Oracle® Secure Backup

Administrator's Guide

Release 10.2

E05407-02

July 2008

ORACLE®

Oracle Secure Backup Administrator's Guide, Release 10.2

E05407-02

Primary Author: Craig B. Foch

Contributing Authors: Lance Ashdown, Paul Gavin, Antonio Romero

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

Contents

5 Backing Up File System Data

8 Performing Maintenance

Part IV Advanced Topics

9 Vaulting

10 Managing Backup Encryption

11 Oracle Secure Backup Catalog Recovery

Preface

This preface contains these topics:

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

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

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.

- *Oracle Secure Backup Migration Guide*

  This book explains how to migrate from Reliaty Backup to Oracle Secure Backup. It also explains how to migrate to Oracle Secure Backup from versions of Legato Storage Manager and Legato Single Server Version previously bundled with Oracle Database.

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/technology/products/secure-backup`

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Oracle Secure Backup Concepts

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

This part contains these chapters:

1

Oracle Secure Backup Concepts

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

This chapter contains these sections:

Oracle Secure Backup Features

Oracle Secure Backup provides reliable, centralized tape backup management, protecting file system data and Oracle Database files. The Oracle Secure Backup **SBT interface** enables you to use **Recovery Manager (RMAN)** to back up and restore Oracle Database files to and from tape. Oracle Secure Backup supports almost every **tape drive** and **tape library** in **Storage Area Network (SAN)** and **Small Computer System Interface (SCSI)** environments.

Oracle Secure Backup enables you to do the following:

- Centrally manage tape backup and restore operations of distributed, mixed-platform environments

  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
- Encrypt all stored data

  See Also: Chapter 10, "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 more than one **tape device**

  You can specify a different **media family** or tape device for each copy of the data.
- Create backups that span more than one **volume**
- 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

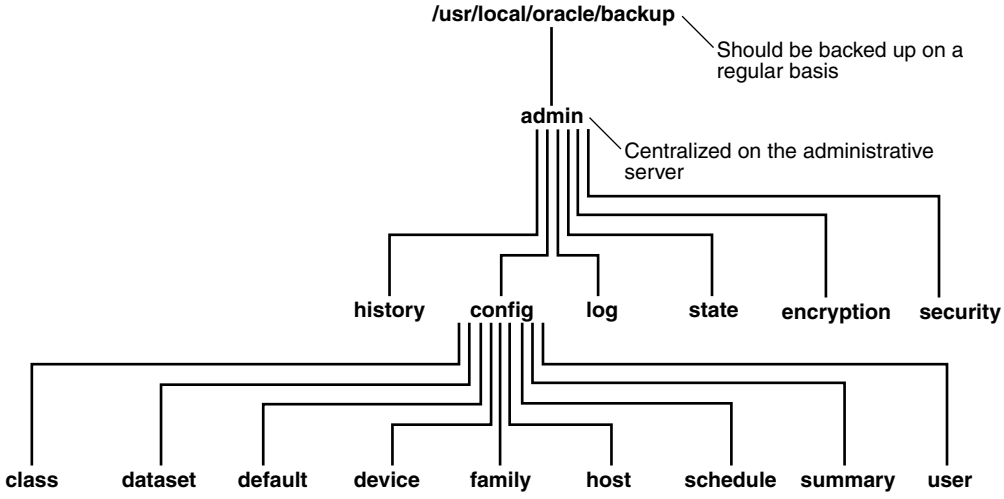
  By default, **Secure Sockets Layer (SSL)** is used for **host authentication** and communication in the **administrative domain**.
- Manage media rotation from one **location** to another
- Automate tape duplication with user-defined policies

Administrative Domains, Catalog Data and Configuration Files

An **administrative domain** is a network of hosts that you manage as a common unit to perform backup and restore operations. 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 is the directory in which Oracle Secure Backup is installed.

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



Oracle Secure Backup administrative data includes configuration data about each domain-wide entity, such as a **class**, a **tape device**, or a **media family**. As shown in Figure 1–1, the config directory contains several subdirectories, each of which represents an **object** that Oracle Secure Backup maintains. In each object directory, Oracle Secure Backup maintains files describing the characteristics of the corresponding object.

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 of these subdirectories contains 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 in size.

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 tape. If the catalog data is lost, for example because a disk fails, then you can restore the most recently backed up catalog from tape 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

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

Table 1–1 (Cont.) Oracle Secure Backup Daemons by Host Type

Daemon	Administrative Server	Media Server	Client
Schedule	yes	no	no
Index	yes	no	no
Apache Web Server	yes	no	no
NDMP	yes	yes	yes
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
- Proxy Daemon

Service Daemon

The observiced **service daemon** provides a wide variety of services. It runs continually on the **administrative server**, **media server**, and **client**.

On the administrative server, observiced 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 **administrative domain**. observiced 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. observiced starts the schedule daemon and the **Apache Web server** during initialization.

When running on a media server or client, observiced 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 **tape device** in the **administrative 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 **Recovery Manager (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 **Network Data Management Protocol (NDMP) tape service** and provides data communication between the **media server** and the **client**. This daemon runs on both the **client** and the 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**. There are two instances of obndmpd running during an active backup or restore operation. If the same host is acting as both the media server and the client, then there are three instances of obndmpd: 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.

Proxy Daemon

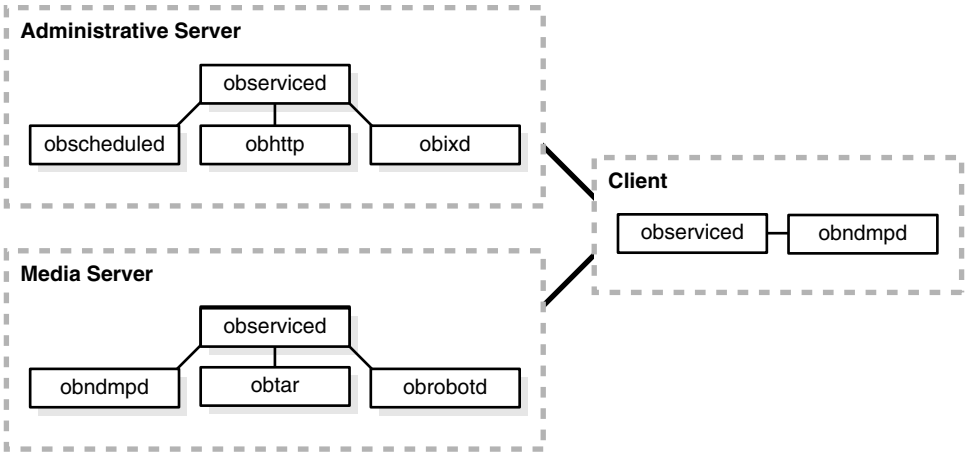
The obproxyd daemon verifies user access for SBT backup and restore operations. The proxy daemon runs on the host that contains the SBT library accessed during the operations. The invocation of the proxy daemon is platform-specific.

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

Figure 1–2 provides a simplified graphical illustration of the relationships among the **daemons** on an **administrative server**, **media server**, and **client**.

Figure 1–2 Daemons in an Administrative Domain



The client host in Figure 1–2 shows an **obtar** instance, but obtar is not itself a daemon. It is the underlying Oracle Secure Backup engine that manipulates the data and tape services 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 observiced daemons are running on all hosts, the observiced 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 observiced to run the backup job.
2. observiced on the administrative server sends a request to obrobotd on the media server to mount the each **volume** required for the backup job.
3. observiced on the administrative server sends a request to observiced 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 tape.

   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 software 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.

Defaults and Policies

Oracle Secure Backup **defaults and policies** control how Oracle Secure Backup operates within an **administrative domain**. Policy settings are maintained on the **administrative server**.

Oracle Secure Backup policies are grouped into several policy classes. Each policy class contains policies that describe a particular area of Oracle Secure Backup operations. The policy classes related to managing Oracle Secure Backup backup and restore functions are as follows:

- 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**.

- 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 domain-wide media management. For example, you can specify a **retention period** for tapes that are members of the `null` **media family**.

- NDMP policies

  These policies specify **Network Data Management Protocol (NDMP)** defaults. For example, you can 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 scheduler. For example, you can specify a frequency at which the scheduler attempts to dispatch backup jobs.

- Storage encryption policies

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

- Vaulting policies

  These policies control the rotation of tapes among from one **location** to another as part of a data protection strategy.

- Volume 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.

See Also: *Oracle Secure Backup Reference* for more information on Oracle Secure Backup policies

Backup Images and Media

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 1–3 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 single unit of media, such as an 8mm tape.
- A **backup section** is the part of a backup image that fits on one physical volume.
- A **backup image** is the product of a backup operation.

Figure 1–3 Backup Images, Backup Sections, and Volumes

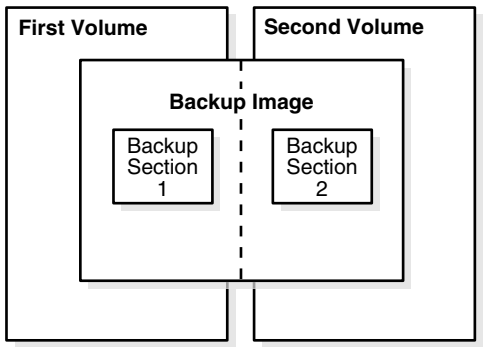
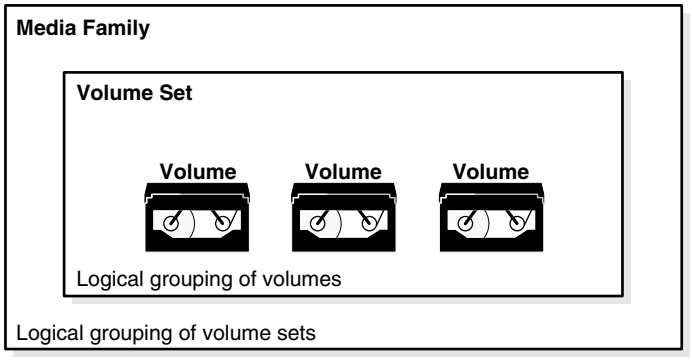


Figure 1–4 provides a graphical illustration of how a **volume set** is related to a **media family**. The concepts are as follows:

- A volume set is a logical grouping of one or more physical volumes spanned by a backup image.
- 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 1–4 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.

This section contains these topics:

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 will use. 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 will be 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 on the `obtar -b` option and the `operations/backupoptions` policy

- Configuration of the tape drive to be used

  You can specify what blocking factor and/or maximum blocking factor 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 on configuring a tape drive

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

  See Also: *Oracle Secure Backup Reference* for more information on the `media/blockingfactor` and `media/maxblockingfactor` policies

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

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 as a result of 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 OS will have a limitation that supersedes all other considerations.

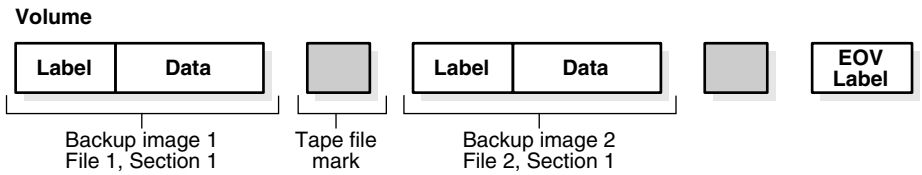
When Oracle Secure Backup begins a restore operation, it does not know what block size was used to write a given tape. Because issuing a read for a too-small block would result in an error condition and a need to reposition the tape, Oracle Secure Backup always starts a restore operation by reading the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

After the first read from the backup image, 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.

Backup Images and Sections

When you run a backup operation in Oracle Secure Backup, you generate a **backup image** on tape. As shown in Figure 1–5, a backup image is a file that consists of at least one **backup section**.

Figure 1–5 Backup Images and Backup Sections



A backup image is uniquely identified in the Oracle Secure Backup **catalog** by its backup ID. Similarly, a backup section is uniquely identified in the catalog by its backup section ID. Example 1–1 shows output from the `lsbu` command for a backup with the ID of `1`.

Example 1–1 Backup

```
ob> lsbu 1
      Backup       Backup  Volume            Volume          File Sect Backup
   Date and Time       ID  ID                Tag                #    #  Level
2005/07/13.11:56:58     1  VOL000003              ADE203        1    1      0
```

Example 1–2 shows output from the `lssection` command for the backup section belonging to the backup shown in Example 1–1.

Example 1–2 Backup Section

```
ob> lssection --vid VOL000003 --file 1
   BSOID  Volume         File Sect  Level  Client        Created     Attributes
     107  VOL000003         1 1         0  brhost2       07/13.11:56 never expires
```

See Also: *Oracle Secure Backup Reference* for complete syntax and semantics for the `lsbu` and `lssection` commands.

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 one of the ways described in "Volumes in a Media Family" on page 1-15.

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. Many libraries are equipped with barcode readers, which enables Oracle Secure Backup to determine the identity of a tape without having to load it and read the **volume label**. Oracle Secure Backup remembers the relationship between a volume tag and each **backup image** it contains in the **catalog**.

Backup Image 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** is referred to as a **backup image label**. It contains the file number, section number, and owner of the backup image.

When a label is displayed, volume-related information is displayed with the header `Volume label` and backup image-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 backup images adhere to the IEEE POSIX.1 data archiving format. Oracle Secure Backup numbers each backup image on a labeled **volume set** with a backup image file number, starting from 1.

When Oracle Secure Backup writes multiple backup images on a **volume**, it places a tape file mark after each backup image. 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 1–6 illustrates the format of a volume that contains two backup images. This figure shows the position of the labels and tape file marks.

Figure 1–6 Two Backup Images on a Volume

Backup images and volume labels, as well as the special `End of Data` and `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 on the volume. Similarly, a backup image label contains

information about the following backup image 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 1–6 is the first volume in the set. The volume label for the first backup image could look like the one in Example 1–3.

Example 1–3 Backup Image 1

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

The volume label for the second backup image could look like the one in Example 1–4.

Example 1–4 Backup Image 2

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

After Oracle Secure Backup creates a backup image, 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 without rewinding the volume.

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

Volume Sets

Oracle Secure Backup enables a single **backup image** to span more than one **volume**. A **volume set** is a set 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 one greater than the sequence number of the previous volume. Consequently, you can back up or restore large amounts of data in a single session.

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

- EOV labels

  If a backup image 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`.

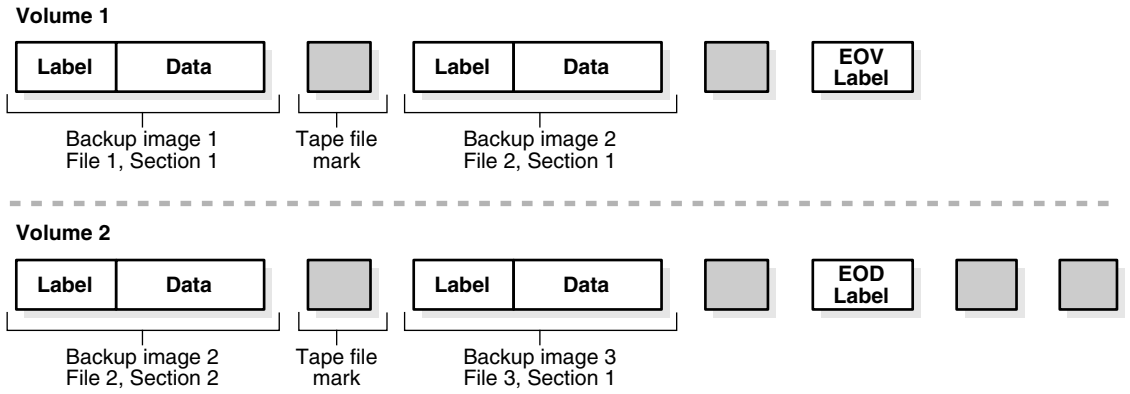
- Section numbers

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

  Note: The section number will always be 1 unless the backup image spans volumes

Figure 1–7 illustrates a volume set that contains three backup images. Backup image 2 spans two volumes.

Figure 1–7 A Single Backup Image on Multiple Volumes



A partial volume label for the first backup image could look like the one shown in Example 1–5.

Example 1–5 Backup Image 1, Section 1

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

The partial volume label for the first section of the second backup image could look like the one shown in Example 1–6.

Example 1–6 Backup Image 2, Section 1

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

The partial volume label for the second section of the second backup image could look like the one shown in Example 1–7.

Example 1–7 Backup Image 2, Section 2

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

The partial volume label for the second section of the second backup image could look like the one shown in Example 1–8.

Example 1–8 Backup Image 3, Section 1

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

Media Families

A **media family** is a named classification of volume sets. This classification ensures that volumes 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.

Media Family Attributes

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 the following occurs:

  – The tape is written to for the first time.

  – The tape is overwritten from the beginning of tape.

  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.

- Volume expiration policy

  A media family can have either of the following mutually exclusive volume **expiration policy** types: content-managed, which is the default, or time-managed. When a **volume set** is expired, Oracle Secure Backup automatically considers each volume in the set eligible to be overwritten and recycled. If the volume set is content-managed, then an individual volume of the set can expire before the remainder of the set.

As a general rule, although a volume might be unexpired and have unused tape remaining, Oracle Secure Backup will not write to a volume whose sequence number is lower than the most recent **volume sequence number** for the media family. Every backup tries to append to the most recent volume in the media family. If this volume is full, then it writes to a new one.

There is an exception to this general rule. If you are having problems with a media family, then you might choose to delete it and create a new one with the same name, rather than modifying the existing media family. Each time a media family is re-created, the volume sequence number resets to zero. In this exceptional case, you can end up writing to a volume with a lower sequence number.

- Write window

  The write window is the period of time 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.

  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. 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.

  > **See Also:** Chapter 9, "Vaulting" for more information on 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 already been created in this family.

> **See Also:**
>
> - "Configuring Media Families" on page 3-1 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 new 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 new 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 new 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.

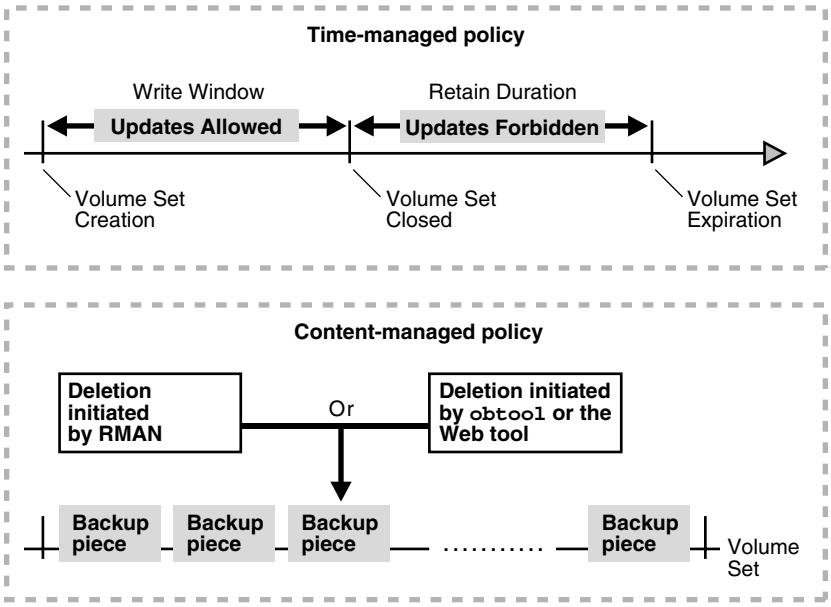
  You can also use the `--vid` option on the `restore` command to ensure that the volume being read is the correct one.

