1-11](#)
 raw restore request, [6-19](#)
 schedules
 adding backup schedules, [5-16](#)
 adding vaulting scan schedules, [11-15](#)
 adding volume duplication schedules, [11-33](#)
 backup, [5-7](#)
 creating one-time backup schedule, [5-20](#)
 disabling vaulting scan schedules, [11-43](#)
 displaying backup schedules, [5-16](#)
 editing backup schedules, [5-17](#)
 job summary, [1-12](#)
 removing backup schedules, [5-18](#), [5-19](#)
 removing volume duplication schedules,
 [11-48](#)
 renaming backup schedules, [5-18](#)
 vaulting scan, [11-15](#)
 volume duplication, [11-7](#), [11-33](#)
 section numbers
 about, [1-24](#)
 Secure Sockets Layer
 See SSL
 security
 OSB backup encryption, [12-4](#)
 sending
 catalog-based restore requests to scheduler,
 [6-14](#)
 raw restore request to scheduler, [6-19](#)
 sequence numbers
 about, [1-23](#)
 service daemon, [1-14](#)
 setting
 policies, [2-19](#)
 space usage
 cloud storage devices
 monitoring, [8-22](#)
 disk pools
 monitoring, [8-16](#)
 SSL, [1-2](#)
 stage loops, [14-3](#)

- staging
 - default stage rule, [14-3](#)
 - setting up, [14-4](#)
- statistics
 - backup, [9-6](#)
- storage locations
 - about, [11-9](#)
 - adding, [11-9](#)
 - editing, [11-39](#)
 - removing, [11-40](#)
 - renaming, [11-40](#)
- strategy
 - backups, [5-6](#)
- summaries
 - job, [1-12](#)
- summary
 - OSB catalog recovery, [13-3](#)
- super-directory
 - OSB catalog, [1-5](#)
- suspending
 - backup and restore jobs, [10-15](#)

T

- tape drive
 - borrowing, [8-14](#)
 - cleaning, [8-14](#)
 - encryption-capable, [12-7](#)
 - managing, [8-5](#)
 - returning, [8-15](#)
 - viewing properties, [8-2](#)
- tape libraries
 - minwritablevolumes policy, [11-49](#)
- tape library
 - automatic tape unloading, [8-3](#)
 - borrowing a tape drive, [8-14](#)
 - cleaning tape drives, [8-14](#)
 - closing a door, [8-11](#)
 - error log, [8-15](#)
 - identifying volumes, [8-11](#)
 - labeling volumes, [8-13](#)
 - loading volumes, [8-12](#)
 - managing, [8-5](#)
 - managing reservations, [8-21](#)
 - opening door, [8-11](#)
 - reservations, [8-21](#)
 - returning a tape drive, [8-15](#)
 - reusing volumes, [8-15](#)
 - unlabeling volumes, [8-14](#)
 - unloading volumes, [8-13](#)
 - viewing properties, [8-5](#)
 - volumes list, [8-5](#)
- tape volume recall, [11-27](#)
- time-managed expiration policies, [1-36](#)
- transcript
 - backup statistics, [9-6](#)

- transcripts
 - displaying job transcripts, [9-4](#)
 - job, [1-12](#)
- transient encryption, [12-7](#)
- triggers
 - configuring, [5-19](#)
 - creating daily backup triggers, [5-21](#)
 - creating monthly backup, [5-23](#)
 - creating one-time backup, [5-20](#)
 - creating quarterly backup triggers, [5-24](#)
 - creating yearly backup triggers, [5-25](#)
 - displaying a trigger schedule, [5-27](#)
 - displaying the triggers page, [5-19](#)
 - editing, [5-26](#)
 - removing, [5-26](#)

U

- unconstrained rotation policy, [11-11](#)
- unlabeling volumes, [8-14](#)
- unloading
 - automatic, [8-3](#)
 - volumes, [8-13](#)
- unmanaged volumes, [11-1](#)
- unmounting volumes, [8-2](#)
- unprivileged backups, [2-2](#)
- updating
 - library inventory, [8-7](#)
- user class, [2-5](#)
- users
 - about, [2-1](#)
 - adding, [2-8](#)
 - and operating system accounts, [2-2](#)
 - assigning preauthorized access, [2-13](#)
 - assigning Windows account information, [2-12](#)
 - changing passwords, [2-10](#)
 - configuring, [2-6](#)
 - configuring preauthorized for RMAN, [4-16](#)
 - creating preauthorized for RMAN, [4-14](#)
 - displaying in Web tool, [2-7](#)
 - editing properties, [2-10](#)
 - illustrated preauthorized for RMAN, [4-14](#)
 - naming, [2-8](#)
 - passwords, [2-8](#)
 - preauthorizations, [2-2](#)
 - removing, [2-14](#)
 - removing preauthorized access, [2-14](#)
 - removing Windows account information, [2-12](#)
 - renaming, [2-14](#)
 - rights, [2-5](#)

V

- validating backups, [1-28](#)
- vaulting
 - adding rotation policies, [11-11](#)

vaulting (*continued*)