  > **See Also:** *Oracle Secure Backup Reference* for complete syntax and semantics for the `mkmf` and `restore` commands

Volume 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 1–8, volumes in a media family use either a **content-managed expiration policy** or **time-managed expiration policy**.

Figure 1–8 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. A content-managed volume expires when each **backup piece** on the volume have been marked as deleted. A volume in a content-managed **volume set** can expire even though the other volumes in the set are not yet expired.

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 1–8, you can delete backup pieces through the RMAN or Oracle Secure Backup interfaces. Deleting backup pieces by means of 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 Database Backup and Recovery User's Guide* to learn about deleting or crosschecking backups
- *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 1–8, Oracle Secure Backup computes the volume expiration time by adding the following:

- The **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.

- The **write window** period

  This is the user-specified period of time during which volumes in a media family can be written to. All volumes in a volume set share the same write window.

- The **retention period**

  This is the user-specified period of time 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, suppose you set the write window for a media family to 7 days and the retention period to 14 days. This means that the data on all volumes in the volume set is retained for 14 days from the close of the write window. Suppose further 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 example, 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.

Caution: 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.

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.

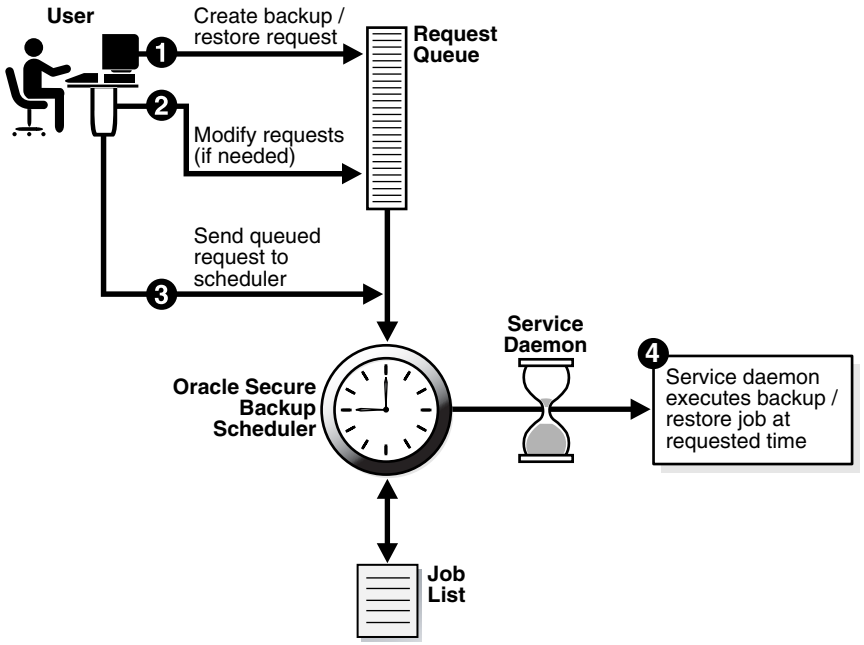
The **scheduler** policies, which are described in "Defaults and Policies" on page 1-6, determine how the scheduler handles backup and restore jobs. You should familiarize yourself with these settings because they determine the frequency with which the scheduler dispatches jobs.

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" on page 4-7.

Figure 1–9 shows the process by which an **Oracle Secure Backup user** can create an **on-demand backup** or restore job.

See Also: "On-Demand Backups" on page 5-4

Figure 1–9 Backup and Restore Requests and Jobs



The steps in the process illustrated in Figure 1–9 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.

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 new 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" on page 5-21
  - *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 numerical job identifier such as `15`.

- Each time you create an **on-demand backup** request and then click **Go** or use the **obtool** `backup --go` command to send your request to the scheduler, Oracle Secure Backup creates a dataset job. It assigns the job an identifier prefixed by the name of the **Oracle Secure Backup 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 obtool `restore --go` command to send your request to the **scheduler**, Oracle Secure Backup creates a restore job for each **backup image** 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 foremost decision criterion that the scheduler uses to run a job is the user-assigned schedule priority. The scheduler dispatches higher priority jobs over lower priority ones, providing all resources required to run the job are available. For example, if twenty jobs are in the scheduler and ready for processing, then Oracle Secure Backup runs the job with the lowest numeric schedule priority.

See Also: "Performing On-Demand File System Backups" on page 5-28 and "Configuring Backup Schedules" on page 5-17

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" on page 8-3

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" on page 8-4

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" on page 3-10

2

Managing Users and Classes

This chapter describes Oracle Secure Backup users and classes and explains how to configure them in your **administrative domain**.

This chapter contains these sections:

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

Understanding 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.

Oracle Secure Backup Users and Passwords

Oracle Secure Backup stores information pertaining to each 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 **Secure Sockets Layer (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.

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. One of these accounts can be used 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 on 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.

NDMP Hosts

When setting up an **Oracle Secure Backup user** account, you can configure user access to a **Network Data Management Protocol (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.

It is recommended that you follow these steps:

To set up and manage Oracle Secure Backup users in your **administrative domain**:

1. Add new Oracle Secure Backup users if necessary.
2. Change the `admin` password if necessary.

   You set the original password when you installed Oracle Secure Backup on the administrative server. This task is described in "Changing a User Password" on page 2-11.
3. Review the attributes of each **Oracle Secure Backup user**r.

   This task is described in "Editing or Displaying User Properties" on page 2-10.
4. Configure **preauthorization** and account settings for unprivileged backups if necessary.

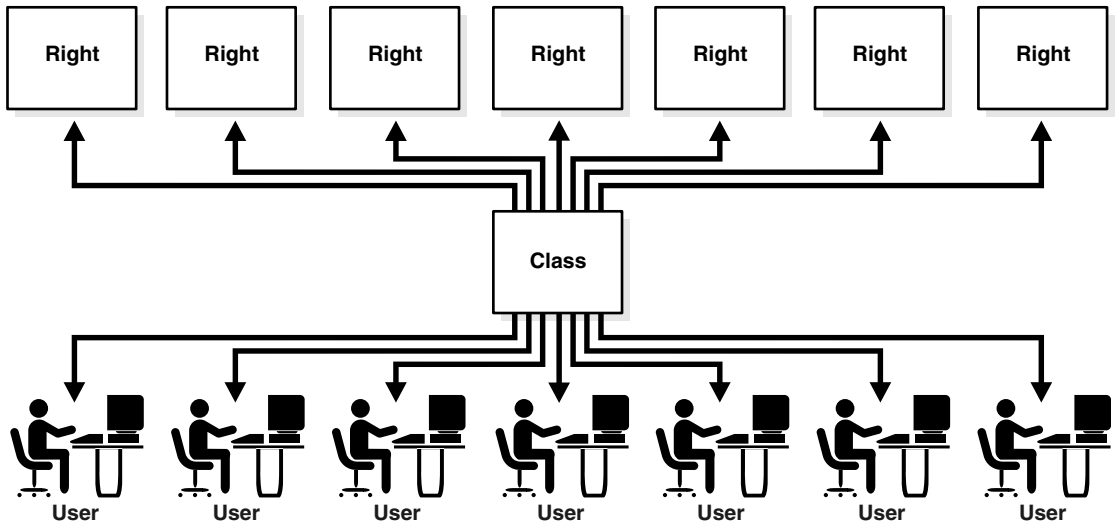
   This task is described in "Assigning Windows Account Information" on page 2-11, and "Assigning Preauthorized Access" on page 2-12.

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 as well as 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.

See Also:

- "Configuring Classes" on page 2-14 for a detailed description of the rights available to each class
- *Oracle Secure Backup Reference* to learn about the **obtool** `user` and `class` commands

Configuring Defaults and Policies

Defaults and policies are configuration settings that 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. The policy defaults are sufficient in most cases to protect your data and secure your network. But if you have special requirements, environments, or backup strategies, then you should review the defaults and make changes where necessary.

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

The classes of policies that you might want to review or change are:

- Media

  This policy class controls 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**.

- NDMP

  This policy class controls settings applicable to hosts that use **NDMP access mode**. For example, you can configure backup environment variables or specify a user name for authentication.

- Operations

  This policy class controls aspects of 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

  This policy class controls the behavior of the Oracle Secure Backup scheduler. For example, you can specify the frequency at which the scheduler attempts to dispatch backup jobs.

- Security

  This policy class controls aspects of administrative domain security. For example, you can enable **Secure Sockets Layer (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.

- Vaulting

  This policy class controls media management. It includes the `autovolumerelease` policy, the customer ID for each third-party **storage**

location, minimum writeable volumes, and report retain time. See Chapter 9, "Vaulting" for more information on these policies.

This section contains these topics:

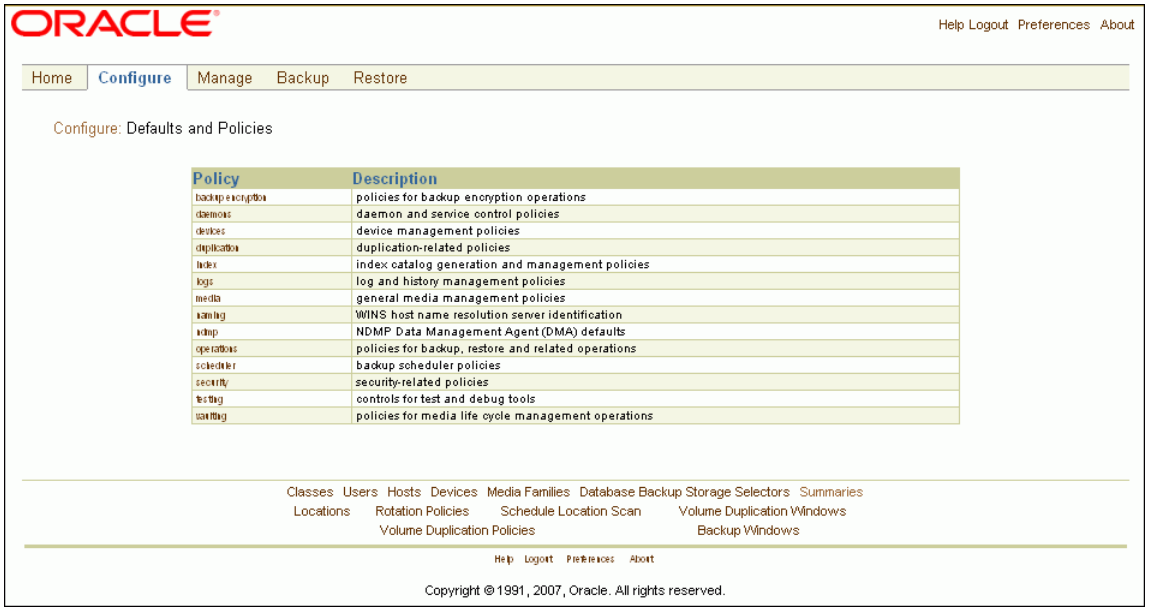
- Viewing Configured Defaults and Policies Values
- Setting a Policy
- Resetting a Policy

See Also: "Defaults and Policies" on page 1-6

Viewing Configured Defaults and Policies Values

In the Advanced section of the Configure page, click **Defaults and Policies** to display the page shown in Figure 2–2. This page lists the policy classes.

Figure 2–2 Defaults and Policies Page



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

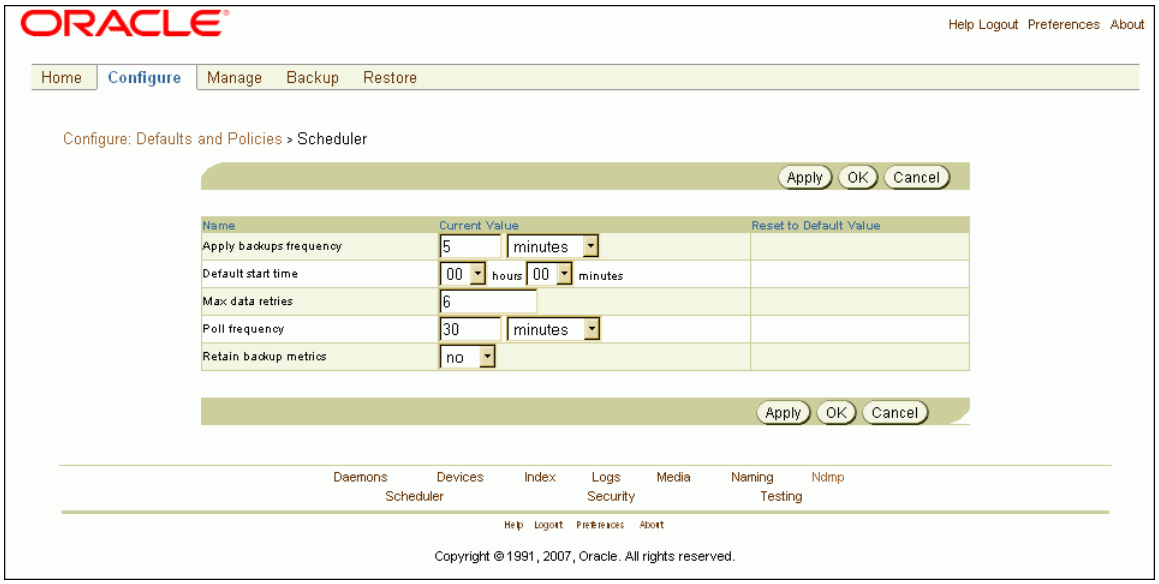
Before changing a policy setting, refer to the "Defaults and Policies" appendix in *Oracle Secure Backup Reference*. This appendix contains extensive descriptions of the policies and describes valid settings. You should not ordinarily be required to change the default settings.

To change a policy setting:

1. 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 2–3 shows the Scheduler page before any changes are made.

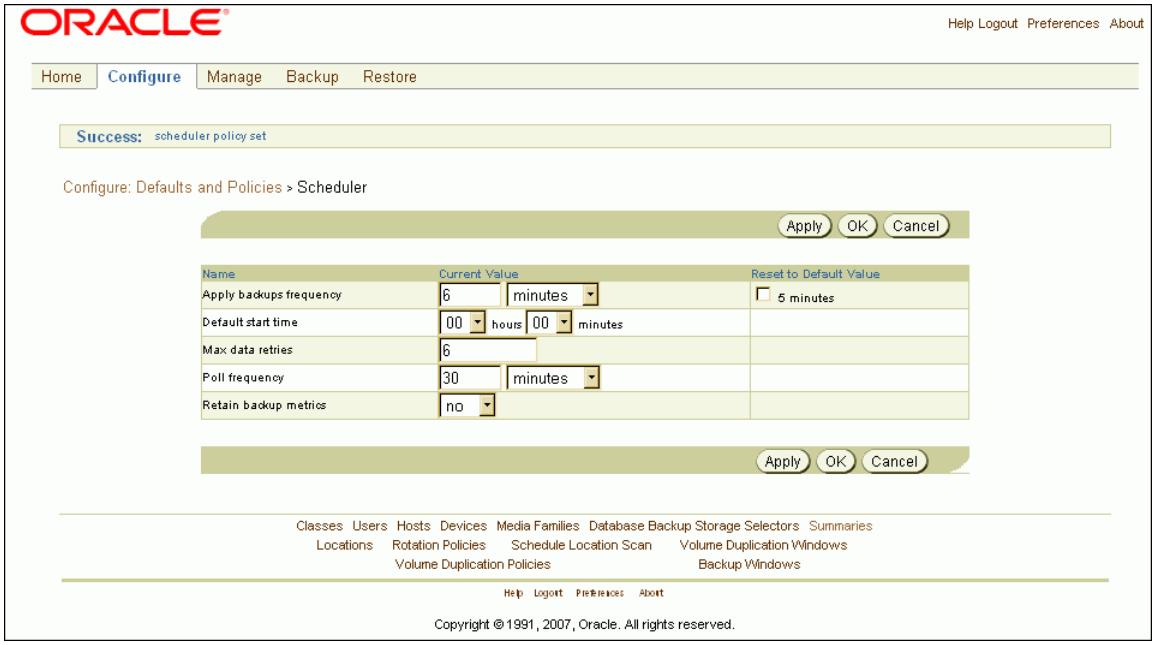
Figure 2–3 Unmodified Scheduler Page



2. Change the settings of one or more policies.
3. Do one of the following:
   - 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 Oracle Secure Backup **Web tool** displays the default value for the policy in the Reset to Default Value column. Figure 2–4 shows the Scheduler page after the backup frequency has been changed to 6 minutes from the default of 5 minutes.

Figure 2–4 Modified Scheduler Page



Resetting a Policy

You can reset the value of a one or more policies to the default value.

To reset a policy:

1. In the Policy column on the Defaults and Policies page, click the name of the policy class that contains the policy to be reset.
2. Select the **Reset to Default Value** column for the policy that you are resetting.
3. Click **Apply** or **OK**.

Configuring 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 Oracle Secure Backup **Web tool**.

This section contains these topics:

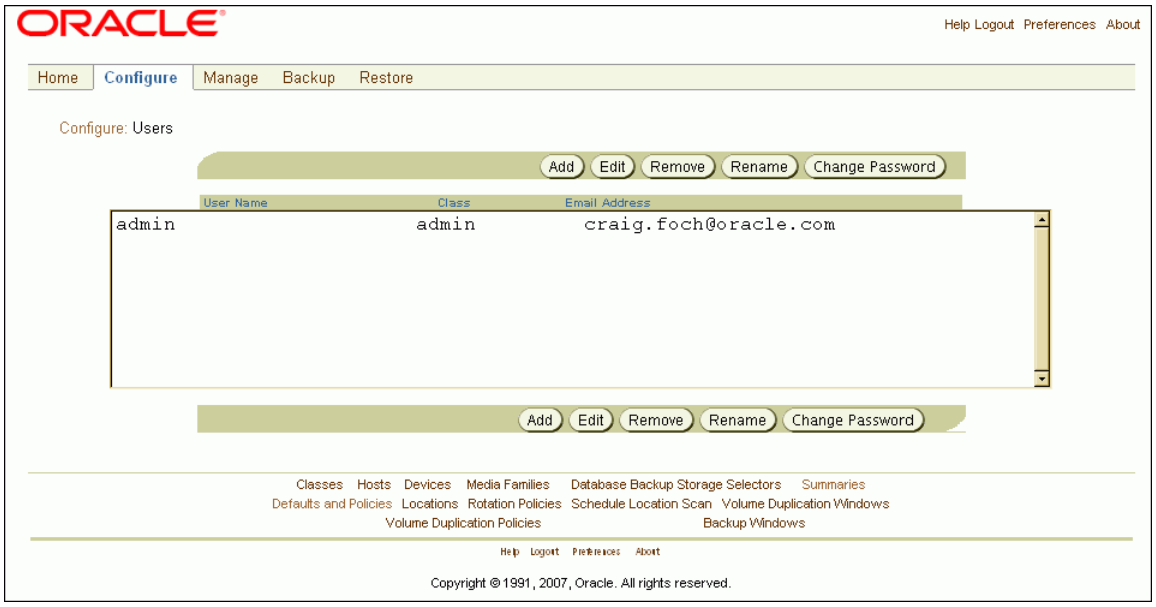
- Displaying the Users Page
- Adding a User
- Editing or Displaying User Properties
- Changing a User Password
- Assigning Windows Account Information
- Assigning Preauthorized Access
- Renaming a User
- Removing a User

See Also: "Oracle Secure Backup Users and Passwords" on page 2-1

Displaying the Users Page

In the Configure page, click **Users** to display the Users page, which is shown in Figure 2–5. This page lists all users authorized by Oracle Secure Backup along with their **class** names and email addresses. You can perform all **Oracle Secure Backup user** configuration tasks in this page or in pages to which it provides links.

Figure 2–5 Users Page



See Also: *Oracle Secure Backup Reference* to learn about the user commands in **obtool**

Adding a User

To add one or more users:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

   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: "Oracle Secure Backup Classes and Rights" on page 2-3

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, such as to deliver a **job summary** or notify the user of a pending input request, it sends email to this address.

11. Click **Apply**, **OK**, or **Cancel**.

12. If the Oracle Secure Backup user you configured must initiate backup and restore operations on Windows clients, then see "Assigning Windows Account Information" on page 2-11.

Editing or Displaying User Properties

This section explains how to modify properties for an existing **Oracle Secure Backup user** account.

Note: To modify Oracle Secure Backup users, you must be a member of a **class** that has this right enabled. See "Oracle Secure Backup Classes and Rights" on page 2-3 for details.

To edit Oracle Secure Backup user properties:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

   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. Make whatever changes you want.

   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" on page 2-13.

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" on page 2-11.

Changing a User Password

This section explains how to modify the password for an existing **Oracle Secure Backup user** account.

> **Note:** To modify Oracle Secure Backup users, you must be a member of a **class** that has this right enabled. See "Oracle Secure Backup Classes and Rights" on page 2-3 for details.

To change an Oracle Secure Backup user password:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

   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 new password.
5. Confirm the new 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.

Assigning Windows Account Information

This section explains how to configure Windows account information for an **Oracle Secure Backup 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 procedure in "Displaying the Users Page" on page 2-8.

   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

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 on the `modify administrative domain's configuration` right

To assign preauthorized access:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

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 Secure Backup user** 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" on page 4-10 for more details about RMAN **preauthorization**

Removing Preauthorized Access

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

To rename an **Oracle Secure Backup user**:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

   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 new page appears.

4. Enter the new 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 new name in the **User Name** list

Removing a User

To remove an **Oracle Secure Backup user**:

1. Follow the procedure in "Displaying the Users Page" on page 2-8.

   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.

Configuring Classes

A **class** defines a set of **rights** that are granted to an **Oracle Secure Backup 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:

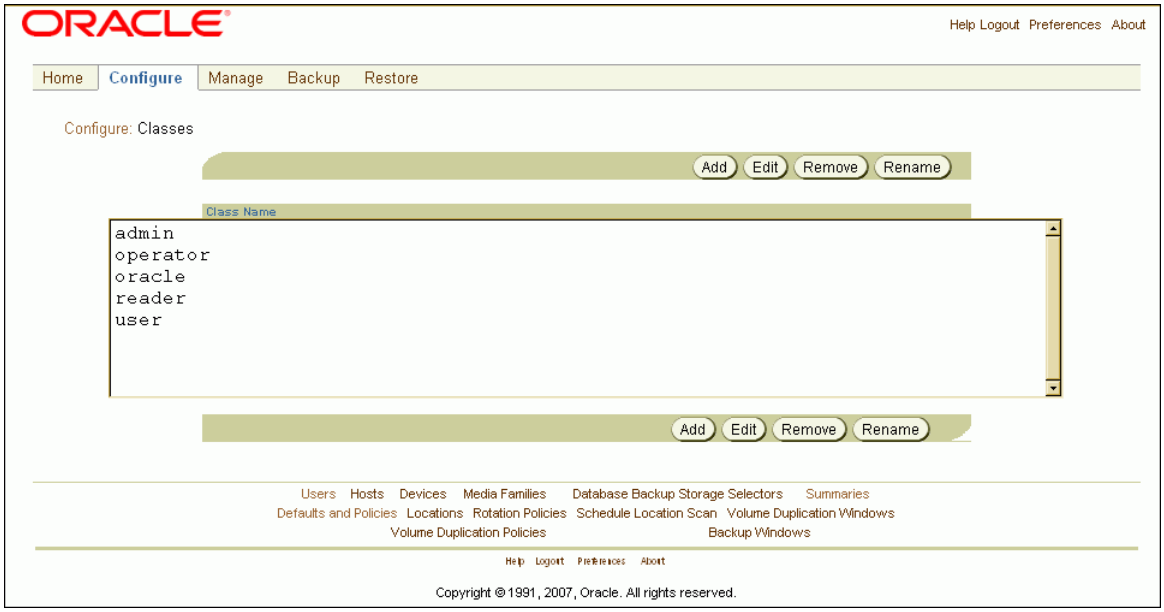
- Displaying the Classes Page
- Adding a Class
- Editing or Displaying Class Properties
- Removing a Class
- Renaming a Class

See Also: "Oracle Secure Backup Classes and Rights" on page 2-3

Displaying the Classes Page

In the Advanced section of the Configure page, click **Classes** to display the Configure: Classes page, as shown in Figure 2–6. You can use this page to manage existing classes or configure new classes.

Figure 2–6 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 procedure in "Displaying the Classes Page" on page 2-14

   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 new 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, the changes do not take effect until the Oracle Secure Backup user exits from the Oracle Secure Backup component currently in use.

> **See Also:** *Oracle Secure Backup Reference* for more information on the `modify administrative domain's configuration` right

To edit a class:

1. Follow the procedure in "Displaying the Classes Page" on page 2-14

   The Configure: Classes page appears.
2. Select the name of the class that you want 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 whatever changes you want.

   You cannot rename a class from this page. To rename a class, see "Renaming a Class" on page 2-16.
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 an **Oracle Secure Backup 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 procedure in "Displaying the Classes Page" on page 2-14

   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

To rename a **class**:

1. Follow the procedure in "Displaying the Classes Page" on page 2-14

The Configure: Classes page appears.

2. Select the class that you want to rename in the **Class Name** list.
3. Click **Rename**.

   A new page appears.
4. Enter the new 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 new name in the Class Name list.

3

Configuring Backup and Media Settings

This chapter explains how to configure backup and media settings for an **administrative domain**.

This chapter contains these sections:

- Configuring Media Families
- Configuring Database Backup Storage Selectors
- Configuring Job Summary Schedules

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), the **retention period**, and the **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" on page 3-5

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: "Media Families" on page 1-14

Displaying Defined Media Families

To display every defined **media family** with Oracle Enterprise Manager Database Control 11*g* (Oracle Database Control 11*g*):

1. From the Oracle Database Control 11*g* home page, click **Availability**.

   The Availability subpage appears.

2. In the Oracle Secure Backup section, click **Oracle Secure Backup Device and Media**.

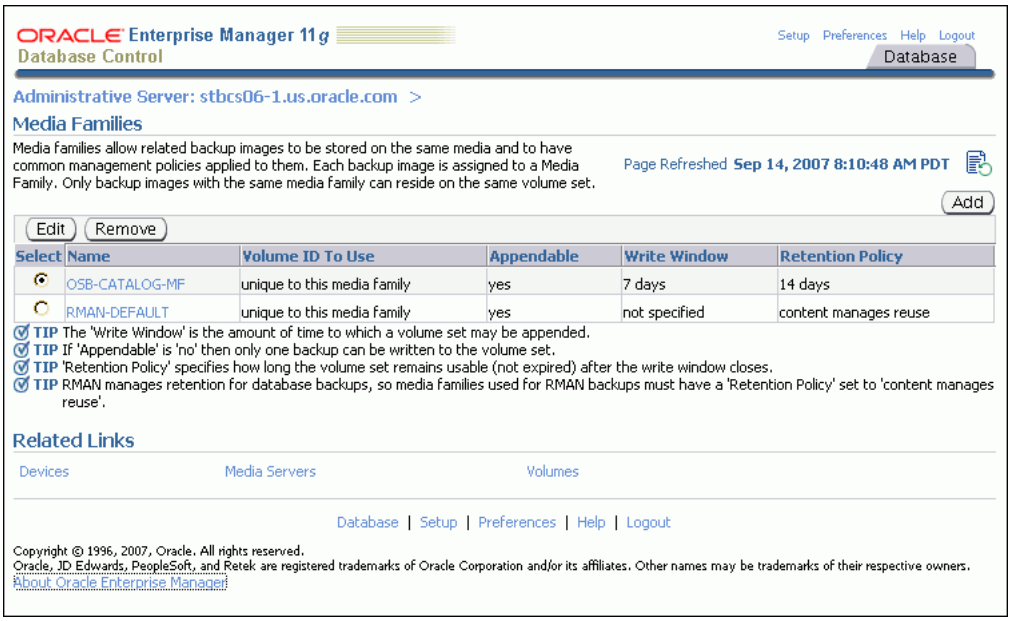
   The Oracle Secure Backup Device and Media: Administrative Server page appears.

3. In the Resources section, click the number to the right of **Media Families**.

   The Media Families page appears.

4. The Media Families page displays a table listing all currently defined media families. For each media family, the table shows:

   - The media family name
   - The **volume ID** to use with this media family
   - Are volumes in this media family appendable?
   - The **write window**
   - The **retention period**



Each entry in the table also has a select option, and the page has Edit, Remove, and Add options. 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

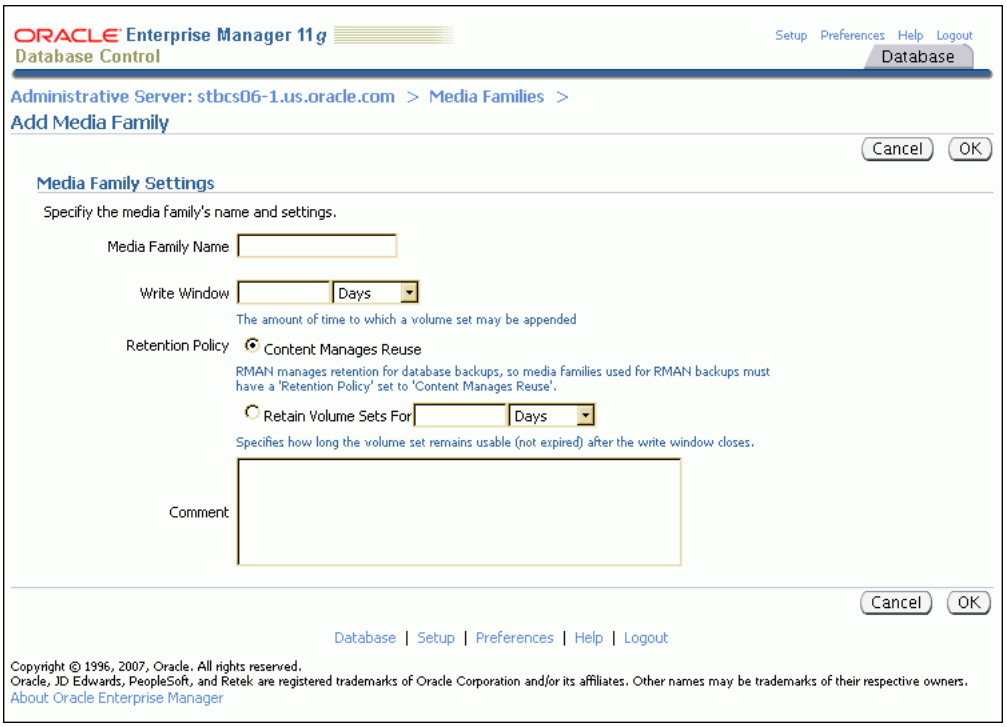
To add a **media family** with Oracle Database Control 11*g*:

1. Follow the steps in "Displaying Defined Media Families" on page 3-2.

   The Oracle Database Control 11*g* Media Families page appears.

2. Click **Add**.

   The Add Media Family page appears.



3. Enter a name for your new media family in the **Media Family Name** field. 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. Enter a value for the media family **write window** in the **Write Window** field. 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 of time 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 the first file is written to the first volume in the set and closes after the specified period of time elapses. When the write window closes, Oracle Secure Backup disallows further updates to the volume set until one of the following conditions is met:

   - It expires.
   - It is relabeled.
   - It is reused.
   - It is unlabeled.
   - It is forcibly overwritten.

   Oracle Secure Backup continues using the volume set for the next backup operation until the write window closes.
5. Select one of the following retention policies:

   - **Content Manages Reuse**

     Volumes that use this retention policy are intended for RMAN backups: you cannot write a **file system backup** to a content-managed volume.

A content-managed volume is eligible to be overwritten when all backup image sections have been marked as deleted. You can delete a **backup piece** through **Recovery Manager (RMAN)** or through the `rmpiece` command in **obtool**. A volume in a content-managed volume set can expire even though other volumes in the same set are not expired.

- **Retain Volume Sets For**

  By specifying this option, you indicate that this media family is time-managed rather than 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** 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.

  Caution: 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.

  ---

6. Enter a description of the media family (optional) and click **OK**.
7. The Media Families page appears with a success message and an entry for your new media family.

Editing or Displaying Media Family Attributes

You can 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 with Oracle Database Control 11*g*:

1. Follow the steps in "Displaying Defined Media Families" on page 3-2.

   The Oracle Database Control 11*g* Media Families page appears.

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

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

3. Make whatever changes you want and click **OK**.

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

Note: You cannot change the name of a media family in Oracle Enterprise Manager Database Control. Use the Oracle Secure Backup **Web tool** or **obtool** `renmf` command instead. See *Oracle Secure Backup Reference* for complete syntax and semantics for the `renmf` command.

Removing a Media Family

To remove a **media family** with Oracle Database Control 11*g*:

1. Follow the steps in "Displaying Defined Media Families" on page 3-2.

   The Oracle Database Control 11*g* 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 Oracle Enterprise Manager Database Control to create a **database backup storage selector**. Database Control gives the selector a system-defined name. If you want to specify the name for the database backup storage selector, then use the `mkssel` command in **obtool**.

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

To display defined database storage selectors with Oracle Database Control 11*g*:

1. From the Oracle Database Control 11*g* home page, click **Availability**.

   The Availability subpage appears.

2. In the Backup/Recovery section, click **Backup Settings**.

   The Backup Settings page appears.

Adding a Database Backup Storage Selector

To configure a **database backup storage selector** with Oracle Database Control 11*g*:

1. Perform the steps in "Displaying Defined Database Backup Storage Selectors" on page 3-6.

   The Backup Settings page appears.

2. In the Oracle Secure Backup section, click **Configure**.

   The Administrative Server Login page appears.

3. Select an Oracle Secure Backup **administrative server** from the **Administrative Server** list.

   Enter the name of an **Oracle Secure Backup user** with administrative privileges on the selected host in the **Username** field.

   Enter the password for this Oracle Secure Backup user in the **Password** field.

   Select Save As Preferred Credential if you want Oracle Database Control 11*g* to remember this user name and password.

   Click **OK**.

   The Backup Storage Selectors page appears.

4. Click **Add**.

   The Add Backup Storage Selector page appears.

5. Under Database Backup Types, select one of the following:

   - **Archive Logs**
   - **Auto Backup**
   - **Full**
   - **Incremental**

6. Select a copy number from the **Copy Number** list.

   If you leave the Copy Number list at the default (`*`), then this storage selector applies to all backups.

7. Select a **media family** from the **Media Family** list.

8. Enter a value in the **Resource Wait Time** field 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.

9. In the Use Devices section, you can specify which **tape device** to use for this backup. If you do not specify any tape devices, then Oracle Secure Backup uses any available tape device in the **administrative domain**.

   To specify a tape device, click **Add**.

   The Use Devices page appears.

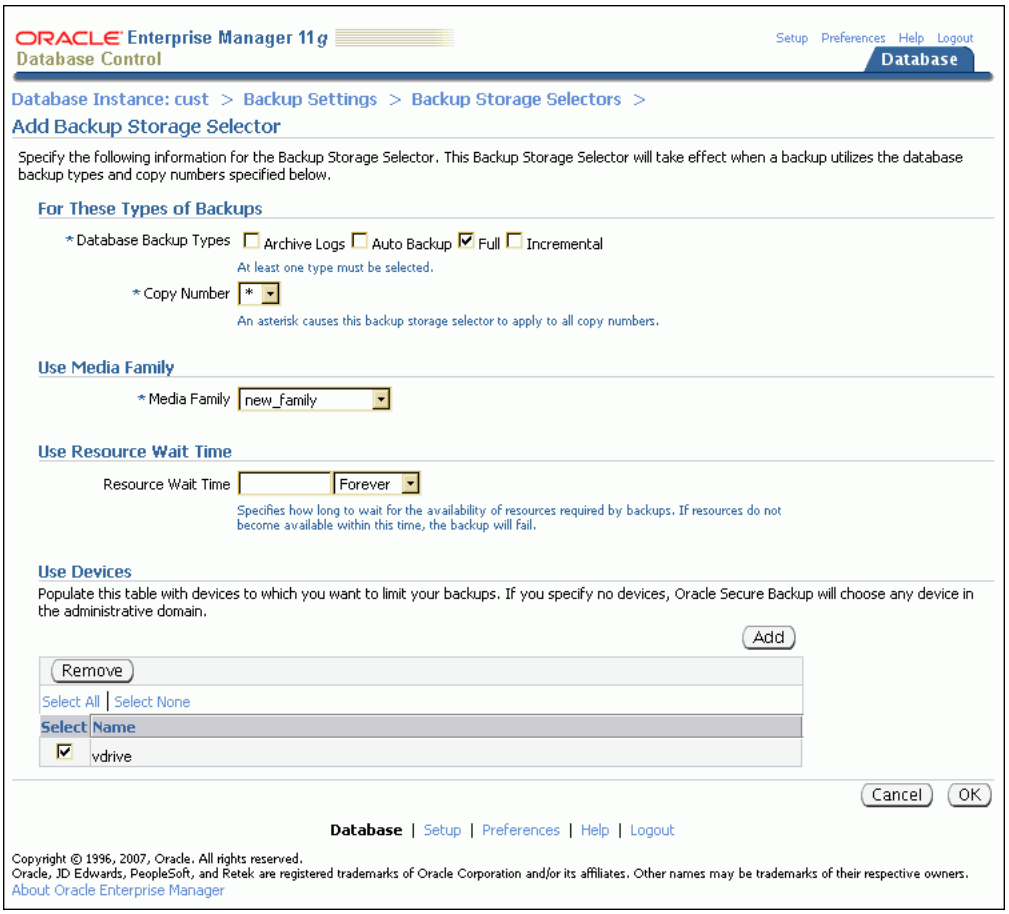
10. If you want to filter the list of tape devices, then enter a tape device name in the **Device Name** field and click **Go**.

    In the Search Results table, select a **tape drive** to add and click **Select**.

    The Add Database Selector page appears with the selected tape drive in the Use Device table.

11. Select the tape drive or drives to use and click **OK**.

The Backup Storage Selectors page appears with a success message, and your new database backup storage selector appears in the table.



Editing a Database Backup Storage Selector

To edit parameters for an existing **database backup storage selector** with Oracle Database Control 11*g*:

1. Perform the steps in "Displaying Defined Database Backup Storage Selectors" on page 3-6.

   The Backup Settings page appears.

2. In the Oracle Secure Backup section, click **Configure**.

   The Administrative Server Login page appears.

3. Select an Oracle Secure Backup **administrative server** from the **Administrative Server** list.

   Enter the name of an **Oracle Secure Backup user** with administrative privileges on the selected host in the **Username** field.