- adding storage locations, [11-9](#)
- adding vaulting scan schedules, [11-15](#)
- adding volume duplication policies, [11-29](#)
- adding volume duplication schedules, [11-33](#)
- adding volume duplication windows, [11-32](#)
- and RMAN, [11-51](#)
- associating rotation policies with media families, [11-14](#)
- associating volume duplication policies with media families, [11-31](#)
- autovolumerelease policy, [11-49](#)
- constrained and unconstrained rotation policies, [11-11](#)
- customeridstring policy, [11-49](#)
- disabling vaulting scan schedules, [11-43](#)
- distribution reports, [11-4](#), [11-28](#)
- duplicateovernetwork policy, [11-50](#)
- duplication over network, [11-35](#)
- duplicationjobpriority policy, [11-50](#)
- editing rotation policies, [11-41](#)
- editing storage locations, [11-39](#)
- editing volume duplication policies, [11-45](#)
- editing volume duplication schedules, [11-48](#)
- example, [11-37](#)
- exception reports, [11-5](#), [11-26](#)
- exporting duplicate volumes, [11-36](#)
- location reports, [11-4](#)
- locations, [11-2](#)
- managed and unmanaged volumes, [11-1](#)
- media movement jobs, [11-19](#)
- minimum writable volumes, [11-22](#)
- minwritablevolumes policy, [11-49](#)
- missing volume reports, [11-5](#)
- on-demand volume duplication, [11-7](#)
- original and duplicate volumes, [11-6](#)
- overview, [11-1](#)
- pick and distribution reports, [11-28](#)
- pick reports, [11-4](#), [11-28](#)
- recalling volumes, [11-27](#)
- removing rotation policies, [11-42](#)
- removing storage locations, [11-40](#)
- removing volume duplication policies, [11-45](#)
- removing volume duplication schedules, [11-48](#)
- removing volume duplication windows, [11-47](#)
- renaming rotation policies, [11-42](#)
- renaming storage locations, [11-40](#)
- renaming volume duplication policies, [11-46](#)
- renaming volume duplication schedules, [11-48](#)
- reportretaintime policy, [11-49](#)
- reports, [11-3](#)
- restore using duplicate volumes, [11-28](#)
- rotation policies, [11-11](#)
- rotation policy events, [11-12](#)

vaulting (*continued*)

- running media movement jobs, [11-19](#)
- schedule reports, [11-4](#)
- vaulting scan schedules, [11-15](#)
- vaulting scans, [11-3](#)
- volume duplication, [11-6](#)
- volume duplication failures, [11-35](#)
- volume duplication jobs, [11-7](#)
- volume duplication policies, [11-29](#)
- volume duplication priority, [11-34](#)
- volume duplication schedules, [11-7](#), [11-33](#)
- volume duplication windows, [11-8](#)
- volume migration, [11-30](#)
- vaulting policies
 - about, [11-49](#), [11-50](#)
 - autovolumerelease, [11-49](#)
 - customeridstring, [11-49](#)
 - minimumwriteablevolumes, [11-49](#)
- vaulting scan schedules, [11-15](#)
- vaulting scans
 - about, [11-3](#)
 - adding schedules, [11-15](#)
 - disabling schedules, [11-43](#)
- view modes
 - exact, [6-5](#)
 - inclusive, [6-5](#)
 - OSB catalog, [6-4](#)
 - specific, [6-5](#)
- viewing
 - tape drive properties, [8-2](#)
 - tape library properties, [8-5](#)
- volume duplication
 - adding schedules, [11-33](#)
 - and NDMP copy-enabled VTL, [11-8](#)
 - removing schedules, [11-48](#)
 - using NDMP copy-enabled VTL, [11-37](#)
- volume duplication policies
 - about, [11-29](#)
 - associating with media families, [11-31](#)
- volume duplication schedules
 - about, [11-33](#)
- volume expiration policy
 - and media family, [1-31](#)
- volume ID
 - user-specified, [1-34](#)
- volume identification sequence
 - and media family, [1-31](#)
- volume sequence files
 - default, [1-33](#)
 - user-specified, [1-33](#)
- volume sets
 - about, [1-23](#)
- volumes
 - about, [1-21](#)
 - adding duplication policies, [11-29](#)
 - adding duplication windows, [11-32](#)

volumes (continued)

- automatic unloading, [8-3](#)
- autovolumerelease policy, [11-49](#)
- browsing, [10-1](#)
- closing a door, [8-11](#)
- duplicating, [11-6](#)
- duplication job failure, [11-35](#)
- duplication jobs, [11-7](#)
- duplication priority, [11-34](#)
- duplication schedules, [11-7](#)
- duplication windows, [11-8](#), [11-32](#)
- editing duplication policies, [11-45](#)
- exporting, [8-8](#)
- exporting duplicates, [11-36](#)
- extending expiration date, [10-6](#)
- extracting, [8-10](#)
- identifying, [8-11](#)
- inserting, [8-9](#)
- inventory update, [8-7](#)
- labeling, [8-13](#)
- library listing, [8-5](#)
- loading, [8-12](#)
- managed and unmanaged compared, [11-1](#)
- migration, [11-30](#)
- minimum writeable, [11-22](#)
- minwritablevolumes policy, [11-49](#)
- mounting, [8-2](#)
- moving, [8-10](#)
- network duplication, [11-35](#)

volumes (continued)

- on-demand duplication, [11-7](#)
- opening a door, [8-11](#)
- original and duplicate volumes, [11-6](#)
- recall, [11-27](#)
- removing duplication policies, [11-45](#)
- removing duplication windows, [11-47](#)
- renaming duplication policies, [11-46](#)
- restore using duplicates, [11-28](#)
- reusing, [8-15](#)
- storage locations, [11-9](#)
- tags, [1-22](#)
- tracking through a vaulting environment, [11-37](#)
- unlabeling, [8-14](#)
- unloading, [8-13](#)
- unmounting, [8-2](#)

W**windows**

- adding duplication windows, [11-32](#)
- removing duplication windows, [11-47](#)
- volume duplication, [11-8](#), [11-32](#)

Windows account information

- assigning to users, [2-12](#)
- removing, [2-12](#)