   Enter the password for this Oracle Secure Backup user in the **Password** field.

   Select Save As Preferred Credential if you want Oracle Database Control 11*g* to remember this user name and password.

   Click **OK**.

   The Backup Storage Selectors page appears.

4. The Backup Storage Selectors page lists all currently configured backup storage selectors. It displays the following information for each storage selector:

   - Database Backup Types
   - Copy Number
   - Media Family
   - Resource Wait Time
   - Devices
   - Backup Storage Selector Name

   Select the backup storage selector that you want to edit and click **Edit**.

   The Edit Backup Storage Selector page appears.

5. Make whatever changes you want to the selected backup storage selector and click **OK**.

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

> **Note:** You cannot change the name of the database backup storage selector in Oracle Enterprise Manager Database Control. Use the Oracle Secure Backup **Web tool** or **obtool** `renssel` command instead. See *Oracle Secure Backup Reference* for complete syntax and semantics for the `renssel` command.

Removing a Database Backup Storage Selector

To remove a **database backup storage selector** with Oracle Database Control 11*g*:

1. Perform the steps in "Displaying Defined Database Backup Storage Selectors" on page 3-6.

   The Backup Settings page appears.

2. In the Oracle Secure Backup section, click **Configure**.

   The Administrative Server Login page appears.

3. Select an Oracle Secure Backup **administrative server** from the **Administrative Server** list.

   Enter the name of an **Oracle Secure Backup user** with administrative privileges on the selected host in the **Username** field.

   Enter the password for this Oracle Secure Backup user in the **Password** field.

   Select Save As Preferred Credential if you want Oracle Database Control 11*g* to remember this user name and password.

   Click **OK**.

   The Backup Storage Selectors page appears.

4. Select the backup storage selector that you want to remove and click **Remove**.

   A confirmation page appears.

5. 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** and restore jobs. You can configure a **job summary schedule** that indicates when the reports should be generated and who should receive them.

Oracle recommends 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: "Job Summaries" on page 1-21

Displaying the Defined Job Summaries Page

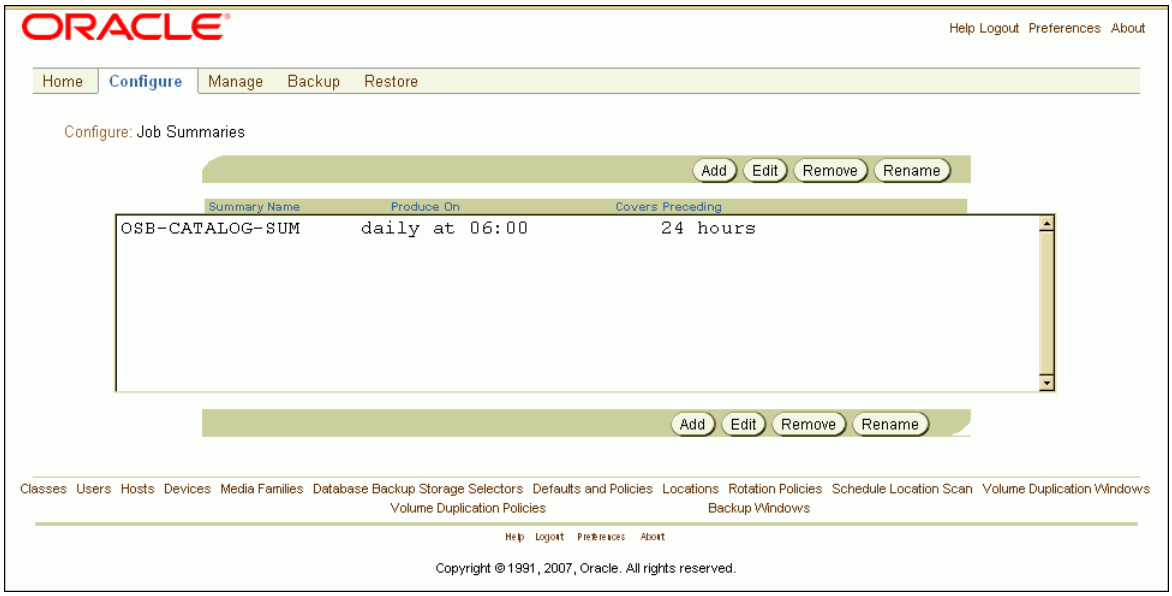
To display the list of currently defined job summaries with the Oracle Secure Backup **Web tool**:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure subpage appears.

2. In the Advanced section, click **Job Summaries**.

   The Configure: Job Summaries page appears.



3. 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

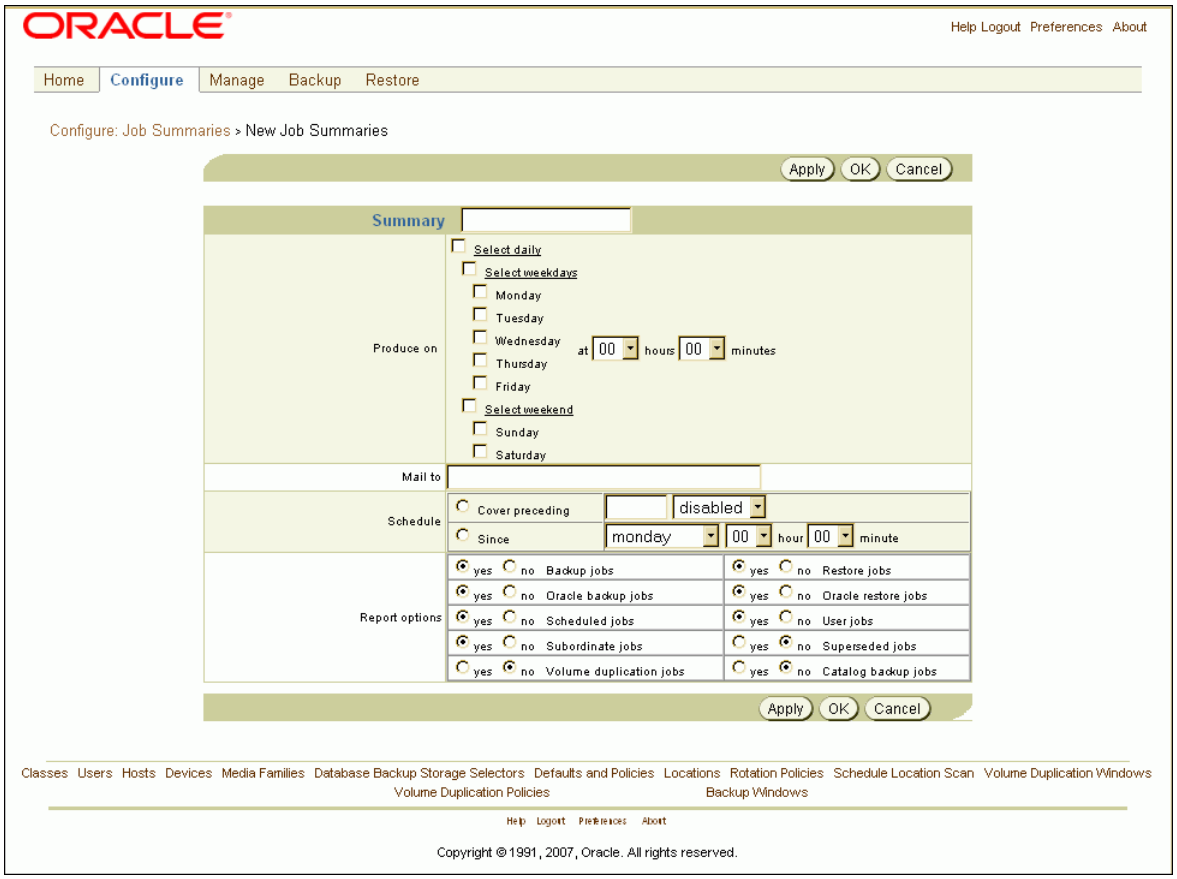
To create a **job summary schedule** schedule with the Oracle Secure Backup **Web tool**:

1. Perform the steps in "Displaying the Defined Job Summaries Page" on page 3-10.

   The Configure: Job Summaries page appears.

2. Click **Add**.

   The Configure: Job Summaries > New Job Summaries page appears.



3. Enter a name for the new **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 the following 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 the following 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 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 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 make it easier to 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 new job summary appears in the list.

Editing a Job Summary Schedule

To edit a **job summary schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the steps in "Displaying the Defined Job Summaries Page" on page 3-10.

   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 new values appear in the table.

Removing a Job Summary Schedule

To remove a **job summary schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the steps in "Displaying the Defined Job Summaries Page" on page 3-10.

   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

To rename a **job summary schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the steps in "Displaying the Defined Job Summaries Page" on page 3-10.

   The Configure: Job Summaries page appears.

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

3. Enter a new 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 new 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:

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:

> **See Also:** *Oracle Database Backup and Recovery User's Guide* for more information on RMAN

About Recovery Manager and Oracle Secure Backup

Oracle Secure Backup serves as a media management layer for **Recovery Manager (RMAN)** through the **SBT interface**. Oracle Secure Backup and third-party backup utilities integrate with RMAN through the SBT interface API.

You can use Oracle Secure Backup with the following product releases:

- Oracle9*i* Database
- Oracle Database 10*g*
- Oracle Database 11*g*
- Oracle Enterprise Manager 10*g* (10.2)
- Oracle Enterprise Manager 11*g* (11.1)

While Oracle Secure Backup supports previous database versions, key functionality has been added beginning with Oracle Database 10*g* 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 10*g* release 2 (10.2)

  - Oracle Enterprise Manager provides a unified interface for RMAN and Oracle Secure Backup. In addition, managing tapes, media servers, and tape devices 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 will 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 will enable the unused-block optimization. If the backup is directly to tape using a third-party media management product, then this will not have any effect because unused-block optimization directly to tape is available only with Oracle Secure Backup.

- Oracle Database 11*g* release 1 (11.1)
  - 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

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 on RMAN

Database Backups

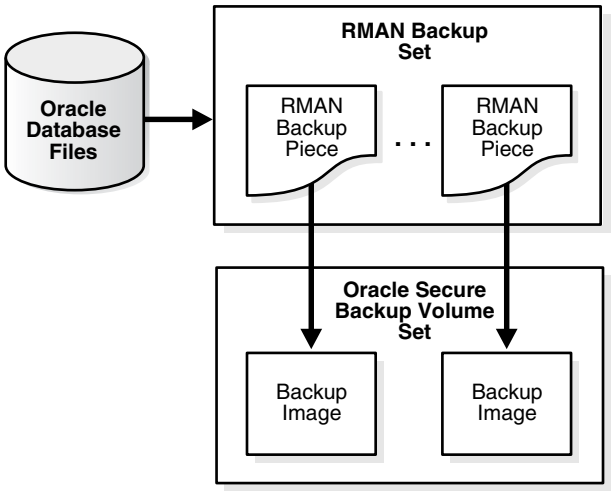
Oracle Secure Backup supplies an **SBT interface** that RMAN can use to back up database files to tape. Within the Oracle Secure Backup **administrative domain**, an SBT backup is initiated through the RMAN command line or Oracle Enterprise Manager, while a **file system backup** is initiated through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

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 on 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**. Figure 4–1 illustrates the relationship between pieces and images. A single backup image can span multiple tapes. Oracle Secure Backup can write database backup images (RMAN backup pieces) and **file system backup** images on the same **volume**.

Figure 4–1 Backup Sets and Backup Images



See Also: "Volume Sets" on page 1-12

Database Backup Storage Selectors

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

Oracle recommends that you define one or more database backup storage selectors to automate the tape 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.

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

A database backup storage selector can also specify the following:

- The content or type of the backup, for example, whether it is a **full backup** or an **incremental backup**
- The copy number of duplexed backups
- Restrictions on which **tape device** can be used for the backup

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, 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.

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.

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/ssel subdirectory of the **Oracle Secure Backup home** on the **administrative server**.

See Also:

- "Creating a Database Backup Storage Selector in Enterprise Manager" on page 4-13
- "Setting Media Management Parameters in RMAN" on page 4-13 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 in **obtool**

Database Restore and Recovery

A restore operation that you initiate through RMAN is called an Oracle Database restore operation.

See Also:

- "Database Backup Storage Selectors" on page 4-3
- "Performing Recovery with RMAN and Oracle Secure Backup" on page 4-20

Interfaces for Managing Database Backup and Recovery

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

- RMAN Command-Line Client
- Oracle Enterprise Manager 10g and 11g Database Control
- Oracle Enterprise Manager 10g Grid 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 **RMAN target database** host must be a member of the Oracle Secure Backup administrative domain. The target database uses the Oracle Secure Backup **SBT interface** on the target host to communicate with the Oracle Secure Backup administrative domain.

Oracle Enterprise Manager 10*g* and 11*g* Database Control

You can manage single-instance database operations, including backup and recovery, through the Oracle Enterprise Manager Database Control. The Database Control console, **RMAN target database**, and Oracle Secure Backup **administrative server** must all be on the same host.

Oracle Enterprise Manager 10*g* Grid Control

You can manage multiple databases with Oracle Enterprise Manager Grid Control. The Grid Control console can run on any database host in the administrative domain. Unlike Oracle Enterprise Manager Database Control, Grid Control is not required to run on the **administrative server** of the Oracle Secure Backup **administrative domain**.

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

When you use Grid Control version 10.2.0.2, you can use Oracle Secure Backup on a host that runs an Oracle Database 10*g* release 1 (10.1) or earlier database, as long as the repository for Enterprise Manager is in an Oracle Database 10*g* release 2 (10.2) database.

RMAN and the Oracle Secure Backup Administrative Domain

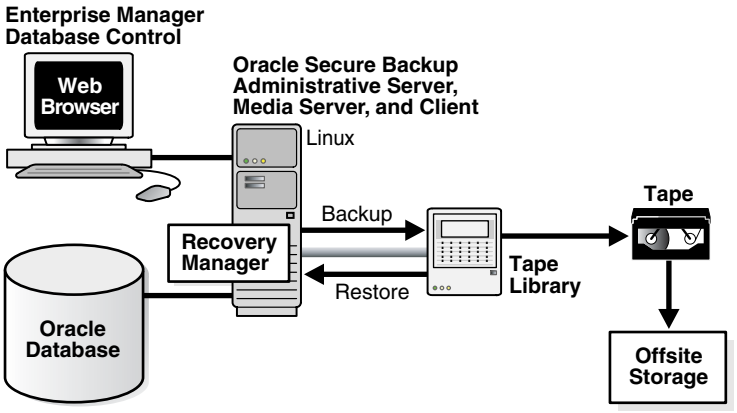
This section describes RMAN operations in the following situations:

- 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



Because the database is installed on the administrative server, you can use Enterprise Manager Database Control console to perform database backup and restore operations involving Oracle Secure Backup.

> **Note:** This chapter is written from the perspective of the administrator of a single-host **domain** that is configured like the one in Figure 4–2.

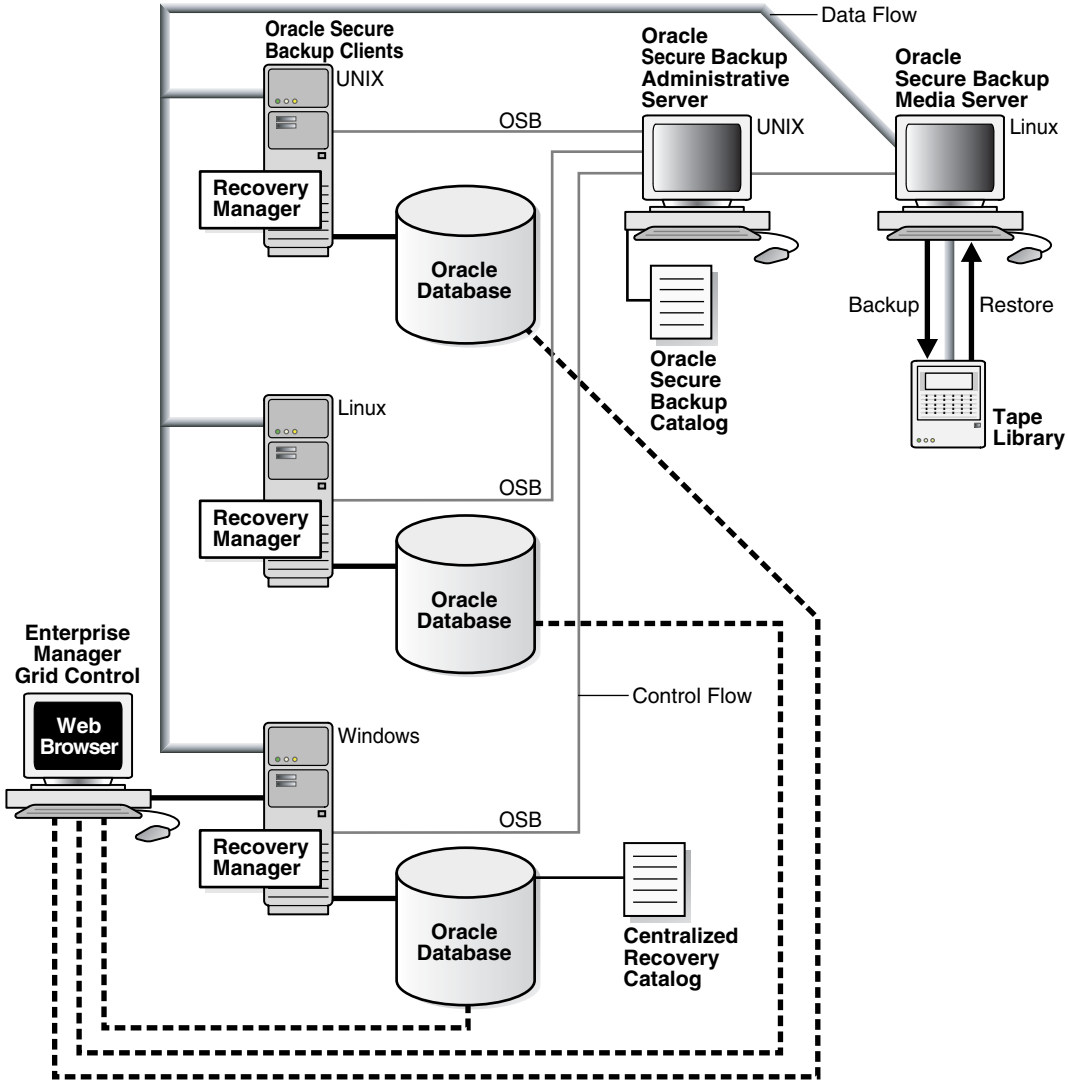
Multiple-Host Administrative Domain with Database Backups

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 **RMAN recovery catalog** to store metadata for backups of all databases in the administrative domain.

Figure 4–3 Multiple-Host Administrative Domain

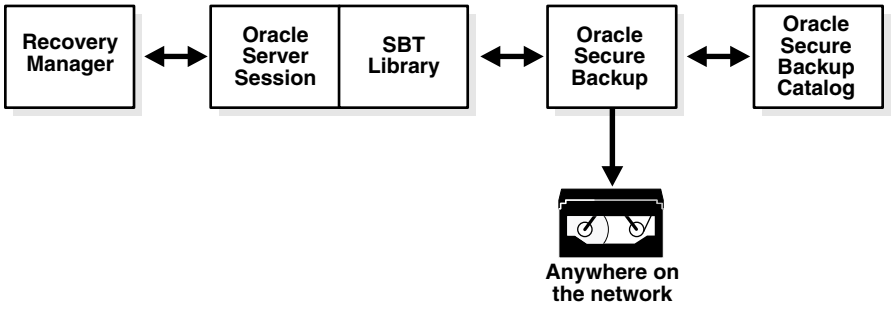


Because the target databases do not reside on the administrative server, you cannot use Oracle Enterprise Manager Database Control to back them up through the Oracle Secure Backup **SBT interface**. You can use Grid Control on one of the clients, however, to initiate SBT operations involving all databases 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 interface**.

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 a `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.

   You can control how long a job waits in the queue through:

   - 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 **obtool** `mkssel` or `chssel` command
   - RMAN parameter `OB_RESOURCE_WAIT_TIME`

     See Also:

     - *Oracle Secure Backup Reference* for more information on the `mkssel` and `chssel` commands
     - "Setting Media Management Parameters in RMAN" on page 4-13
6. For RMAN restore operations, the start time depends on the setting of the `rmanrestorestartdelay` policy in the operations policy class.
7. RMAN creates or restores the backup pieces.

8. 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.

   See Also: *Oracle Secure Backup Reference* to learn about **defaults and policies**

Configuring Oracle Secure Backup for Use with RMAN

To configure Oracle Secure Backup for use with **Recovery Manager (RMAN)**, perform the following steps in Oracle Secure Backup:

1. Configure RMAN access to the Oracle Secure Backup **SBT interface**. If you are using Enterprise Manager Database Control, then this step involves registering the **administrative server** with Enterprise Manager.

   See Also: "Configuring RMAN Access to the Oracle Secure Backup SBT Library" on page 4-10

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

   Note: This is a required step. An RMAN backup operation will fail without it.

   See Also: "Creating a Preauthorized Oracle Secure Backup User" on page 4-10

3. Oracle recommends 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" on page 4-12

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" on page 4-13
   - "Setting Media Management Parameters in RMAN" on page 4-13

You can perform the preceding tasks in any Oracle Secure Backup interface. Where possible, this section explains how to perform these tasks through the Enterprise Manager Database Control console.

See Also: "Interfaces for Managing Database Backup and Recovery" on page 4-5

Configuring RMAN Access to the Oracle Secure Backup SBT Library

You can use Enterprise Manager Database 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 Oracle 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. First, 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. Second, 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 on 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.

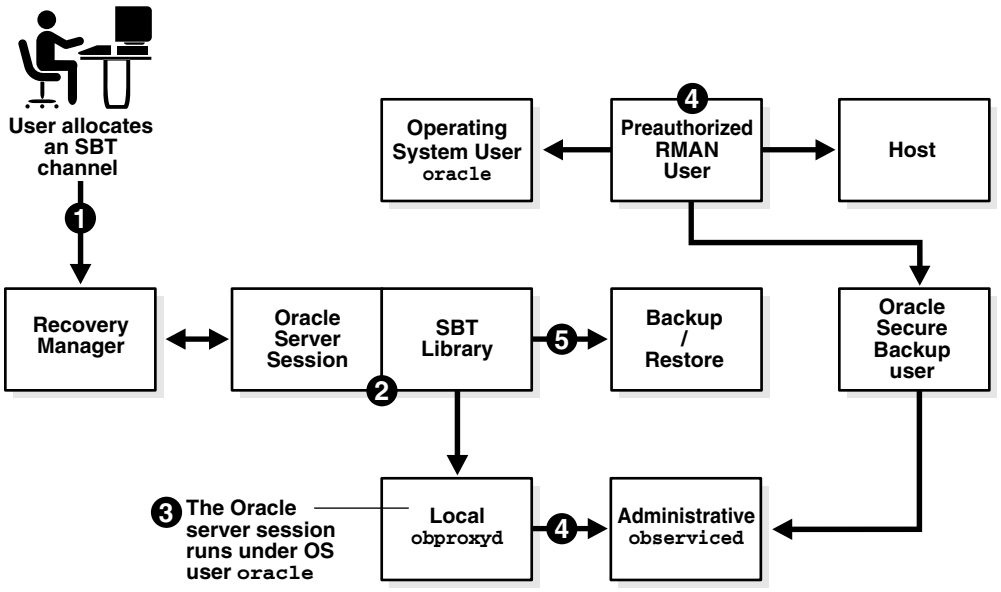
You can also preauthorize an Oracle Secure Backup user for command-line (obtool) operations. This is useful if you use backup and restore scripts.

> **See Also:** "Assigning Preauthorized Access" on page 2-12

How Oracle Secure Backup Preauthorizes SBT Backups

Figure 4–5 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 on 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 interface** use the operating system user defined by the Oracle Secure Backup user to access the host. In the example shown in Figure 4–5, 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 **obtool** `mkuser` command.

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 Oracle Secure Backup Web tool or the obtool `mkuser` command. 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.

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

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

> **See Also:** *Oracle Secure Backup Reference* to learn about the `mkuser` command

Creating Media Families for RMAN Backups

Oracle recommends 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" on page 1-17
> - "Editing or Displaying Media Family Attributes" on page 3-5

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" on page 3-3 for information on adding a media family with Oracle Database Control 11*g*.
- *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. Time-managed volumes can be used 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.

Caution: 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 Database Control to create a **database backup storage selector**. Database Control gives the selector a system-defined name. If you want to specify the name for the database backup storage selector, then 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 **Recovery Manager (RMAN)**. In some circumstances, however, you might want to override the database storage selectors by setting RMAN parameters.

This section assumes that you are familiar with setting RMAN media management parameters. You can specify media management parameters in RMAN by the following means:

- Environment variables, which are specified with the `ENV` parameter of the `PARMS` option on the `CONFIGURE` or `ALLOCATE CHANNEL` commands
- The RMAN `SEND` command

You can use the following Oracle Secure Backup parameters in RMAN backup and restore jobs:

- `OB_MEDIA_FAMILY[_n]`

  Use this parameter to define which media can be used for backup jobs.

- `OB_DEVICE[_n]`

  Use this parameter to define which tape drives can be used for backups.

- `OB_RESOURCE_WAIT_TIME`

Use this parameter to specify the duration for which a backup or restore job should wait for the required resources to become available.

In general, these media management parameters override the settings of matching database backup storage selectors.

> **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" on page 4-16.
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.

Primary and Subordinate RMAN Backup Jobs

When a database backup job is started, Oracle Secure Backup interprets the RMAN commands and creates a subordinate job for the database it includes. All Oracle Secure Backup RMAN backups include at least one subordinate job. But if there are conditions that require separate jobs to be spawned, then Oracle Secure Backup creates multiple subordinate jobs. If you back up two identical copies of the database to separate drives, for example, then two subordinate jobs are generated by the parent job.

The following example shows a database backup and its two subordinate jobs. In this case there are two copies of the backup being written to separate tape drives.

```
Recovery Manager: Release 10.2.0.2.0 - Production on Wed Jun 25 12:18:32 2008

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

RMAN-06568: connected to target database: TSTVW1 (DBID=1586108579, not open)
RMAN-06009: using target database control file instead of recovery catalog

RMAN> run {
2> set backup COPIES 2 ;
```

```
3> backup tablespace tbs_mult ;
4> }
5>
RMAN-03023: executing command: SET BACKUP COPIES

RMAN-03090: Starting backup at 25-JUN-08
RMAN-08030: allocated channel: ORA_SBT_TAPE_1
RMAN-08500: channel ORA_SBT_TAPE_1: sid=93 devtype=SBT_TAPE
RMAN-08526: channel ORA_SBT_TAPE_1: Oracle Secure Backup
RMAN-08008: channel ORA_SBT_TAPE_1: starting full datafile backupset
RMAN-08010: channel ORA_SBT_TAPE_1: specifying datafile(s) in backupset
RMAN-08522: input datafile fno=00004 name=/ade/jfersten_tstvw1/oracle/dbs/tbs_mult.dat
RMAN-08038: channel ORA_SBT_TAPE_1: starting piece 1 at 25-JUN-08
RMAN-08053: channel ORA_SBT_TAPE_1: finished piece 1 at 25-JUN-08 with 2 copies
and tag TAG20080625T121838
RMAN-08503: piece handle=06jjqgcu_1_1 comment=API Version 2.0,MMS Version 10.2.0.0
RMAN-08503: piece handle=06jjqgcu_1_2 comment=API Version 2.0,MMS Version 10.2.0.0
RMAN-08540: channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:11:06
RMAN-03091: Finished backup at 25-JUN-08

Recovery Manager complete.
```

The primary job is sbt/8:

```
ob> lsj -l --log sbt/8
sbt/8:
    Type:                   database tstvw1 (dbid=1586108579)
    Scheduled time:         none
    State:                  completed successfully at 2008/06/25.12:29
    Priority:               100
    Privileged op:          no
    Run on host:            (administrative server)
    Attempts:               0
    Log:
        2008/06/25.12:29:37 Job completed successfully.
```

The subordinates spawned by sbt/8 are sbt/8.1 and sbt/8.2.

```
ob> lsj -l sbt/8.1
sbt/8.1:
    Type:                   datafile backup
    Backup piece:           06jjqgcu_1_1
    Family:                 verylongmediafamilyname
    Encryption:             off
    Scheduled time:         none
    State:                  completed successfully at 2008/06/25.12:29
    Priority:               100
    Privileged op:          no
    Run on host:            brhost3
    Attempts:               1
ob> lsj -l sbt/8.2
sbt/8.2:
    Type:                   datafile backup
    Backup piece:           06jjqgcu_1_2
    Family:                 verylongmediafamilyname
    Encryption:             off
    Scheduled time:         none
    State:                  completed successfully at 2008/06/25.12:29
    Priority:               100
    Privileged op:          no
    Run on host:            brhost3
```

```
    Attempts:              1
```

In job descriptions, Oracle Secure Backup assigns these jobs names determined by what type of RMAN backup is being performed. Valid types include archivelog, database, datafile, and controlfile. Oracle Secure Backup assigns each RMAN job an identifier whose prefix is the parent sbt job id, followed by a dot (.), followed by a unique small number. For example, 15.1 could be a subordinate job for scheduled job 15. The following example shows a typical `lsj` output containing a variety of Oracle Secure Backup RMAN backups:

```
sbt/1.1 none  archivelog backup        completed successfully at 2008/06/25.12:04
sbt/2   none  database tstvw1          completed successfully at 2008/06/25.12:04
sbt/2.1 none  controlfile autobackup   completed successfully at 2008/06/25.12:04
sbt/3   none  database tstvw1          completed successfully at 2008/06/25.12:05
sbt/3.1 none  datafile backup          completed successfully at 2008/06/25.12:05
sbt/4   none  database tstvw1          completed successfully at 2008/06/25.12:06
sbt/4.1 none  restore piece '03jgj1_1' completed successfully at 2008/06/25.12:06
sbt/5   none  database tstvw1          completed successfully at 2008/06/25.12:06
sbt/5.1 none  incremental backup       completed successfully at 2008/06/25.12:06
sbt/6   none  database tstvw1          completed successfully at 2008/06/25.12:12
sbt/6.1 none  datafile backup          completed successfully at 2008/06/25.12:12
sbt/7   none  database tstvw1          completed successfully at 2008/06/25.12:17
sbt/7.1 none  restore piece '05jgj0_1' completed successfully at 2008/06/25.12:17
sbt/8   none  database tstvw1          completed successfully at 2008/06/25.12:29
sbt/8.1 none  datafile backup          completed successfully at 2008/06/25.12:29
sbt/8.2 none  datafile backup          completed successfully at 2008/06/25.12:29
```

Performing Backups with RMAN and Oracle Secure Backup

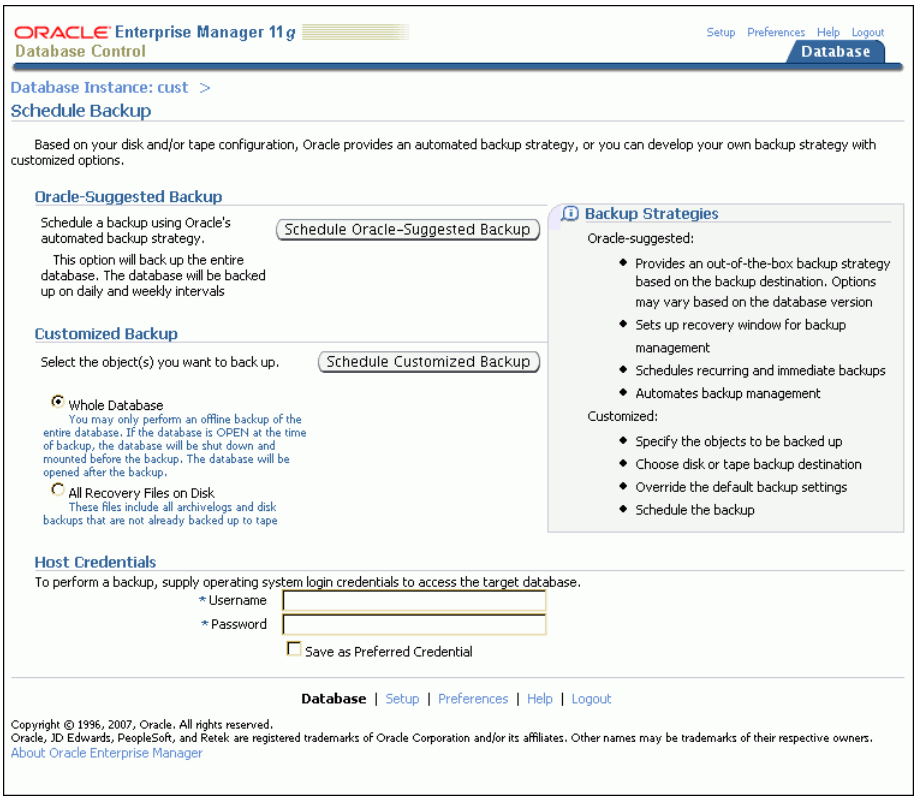
After you have configured RMAN to use the Oracle Secure Backup **SBT interface**, the procedure for making RMAN backups is the same as described in *Oracle Database Backup and Recovery User's Guide*. This section describes how to use Enterprise Manager to back up the whole database through the Oracle Secure Backup SBT interface.

To back up the database using Oracle Database Control 11*g*:

1. Log in to the Oracle Enterprise Manager Database Control as an **Oracle Secure Backup user** with database administrator **rights**.
2. Click **Availability**.

   The Availability subpage appears.
3. In the Manage section, click **Schedule Backup**.

   The Database Instance: *database_name* > Schedule Backup page appears.



4. Perform the following actions:

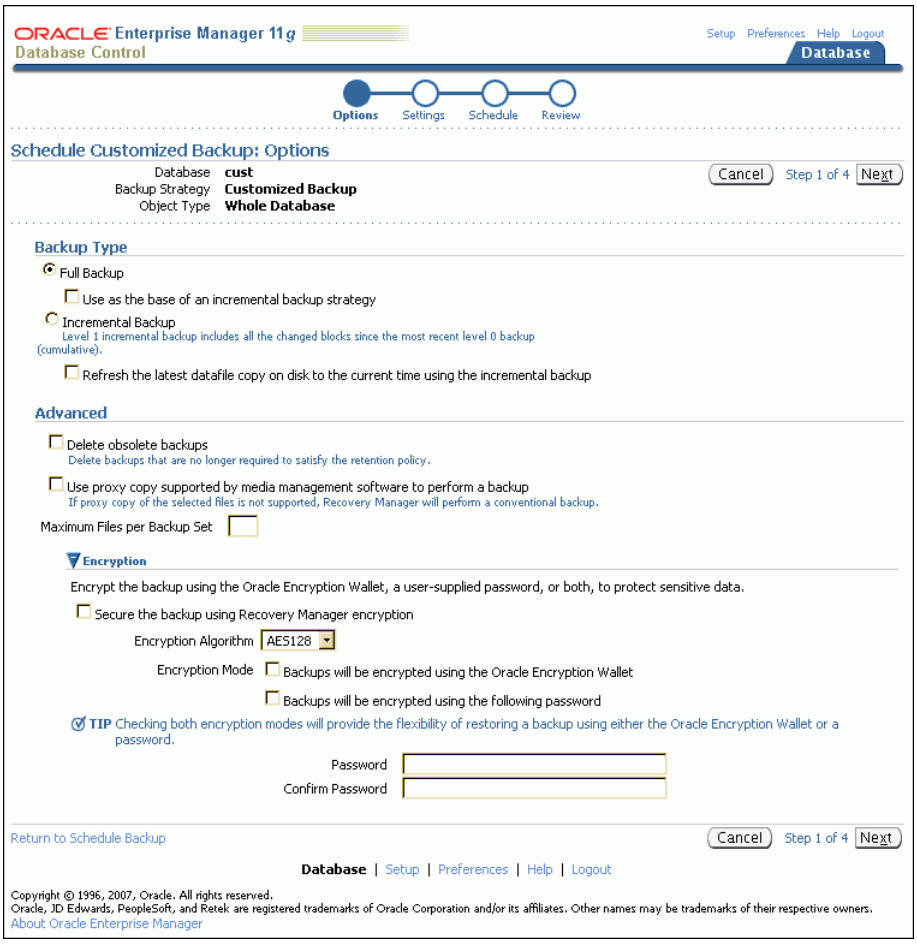
   a. In the Customized Backup section, select **Whole Database**.

      This option specifies an online backup of the Oracle Database data files and archive logs.

   b. In the Host Credentials section, enter the credentials of an Oracle Secure Backup user with access to the targeted database in the **Username** and **Password** fields. Select **Save as Preferred Credential** if you want Oracle Database Control 11*g* to remember these credentials.

   c. Click **Schedule Customized Backup**.

   The Schedule Customized Backup: Options page appears.

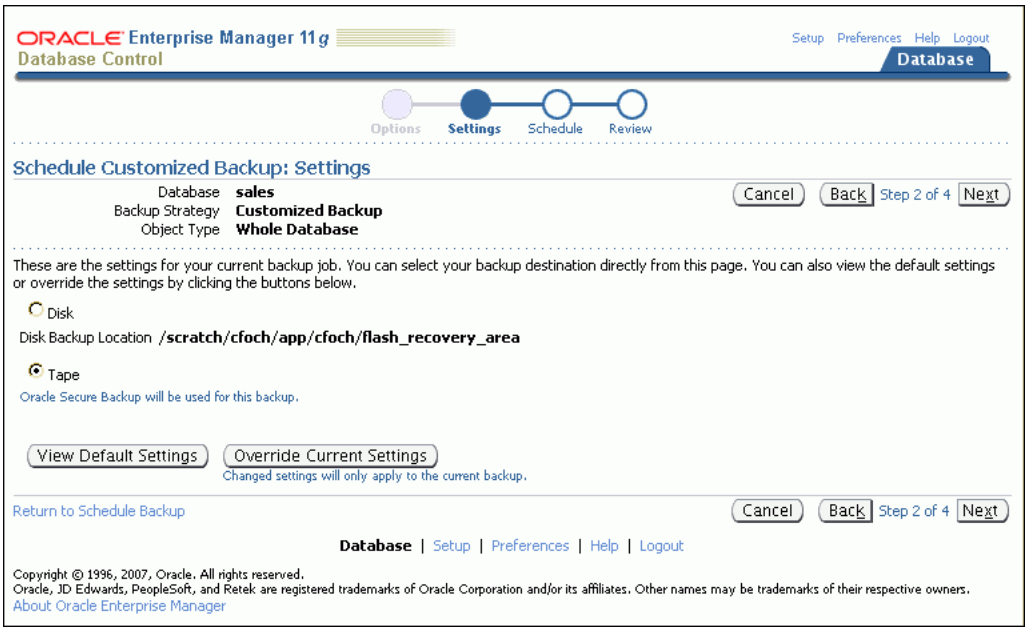


5. Select **Full Backup** in the Backup Type section.
6. Select the **Secure the backup using Recovery Manager encryption** option if you want to encrypt the backup using RMAN encryption.
   a. Select an encryption algorithm from the **Encryption Algorithm** list.
   b. Select an encryption mode.

      Selecting both encryption modes provides the flexibility of restoring a backup using either the Oracle Secure Backup encryption **wallet** or a password.

      If you select password-protected encryption, then enter a password in the **Password** and **Confirm Password** fields.
7. Click **Next**.

   The Schedule Customized Backup: Settings page appears.

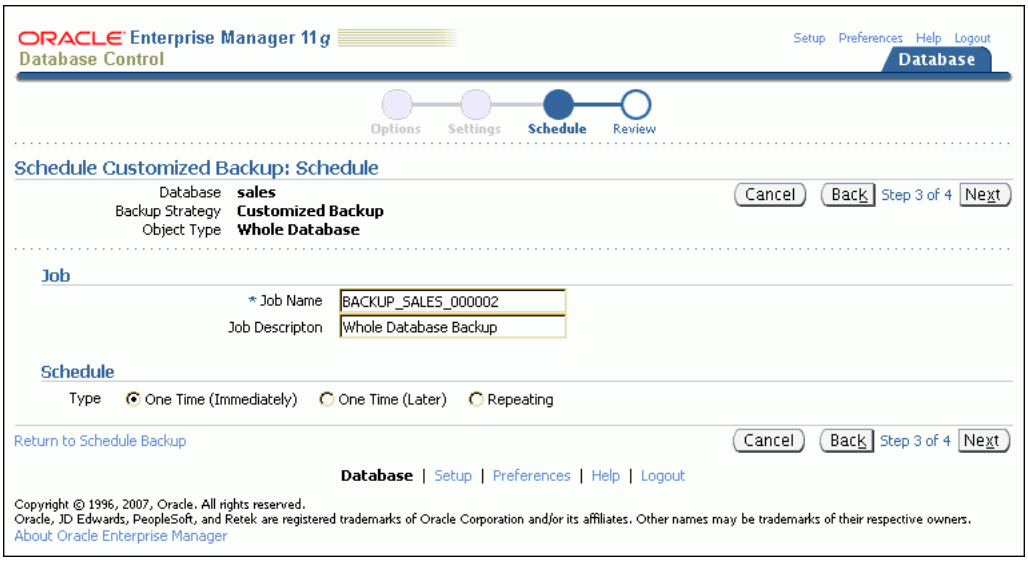


8. Click **View Default Settings** to view the backup settings for the current backup.

   Click **Override Current Settings** to go the Backup Settings page, which allows you to change the current settings for number of tape drives and tape backup type. Click the **Override** button in the Oracle Secure Backup section of the Backup Settings page to change the media family, designated tape drives, or both for the current backup only.

   Select the **Tape** option and then click **Next**.

   The Schedule Customized Backup: Schedule page appears.



9. In the Job section, this page displays a job name in the **Job** field and the type of backup in the **Job** Description field.

   Select a schedule type. Your options are:

   - **One Time (Immediately)**

- **One Time (Later)**
- **Repeating**

Click **Next**.

The Schedule Customized Backup: Review appears.

10. Review your backup characteristics and then click **Submit Job**.

    The Status page appears.

11. Click **View Job** to monitor the progress of the backup.

    The Execution: *database_name* page appears.

    Refresh the page until the **Backup** link appears.

12. Click **Backup**.

    The Step: Backup page appears.

    Refresh this page to display the RMAN output for the backup job.

Performing Recovery with RMAN and Oracle Secure Backup

After you have configured RMAN to use the Oracle Secure Backup **SBT interface**, the procedure for restoring database files is the same as described in *Oracle Database Backup and Recovery User's Guide*. For step-by-step instructions on restoring and recovering your whole database using Oracle Database Control, see the Oracle by Example at the following URL:

`http://www.oracle.com/technology/obe/11gr1_2day_dba/backup/backup.htm#t6`

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 **SBT interface** to Oracle Secure Backup.

  This option is available with Oracle9*i* forward. While encryption occurs outside the database, the data is encrypted on the server prior to 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: Chapter 10, "Managing Backup Encryption"

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

Oracle Secure Backup maintains a **catalog** of metadata for Oracle Secure Backup jobs on the **administrative server**. You can use the Oracle Secure Backup **Web tool** to display catalog metadata about each **backup piece**, referred to as a **backup image** in the Oracle Secure Backup Web tool. Alternatively, you can use the `lsjob`, `catxcr`, and `lspiece` commands in **obtool**.

> **See Also:** *Oracle Database Backup and Recovery User's Guide* for more information on accessing RMAN metadata

Expiration of RMAN Backups on Tape

You can make RMAN backups on a **volume** that use a **content-managed expiration policy** or a **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 as long as 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 will then fail 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 interface** are subject to all Oracle Secure Backup job management commands.

> **See Also:** "Managing Backup and Restore Jobs" on page 8-1

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 2005/08/11.11:29
oracle/1.1       none    datafile backup                completed successfully at 2005/08/11.11:29
oracle/2         none    database orcl (dbid=1091504057) completed successfully at 2005/08/11.11:56
oracle/2.1       none    datafile backup                completed successfully at 2005/08/11.11:56
oracle/3         none    database orcl (dbid=1091504057) completed successfully at 2005/08/11.11:57
oracle/3.1       none    restore piece '06grqejs_1_1'   completed successfully at 2005/08/11.11:57
```

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**.

Example 4–3 Transcript of an Archived Log Backup Job

```
ob> catxcr --head 22 sbt/6.1
2005/06/28.13:01:04
```

```
2005/06/28.13:01:04
2005/06/28.13:01:04         Transcript for job sbt/6.1 running on stadv07
2005/06/28.13:01:04
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 2005
    Media family:       RMAN-DEFAULT
    Volume set expires: never; content manages reuse

Archive label:
    File number:        1
    File section:       1
    Owner:              root
    Client host:        stadv07
    Backup level:       0
    S/w compression:    no
    Archive created:    Tue Jun 28 13:01:30 2005
```

See Also:

- *Oracle Secure Backup Reference* for complete syntax and semantics for the **obtool** `catxcr` command
- "Displaying Job Transcripts" on page 8-4 for instructions on using the Oracle Secure Backup **Web tool** to display job transcripts

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 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** piece 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 obtool `lspiece` command to display information about backup pieces recorded in the Oracle Secure Backup **catalog**. Example 4–4 shows sample output for `lspiece`.

Example 4–4 Displaying Backup Pieces

```
ob> lspiece --long
Backup piece OID:       104
    Database:               ob
    Database ID:            1566254457
    Content:                archivelog
    Copy number:            0
    Created:                2005/06/28.13:01
    Host:                   stadv07
    Piece name:             05go3tgd_1_1
Backup piece OID:       105
    Database:               ob
    Database ID:            1566254457
    Content:                archivelog
    Copy number:            0
    Created:                2005/06/28.13:02
    Host:                   stadv07
    Piece name:             06go3ti5_1_1
```

> **See Also:**
>
> - "RMAN Backup Sets and Oracle Secure Backup Images" on page 4-3
> - "Managing Backup Images" on page 8-10 for instructions on using the Oracle Secure Backup Web tool to display information about backup pieces
> - *Oracle Secure Backup Reference* for complete syntax and semantics for the obtool `lspiece` command

Using RMAN and Oracle Secure Backup in an Oracle RAC Environment

You can use the Oracle Secure Backup SBT library in conjunction with RMAN to back up a database in an Oracle Real Application Clusters (Oracle RAC) system.

This section contains these topics:

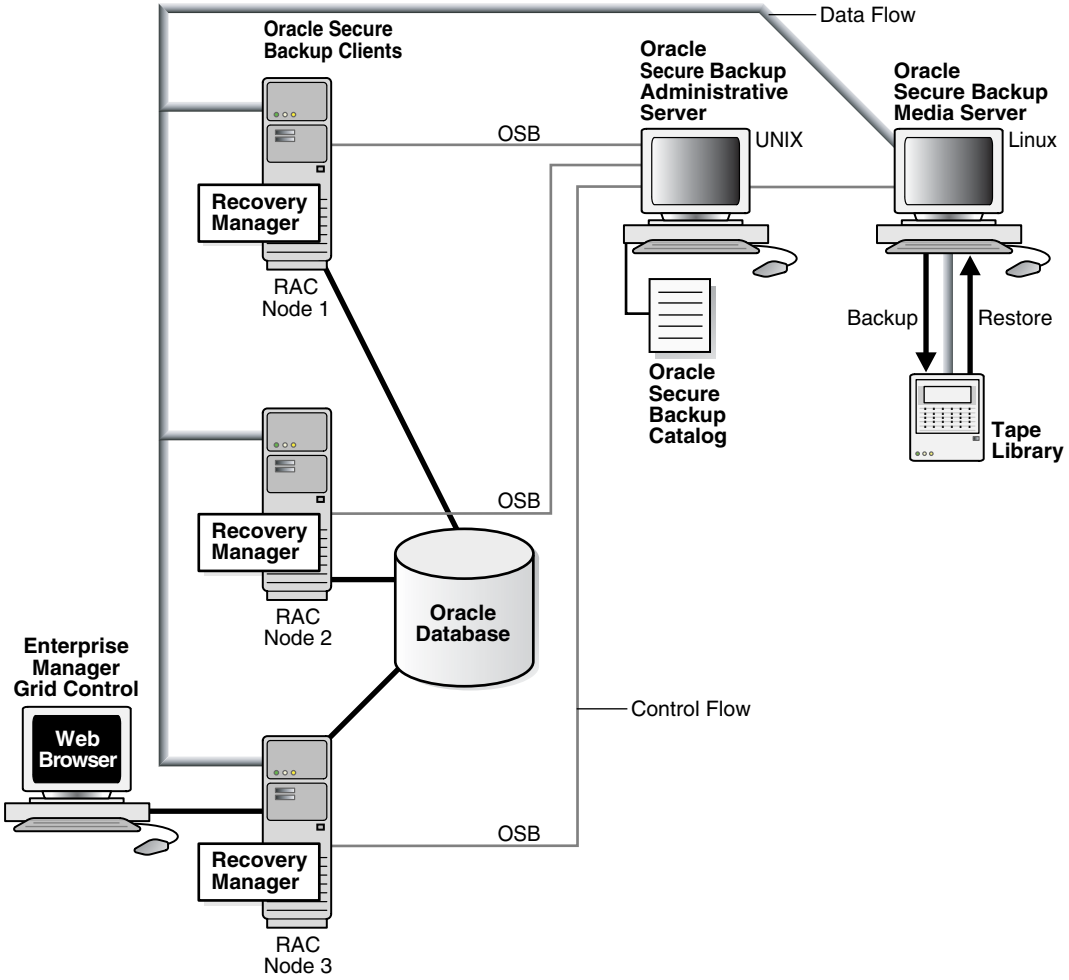
- Installing Oracle Secure Backup in an Oracle RAC Environment
- Network Versus Local Backups
- Duplexed Backup Operations

Installing Oracle Secure Backup in an Oracle RAC Environment

Oracle recommends 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 Oracle Secure Backup **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. Beginning with Oracle Database 10*g* release 2 (10.2), RMAN backups can be dynamically allocated in the Oracle RAC environment based on the work load distribution. This 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.

But if one of the nodes in the Oracle RAC environment is a **media server**, then it is more efficient for that node always to perform a backup operation, writing to a locally accessed **tape device**. This avoids having to use network bandwith for backups, as would happen if a RAC node configured as a client were to perform the backup.

You can configure RMAN backups to be performed from specific nodes. Oracle recommends 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 should be used, three from each host. This gets configured once and will apply to every backup and restore operation, unless you override this setting. You can then start an RMAN operation by connecting to any node within the Oracle RAC environment, and the operation will be performed only on the two configured hosts.

Note: If you choose not to configure persistent settings, then you can accomplish the same thing in RMAN scripts by allocating channels by host.

Duplexed Backup Operations

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" on page 3-1
- "Database Backup Storage Selectors" on page 4-3

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 database 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 will be failed for the other copy as well.

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

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 tape. 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 backup**s, 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

This section provides an overview of file system backups using Oracle Secure Backup.

This section contains these topics:

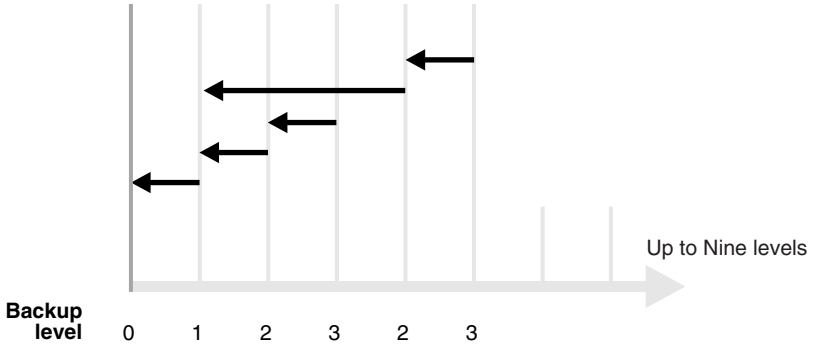
- Choosing a Backup Strategy
- Choosing a Backup Schedule

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 the same as a level 10 incremental backup. Oracle Secure Backup does not support the level 10 backup in conjunction 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/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" on page 5-9

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.

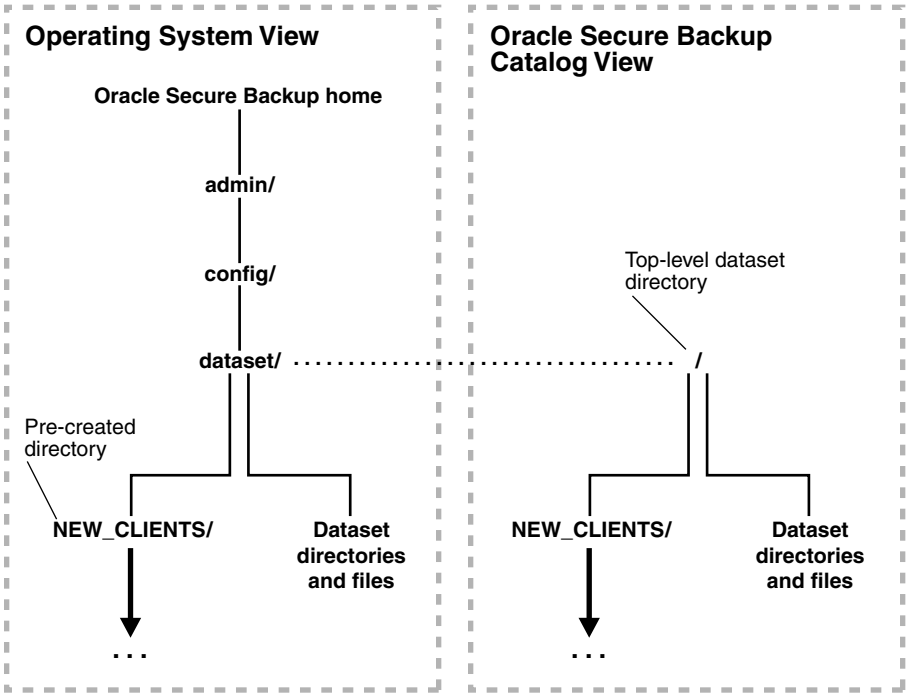
Example 5–1 Sample Dataset File

```
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
}
```

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" on page 5-10
- *Oracle Secure Backup Reference* for a description of the Oracle Secure Backup dataset language and information on the obtool dataset commands

Scheduled Backups

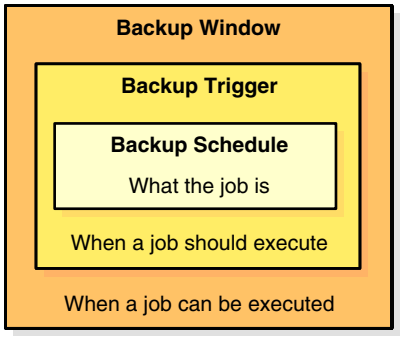
A **scheduled backup** is the basis of your backup strategy. Your first task after setting up the **administrative domain** should be choosing and configuring a **backup schedule** that makes sense for your environment.

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 will be 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 will continue 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: "About Backup Schedules" on page 5-18

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:

- "Oracle Secure Backup Users and Passwords" on page 2-1
- *Oracle Secure Backup Reference* for more information on the `perform backups as privileged user` right

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 **Network Data Management Protocol (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 new 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" on page 8-13

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 Oracle Secure Backup **Web tool** to browse the catalog to determine what you have backed up.

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 interface**, it records the name and attributes of the objects it backs up. It writes this data to the catalog stored on the **administrative server**.

> **See Also:** "Database Backups" on page 4-3

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 that you want 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.

> **See Also:** "Oracle Secure Backup Classes and Rights" on page 2-3 for more information on 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.

Oracle Secure Backup provides two means to control how time affects the data you select when browsing backup catalogs:

- Catalog 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 5–1. The data selector describes, either explicitly or by inference, the identity of each **backup image** section containing the data of interest.

> **See Also:** "Backup Images and Media" on page 1-8 for more information on backup images and sections

Table 5–1 Data Selectors

Selector	Description
`latest`	Shows most recent file system objects.

Table 5–1 (Cont.) Data Selectors

Selector	Description
`earliest`	Shows least recent file system objects.
`all`	Shows all instances of file system objects.
backup-id	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 numerical 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.
date-time	Shows the file system object as it existed in a backup no later than the given date and time.
date-range	Shows all objects backed up exactly between two date-time values.

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 more information on 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 5–2 shows the files that are backed up as well as 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 5–2 Backup of the /numbers Directory

Date	Contents of /numbers				Backup volume and image	Backup ID
5/1/05	`file1.dat`	`file2.dat`	`file3.dat`		volume FULL-02, file 5	20
5/2/05		`file2.dat`	`file3.dat`		volume FULL-02, file 9	30
5/3/05	`file1.dat`	`file2.dat`			volume FULL-03, file 3, section 1	40
		`file2.dat`		`file4.dat`	volume FULL-04, file 3, section 2	46

Table 5–3 describes the effect of various data selectors on the file system object references.

Table 5–3 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)

Table 5–3 (Cont.) Data Selectors for Backups of the /numbers Directory

Data Selector	Object Reference	Backup Image Sections Selected (Backup IDs)
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)
05/05	`/numbers/file1.dat`	(none)
05/05	`/numbers`	FULL-02, file 9 (30)
05/04-05/05	`/numbers/file4.dat`	(none)
05/04-05/05	`/numbers/file1.dat`	FULL-02, file 5 (20)
05/04-05/05	`/numbers`	FULL-02, file 5 (20) and FULL-02, file 9 (30)

Catalog View Modes

The catalog view mode is independent of data selectors. 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 two 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 5–2 on page 5-7 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 the data selector. If you set the view mode to exact, then the `latest` setting in Table 5–3 would display only file1.dat, file2.dat, and file4.dat.

Backing Up Individual Files

Some **Network Data Management Protocol (NDMP)** data services provide only for backup of directories and their contents. 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.

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 will 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** as well as 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" on page 5-2

- How frequently will 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 will probably spend more time performing the backups and less time restoring data. If you schedule includes less frequent full backups, then you will 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 more than one **administrative domain**.

  See Also: "Administrative Domains, Catalog Data and Configuration Files" on page 1-2

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" on page 5-2

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 incremental 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** to fully restore a given tree. If you use incremental backups, however, then you might be required to restore several backup images.

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 in order to restore a directory, only the level 0 backup and one level 3 backup from the date required would be necessary.

A **differential incremental 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 tape. 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.

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:

See Also:

- "Backup Datasets" on page 5-2
- *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 that you want 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 5–2 brhost2.ds

```
include host brhost2 {
    exclude name core
    exclude name *.bak
    exclude name *~

    include path /
    include path /usr
    include path /home
}
```

Example 5–3 includes all files in the / and /usr file systems on host brhost3 except for core dumps and editor backup files.

Example 5–3 brhost3.ds

```
include host brhost3 {
    exclude name core
    exclude name *.bak
    exclude name *~

    include path /
    include path /usr
}
```

Example 5–4 includes all files in the C:\Documents and Settings folder on host winhost1 except for log files.

Example 5–4 winhost1.ds

```
include host winhost1
include path "C:\Documents and Settings" {
  exclude name *.log
}
```

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.

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
```

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 a number of 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.

Example 5–6 brhosts.ds

```
include host brhost2
include host brhost3
include host brhost4

include path /
include path /home
```

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 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

Displaying the Datasets Page

In the Backup page, click **Datasets** to display the page shown in Figure 5–4. This page lists every **dataset file** and **dataset directory**. Dataset directories appear in the Path list with a forward 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.

Figure 5–4 Datasets Page

See Also: *Oracle Secure Backup Reference* to learn about the dataset commands in **obtool**

Adding a Dataset File

To add a **dataset file** with the Oracle Secure Backup **Web tool**:

1. Follow the procedure in "Displaying the Datasets Page" on page 5-12.

   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 new 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" on page 5-14 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 with the Oracle Secure Backup **Web tool**:

1. Follow the procedure in "Displaying the Datasets Page" on page 5-12.

   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

To edit parameters in an existing **dataset file** with the Oracle Secure Backup **Web tool**:

1. Follow the procedure in "Displaying the Datasets Page" on page 5-12.

   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" on page 5-15.

   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" on page 5-14.

Renaming a Dataset

To rename a **dataset file** or **dataset directory** with the Oracle Secure Backup **Web tool**:

1. Follow the procedure in "Displaying the Datasets Page" on page 5-12.

   The Backup: Datasets page appears.

2. Select the dataset file or directory from the **Path** list and click **Rename**.

   A new page appears.

3. Enter the new 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

To remove a **dataset file** or **dataset directory** with the Oracle Secure Backup **Web tool**:

1. Follow the procedure in "Displaying the Datasets Page" on page 5-12.

   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:

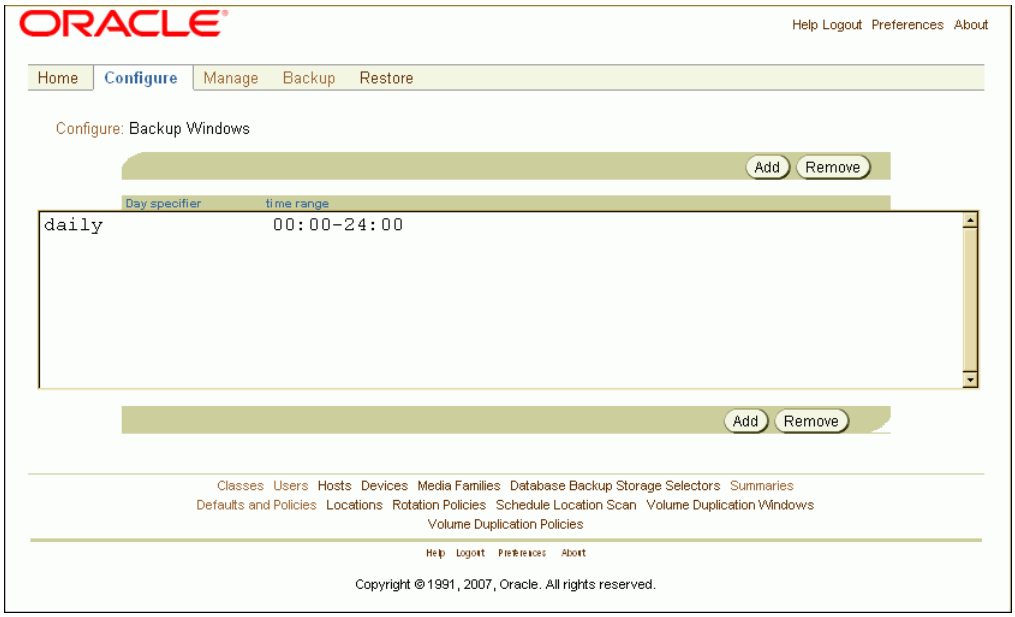
- Displaying the Backup Windows Page
- Adding a Backup Window
- Removing a Backup Window

> **See Also:** "Scheduled Backups" on page 5-4 for a conceptual overview of backup windows

Displaying the Backup Windows Page

In the Configure subpage, click **Backup Windows** in the Advanced section to display the page shown in Figure 5–5. You can perform all **backup window** creation and configuration tasks in this page or in pages to which it provides links.

Figure 5–5 Backup Windows Page



See Also: *Oracle Secure Backup Reference* to learn about the backup window commands in **obtool**

Adding a Backup Window

To add a **backup window** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Backup Windows Page" on page 5-15.

   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 already 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 new backup window.

   The Configure: Backup Windows page displays a success message, and your new 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 new 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

To remove an existing **backup window** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Backup Windows Page" on page 5-15.

   The Configure: Backup Windows page appears.

2. Select the backup window that you want 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 more than one time range 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" on page 5-16

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:

About Backup Schedules

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 on the `modify administrative domain's configuration` right

2. Create a **dataset file** for each backup that you want 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" on page 5-10

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 will 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" on page 5-15

4. Create a **backup schedule**.

   Backup schedules specify the dataset, **media family**, backup priority, and so on.

   See Also: "Adding a Backup Schedule" on page 5-19

5. Create at least one **trigger**.

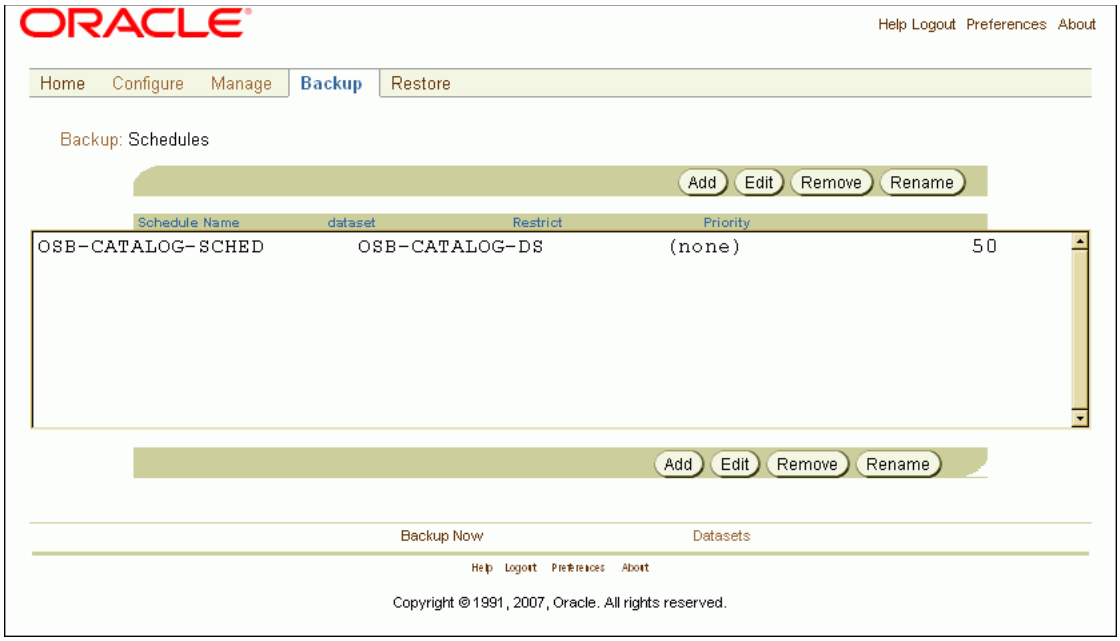
   Triggers are the days and times that the scheduled backups will run. If you create a backup schedule but do not configure triggers for this schedule, then no backups will occur.

   See Also: "Configuring Triggers" on page 5-21

Displaying the Schedules Page

In the Backup page, click **Schedules** to display the page shown in Figure 5–6. You can perform all **backup schedule** creation and configuration tasks in this page or in pages to which it provides links.

Figure 5–6 Backup Schedules Page



See Also: *Oracle Secure Backup Reference* to learn about the schedule commands in **obtool**

Adding a Backup Schedule

To add a **backup schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Schedules Page" on page 5-19.

   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. Select the **dataset file** or **dataset directory** that you want to include in the backup job in the **Datasets** list.

6. Select a restriction in the **Restrictions** field.

This step is optional. You can restrict a **scheduled backup** to specific tape devices. 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.

7. Enter any information that want to store with the backup schedule in the **Comments** field.

   This step is optional

8. Click **OK**.

   The Backup: Schedules page displays a success message, and your new backup schedule appears in the list of schedules.

Editing or Viewing Backup Schedule Properties

To edit or view properties for an existing **backup schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Schedules Page" on page 5-19.

   The Backup: Schedules page appears.

2. In the Schedules page, select the schedule you want to edit or view and click **Edit**.

   The Backup: Schedules > *schedule_name* page appears.

3. Make whatever changes you want.

   You cannot rename a backup schedule from this page. To rename a backup schedule, see "Renaming a Backup Schedule" on page 5-21.

4. Click Apply to apply the changes and remain on the Backup: Schedules > *schedule_name* page.

5. 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.

6. 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 will never run.

   See Also: "Configuring Triggers" on page 5-21

7. Click **Cancel** to return to the Backup: Schedules page without changing anything.

   If you have already 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

To remove an existing **backup schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Schedules Page" on page 5-19.

   The Backup: Schedules page appears.

2. Select the backup schedule that you want to remove from the list of schedules and click **Remove**.

A new page appears with a confirmation message.

3. 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

To rename a **backup schedule** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Schedules Page" on page 5-19.

   The Backup: Schedules page appears.

2. Select the backup schedule that you want to rename from the list of schedules and click **Rename**.

   A new page appears.

3. Enter a new 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 new 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 will never run.

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

To display the Oracle Secure Backup **Web tool** Triggers page:

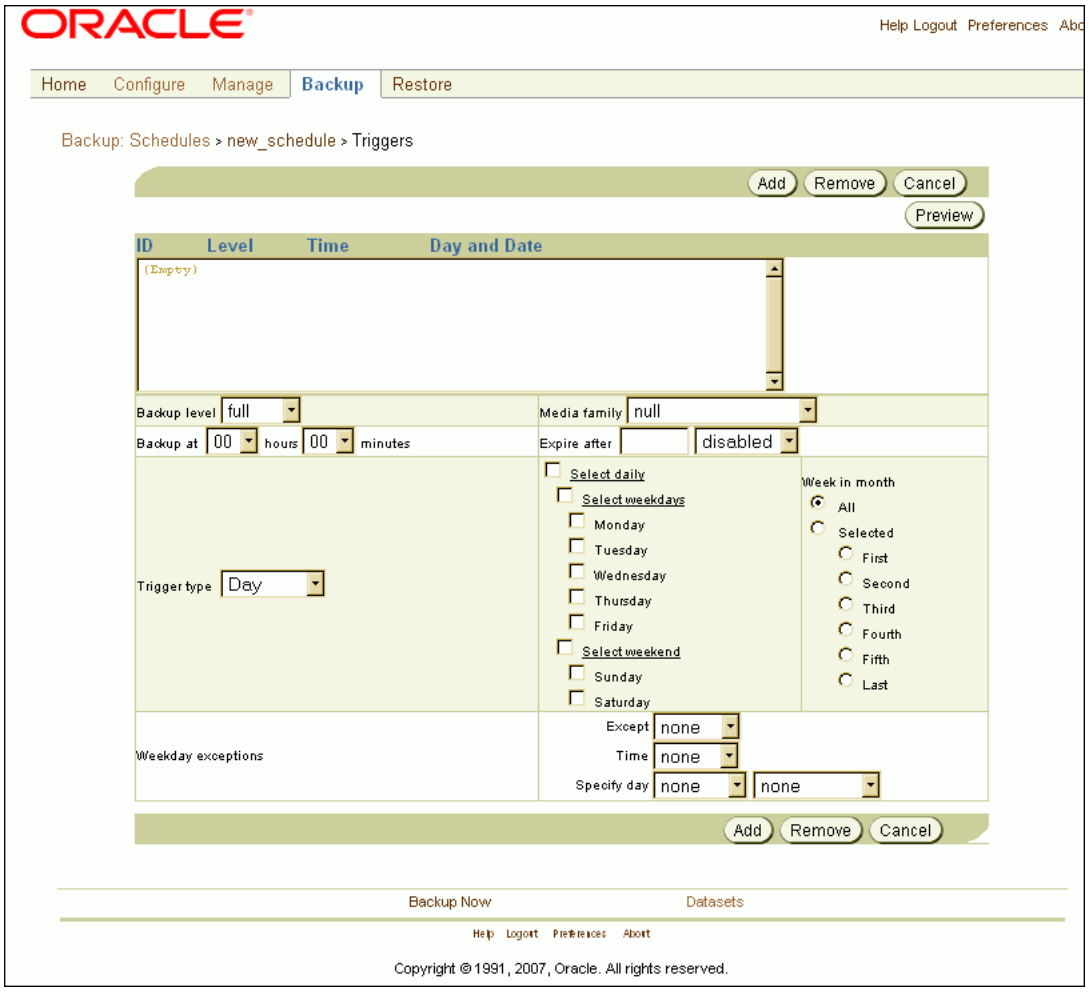
1. In the Backup page, click **Schedules**.

   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* > Triggers page appears, as shown in Figure 5–7.

Figure 5–7 Triggers Page



Creating a One-Time Backup Trigger

To create a one-time backup **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 the same as 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 numerical backup level.

   - **incr**

Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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** 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 that you want 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 new trigger appears in the list of triggers.

Creating a Daily Backup Trigger

To create a daily backup **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 the same as 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 numerical backup level.

   - **incr**

     Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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** 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 will run 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 will run. Your choice 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 new trigger appears in the list of triggers.

Creating a Monthly Backup Trigger

To schedule a monthly backup **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 the same as 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 numerical backup level.
   - **incr**

     Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

     Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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** 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 new trigger appears in the list of triggers.

Creating a Quarterly Backup Trigger

To schedule a quarterly backup **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 the same as 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 numerical backup level.
   - **incr**

     Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

     Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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** 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 the following 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 new trigger appears in the list of triggers.

Creating a Yearly Backup Trigger

To create a yearly backup **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 the same as 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 numerical backup level.

   - **incr**

     Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

     Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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** 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 the following 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 new trigger appears in the list of triggers.

Editing a Trigger

To edit a **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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 new trigger that differs only slightly from an existing trigger by editing the existing trigger and then clicking **Add**.

Removing a Trigger

To remove a **trigger** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   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

To display a **trigger** schedule with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Triggers Page" on page 5-21.

   The Backup: Schedules > *schedule_name* > Triggers page appears.
2. Select the trigger you want displayed and click **Preview**.

Performing On-Demand File System Backups

This section contains these topics:

- 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" on page 5-4

About 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** as well as 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.

   You must have the `modify administrative domain's configuration` right to create a **dataset file**.

   See Also:

   - "Creating Dataset Files" on page 5-10
   - *Oracle Secure Backup Reference* for more information on 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 backup**s and the `perform backups as privileged user` right to perform **privileged backup**s.

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:

   - "Jobs and Requests" on page 1-18
   - "Adding an On-Demand Backup Request" on page 5-30

4. Review, delete, or add to the list of backup requests.

   This step is optional.

   See Also:

   - "Displaying the Backup Now Page" on page 5-30
   - "Removing a Backup Request" on page 5-32

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" on page 5-32

Displaying the Backup Now Page

In the Oracle Secure Backup **Web tool** Backup page, click **Backup Now** to display the page shown in Figure 5–8. 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.

You can perform all **on-demand backup** creation and configuration tasks in this page or in pages to which it provides links.

Figure 5–8 Backup Now Page

See Also: *Oracle Secure Backup Reference* to learn about the backup commands in obtool

Adding an On-Demand Backup Request

To add an on-demand **backup request** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Backup Now Page" on page 5-30.

   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. 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.

5. 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 will never expire.

> **See Also:** *Oracle Secure Backup Reference* for more information

6. 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 the same as 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 numerical backup level.
   - **incr**

     Select this option to back up only data modified since the last backup, regardless of its backup level. This option is the same as backup level 10.

     Caution: Oracle Secure Backup does not support the **incr** backup level in conjunction 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/incremental **backup schedule**. This option is useful when you want to create a **backup image** for off-site storage without disturbing your **incremental backup** schedule.
7. Select a **media family** to which this backup should be assigned in the **Media family** list.
8. Select restrictions on this backup in the **Restrictions** field. You can select a particular **tape device**. You can also use click and shift-click to select a range of tape devices or control-click to select additional individual tape devices. Restrictions come in the following forms:
   - *device*

     This form specifies a particular tape device.
   - *@hostname*

     This form specifies any tape drive attached to the specified host.
   - *device@hostname*

     This form specifies any drive-host **attachment**.

   If no tape device is selected, then Oracle Secure Backup uses tape device polling to find any available tape device for use in backup and restore operations.
9. Enter a priority for the backup job in the **Priority** list.

The priority of a job is a positive integer value. 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. The default value is **100**.

10. Choose whether you want the backup to operate in **unprivileged** or **privileged** mode. Unprivileged mode is the default.

    See Also: "On-Demand Backups" on page 5-4

11. Select one of the following 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 passphase. If you select this option, then you must also select an encryption algorithm option and enter a passphrase in the **specify passphrase** field.

12. Click **OK**.

    The Backup: Backup Now page displays a success message, and your new 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 with the Oracle Secure Backup Web tool:

1. Perform the procedure in "Displaying the Backup Now Page" on page 5-30.

   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

To send every pending **backup request** to the **scheduler** with the Oracle Secure Backup **Web tool**:

1. Perform the procedure in "Displaying the Backup Now Page" on page 5-30.

   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" on page 4-22 to view the output for each job

Backing Up Critical Data on the Administrative Server

"Administrative Domains, Catalog Data and Configuration Files" on page 1-2 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 as well as all backup and **volume** records.

Oracle Secure Backup is configured on installation to perform automatic regular **catalog** backup jobs. No configuration is required, but Oracle Secure Backup catalog recovery can be extended and customized by the backup administrator.

> **See Also:** Chapter 11, "Oracle Secure Backup Catalog Recovery"

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" on page 4-1
- Chapter 11, "Oracle Secure Backup Catalog Recovery"
- *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.

  See Also: "Backup Catalog" on page 5-5 for an overview of the Oracle Secure Backup catalog

- 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: "Volumes" on page 1-11 for an explanation of volume IDs and backup images

- 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 on obtar

The sequence of steps is basically the same for both catalog-based and raw restore operations. Create a file system restore job as follows:

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:
   - If you want to restore files in privileged mode or restore to an **Network Data Management Protocol (NDMP)** host, then you need the `perform restores as privileged user` right.
   - If you want to restore files in unprivileged mode, then you need the `perform restores as self` right.
   - If you want to browse the catalog, then 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 on Oracle Secure Backup rights
2. Identify the backups that you want to restore.

   For a catalog-based restore, locate the files in the catalog.

   See Also: "Browsing the Backup Catalog" on page 6-4

   For a raw restore, identify the volumes and **backup section** file numbers from which to restore the backups.

   See Also: "Displaying Backup Sections" on page 8-10
3. Create one or more restore requests.

   See Also:
   - "Sending Catalog-Based Restore Requests to the Scheduler" on page 6-7
   - "Sending Raw Restore Requests to the Scheduler" on page 6-11

   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 on background timeout.
4. Delete the queued restore requests if necessary.

See Also:

- "Removing a Catalog-Based Restore Request" on page 6-7
- "Removing a Raw Restore Request" on page 6-11

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 Catalog-Based Restore Requests to the Scheduler" on page 6-7
   - "Sending Raw Restore Requests to the Scheduler" on page 6-11

Performing a Catalog-Based Restore Operation

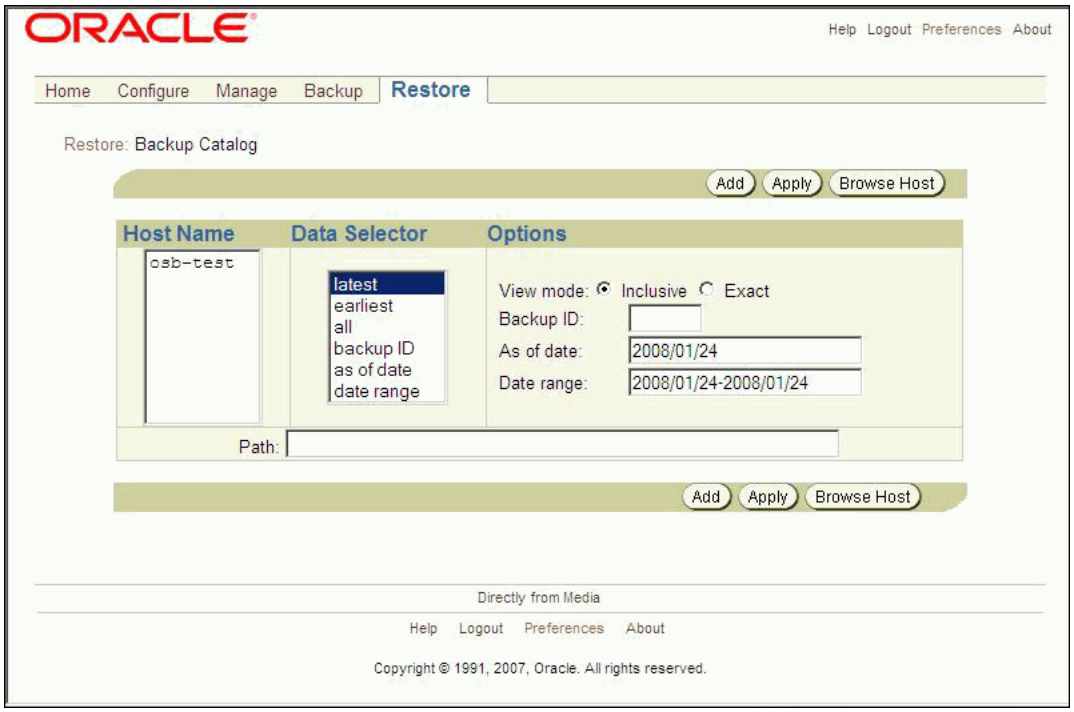
This section describes how to create a restore request by browsing a backup **catalog**.

This section contains these topics:

Displaying Backup Catalog Page

In 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

To browse the **catalog** and designate specific data to restore:

1. Perform the procedure in "Displaying Backup Catalog Page" on page 6-3.

   The Restore: Backup Catalog page appears.

2. Select a host name from the **Host Name** list.

   The host should be the one on which the data was originally backed up.

3. Select one or more data selectors in the **Data Selector** list.

   See Also: "Catalog Data Selectors" on page 5-6

4. Select any of the following data selector options.

   - **backup ID**

     If you select this option, then you must also enter one or more comma-delimited backup IDs in the **Backup ID** field.

     See Also: "Listing All Backups of a Client" on page 6-8 explains how to obtain a backup ID from the list of backups for this **client**

   - **as of date**

     If you select this option, then you must also enter a date, time, or both in the **As of date** field.

   - Select **date range** and enter the range in the **Date range** field.

     If you select this option, then you must also enter a range in the **Date range** field. For example, you could enter `2007/5/1-2007/5/31`.

5. Select a **View mode**.

   See Also: "Catalog View Modes" on page 5-8 for a description of the inclusive and exact view modes

6. You can enter the path name of the directory to browse in the **Path** field. If you do not enter a path, then Oracle Secure Backup displays the top-most directory in the **client** naming hierarchy.
7. Click **Browse Host**.

   The Restore: Backup Catalog > *host_name* page appears with the selected directory contents displayed.
8. Click a directory name to make it your current directory and view its contents.

   You can repeat this operation until you find the data to be restored. The Oracle Secure Backup **Web tool** displays the contents of the selected directory, with the directory name in gray if you have visited it or in orange if you have not.
9. To change the data selector at any time without leaving this page:
   - Adjust the selections in the **Data Selector** list.
   - Update the **Backup ID**, **As of date**, or **Date range** fields if any apply.
   - Click **Apply**.

     The Restore: Backup Catalog page appears with the new data selector applied. If the view mode is inclusive, then it will look the same as the previous page. The instances of file system objects selected when you display properties, however, will reflect the new data selector setting.
10. To change the view mode without leaving this page:
    - Select either **Inclusive** or **Exact** view mode.
    - Click **Apply**.

      Oracle Secure Backup applies the new view mode and redisplays the page.

Creating a Catalog-Based Restore Request

This section explains how to specify various restore options in order to finalize the restore request.

To create a catalog-based restore request:

1. 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**.
2. 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.

3. You can enter an alternate path name for each file or directory to restore.

   This step is optional.

   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.

   Caution: 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.

4. You can select the **Device** option to specify a **tape drive** to use to perform the restore operation.

   This step is optional.

   By default, Oracle Secure Backup automatically selects the best tape drive.

5. Choose whether you want the restore to operate in **unprivileged** or **privileged** mode.

   An unprivileged restore runs under your UNIX user identity or Windows account identity, as configured in your **Oracle Secure Backup user** profile. Your access to file system data, therefore, is constrained by the **rights** of the UNIX user or Windows 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: "Configuring Users" on page 2-8

6. You can enter one or more **obtar** options in the **Obtar option(s)** field.

   This step is optional.

   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

7. Select **No high speed positioning** if you do not want to use available position data to speed the restore.

8. Click **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 will 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** applied during the

restore job. Files that were deleted prior to 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.

9. Select one of the following:
   - **Replace existing files**

     This option overwrites any existing files with those restored from the backup image.
   - **Keep existing files**

     This option keeps any existing files instead of overwriting them with files from the backup image.
10. If you are restoring to a Windows system, then select one of the following:
    - **Replace in use files**

      This option replaces in-use files with those from the backup image. 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. 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.
12. To create additional catalog-based restore requests, return to "Browsing the Backup Catalog" on page 6-4.

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. In the Backup Catalog page, select a host from the **Host Name** list.
2. Click **Browse Host**.

   Oracle Secure Backup displays the **Browse Host** page.
3. In the **Restore items** list, select the restore request you want to remove.
4. Click **Remove**.

   Oracle Secure Backup redisplays 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. In the Backup Catalog page, select a host from the **Host Name** list.
2. Click **Browse Host**.

   Oracle Secure Backup displays the Browse Host page.
3. 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.
4. Display the transcript of the job to ensure that it completed successfully.

See Also: "Displaying Job Transcripts" on page 8-4

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**:

1. From the Backup Catalog page, select a host from the **Host Name** list box.
2. Click **Browse Host**.

   Oracle Secure Backup displays the Browse Host page.
3. 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**.

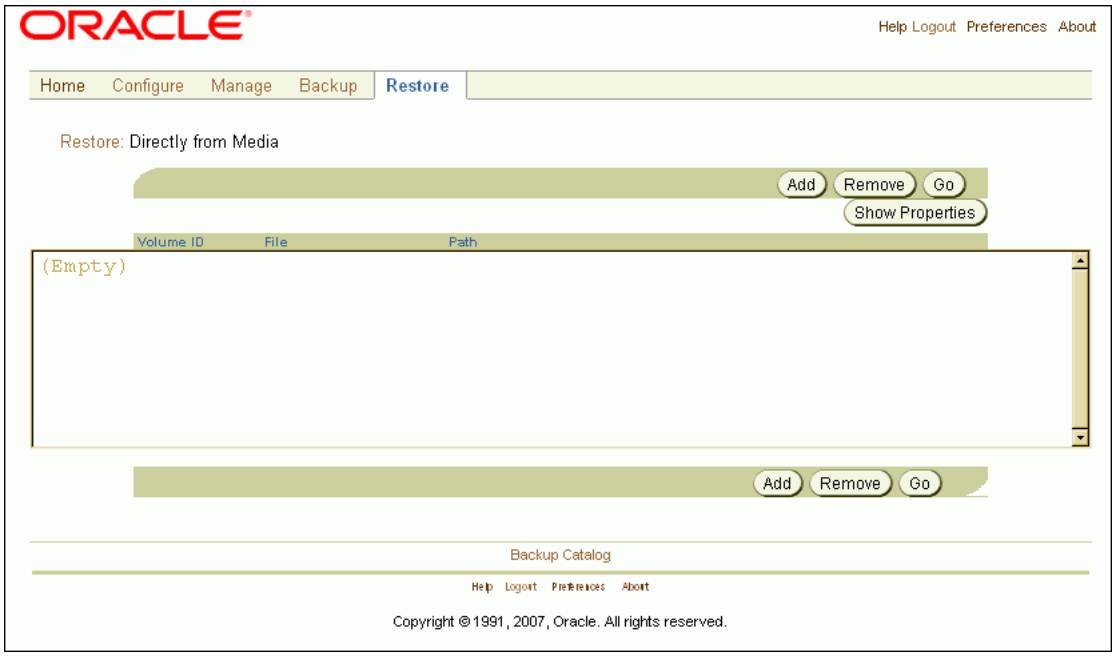
This section contains these topics:

- Displaying Directly From Media Page
- Creating a Raw Restore Request
- Removing a Raw Restore Request
- Sending Raw Restore Requests to the Scheduler

Displaying Directly From Media Page

In the Restore page, click **Directly from Media** to display the page shown in Figure 6–2. You can use this page to perform a raw restore operation.

Figure 6–2 Directly From Media Page



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**.

- The identity of the tape volumes 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. In the Directly from Media page, click **Add**.

   The Options page appears.

2. Select **Device** to specify a **tape drive** to use for the restore operation.

   This step is optional. By default, Oracle Secure Backup automatically selects the best tape drive.

3. Choose whether you want the restore to operate in **unprivileged** or **privileged** mode.

   Unprivileged mode is the default.

4. Enter the backup image file number from which to restore data in the **File Number** text field.

   See Also: "Volume Sets" on page 1-12 to learn about file numbers

5. Do at least one of the following:
   - Enter the first volume ID from which to begin data restore in the **Volume ID(s)** field

     See Also: "Volume Sets" on page 1-12 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: "Volumes" on page 1-11

6. 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 on obtar

7. Select **NDMP incremental restore** to direct certain **Network Attached Storage (NAS)** data servers to apply incremental restore rules.

   Restore operations are usually additive. Each file and directory restored from a **full backup** or an **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 prior to the last incremental backup are deleted by the NAS **data service** upon restore of that incremental backup.

8. Select one of the following:
   - **Replace existing files**

     This option overwrites any existing files with those restored from the backup image.

   - **Keep existing files**

     This option keeps any existing files instead of overwriting them with files from the backup image.

9. If you are restoring to a Windows system, then select one of the following:
   - **Replace in use files**

     This option replaces in-use files with those from the backup image. 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.

10. Select one of the following: **All** to
    - **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 as reported previously by Oracle Secure Backup, then enter it in the **Position** field. If you do not, then leave this field blank.

11. Select a host to which to restore the data in the **To host** list.
12. Enter a path name in the **Alternate path** field if you want to restore data using a different name than the one that was saved.

    For example, assume that 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 alternate directory, enter the new 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.
13. 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.

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. In the Directly from Media page, select the request that you want to remove.
2. Click **Remove**.

   Oracle Secure Backup redisplays 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. In 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.
2. Display the transcript of the job to ensure that it completed successfully.

   See Also: "Displaying Job Transcripts" on page 8-4

Part III

Managing Operations

This part explains how to manage tape devices and media and perform routine maintenance operations.

This part contains these chapters:

7

Managing Tape Devices

This chapter explains how to manage tapes and tape devices with Oracle Secure Backup.

This chapter contains these sections:

- Managing Tape Drives
- Managing Tape Libraries
- Managing Device Reservations
- Automatic Volume Unloading

Managing Tape Drives

This section explains how to mount and unmount volumes in a **tape drive**. A **volume** is a single unit of media, such as 8mm tape. 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. In the Manage page, click **Drives**.

   The Drives page appears. This page lists every **dataset file** and **dataset directory**. You can use this page to mount and unmount volumes.

2. Select a tape drive from the drives list.

The Oracle Secure Backup **Web tool** displays the names all tape drives that are attached to a **media server**. A tape drive can have one of the following 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.

3. 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 new 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.

4. From the **Mount and Unmount** options group, optionally choose one of the following 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**.

5. Click **Mount** to mount the volume.

The Oracle Secure Backup Web tool displays the tape drive name and **volume ID** in the status area.

6. 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 and Volume Labels" on page 1-11 for details about volumes and volume IDs

Managing Tape Libraries

This section explains how to view and control a **tape library** or **tape drive**.

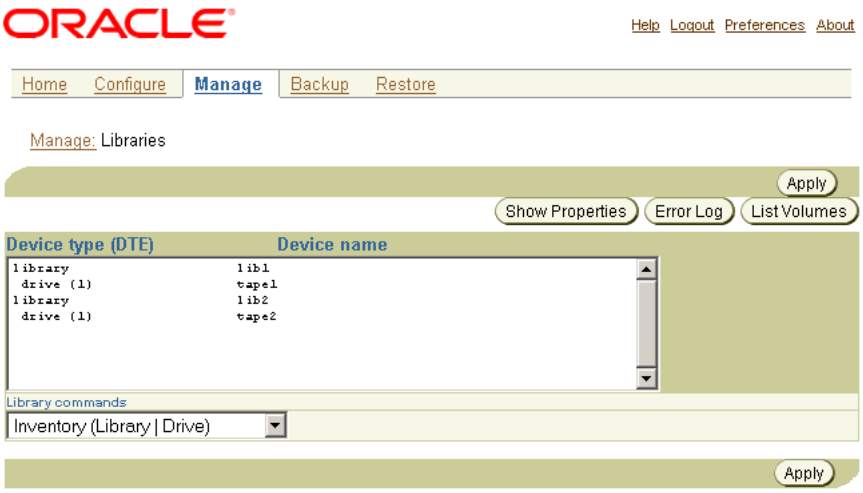
This section contains these topics:

Running Library Commands

To manage a **tape library** or **tape drive**:

1. In the Manage page, click **Libraries**.

   The Libraries page appears. 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.



2. In the Devices list, select a **tape library** or **tape drive**.
3. Choose one of the commands from the **Library commands** menu shown in Table 7–1. 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 a tape 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 7–1 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" on page 7-5	`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" on page 7-5	`importvol`
Export volume	Library or Drive	Moves one or more volumes to the import/export mechanism for removal from the library.	"Exporting a Volume" on page 7-6	`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" on page 7-6	`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" on page 7-7	`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" on page 7-7	`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" on page 7-8	`opendoor`
Close Door	Library	Closes the import/export door if the library. This command only works for libraries that support it.	"Closing a Door" on page 7-8	`closedoor`
Identify Volume	Drive	Loads selected volumes, reads their volume labels and returns the volumes to their original storage elements.	"Identifying a Volume" on page 7-8	`identifyvol`
Load Volume	Drive	Moves a volume from the indicated storage element to the selected drive.	"Loading a Volume" on page 7-9	`loadvol`
Unload Volume	Drive	Moves a tape from the selected drive to the storage element you specify.	"Unloading a Volume" on page 7-10	`unloadvol`
Label Volume	Drive	Loads selected volumes and physically labels them. Oracle Secure Backup updates its catalog and the inventory display	"Labeling a Volume" on page 7-10	`labelvol`
Unlabel Volume	Drive	Loads selected volumes and physically removes their Oracle Secure Backup volume labels and backup data.	"Unlabeling a Volume" on page 7-10	`unlabelvol`
Clean	Drive	Requests that a cleaning be performed on the selected tape drive.	"Cleaning a Tape Drive" on page 7-11	`clean`

Table 7–1 (Cont.) Library Commands

Menu Command	Applies to	Description	Section	obtool Command
Borrow	Drive	Borrows the selected drive.	"Borrowing a Tape Drive" on page 7-11	`borrowdev`
Return	Drive	Returns a currently borrowed drive.	"Returning a Tape Drive" on page 7-11	`returndev`
Reuse Volume	Drive	Loads selected volumes and relabels them so as to be reusable.	"Reusing a Volume" on page 7-12	`reusevol`

4. Click **Apply** to accept your selections.

   The Oracle Secure Backup **Web tool** displays a new 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:

1. In the Libraries page, select a tape library or **tape drive** in the Devices list.
2. From the **Library commands** list, select **Inventory (Library | Drive)**.
3. 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.
4. 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. In the Libraries page, select a tape library or **tape drive** in the Devices list.
2. From the **Library commands** list, select **Import Volume (Library | Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Options** group, select one of the following 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" on page 7-8. 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.

5. In the **IEE Range** field, enter a range of import/export elements containing the volumes to be imported.
6. Click **Apply**, **OK**, or **Cancel**.

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. In the Libraries page, select a tape library or **tape drive** in the Devices list.
2. From the **Library commands** list, select **Export Volume (Library | Drive)**.
3. Click **Apply** to accept your selection.
4. 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**.
5. 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. In the Libraries page, select a tape library or **tape drive** in the Devices list.
2. From the **Library commands** list, select **Insert Volume (Library | Drive)**.
3. Click **Apply** to accept your selection.
4. If you have inserted a volume with a known **volume ID** or **barcode**, then select one of the following 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.

     ---
5. In the **Storage element** field, enter the **storage element** number for the inserted volume.
6. Select one of the following 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 the cleaning tape has been used.

  – **Max uses**

    Enter the maximum number of times the cleaning tape can be used.

7. 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. In the Libraries page, select a tape library or **tape drive** in the Devices list.
2. From the **Library commands** list, select **Extract Volume (Library | Drive)**.
3. Click **Apply** to accept your selection.
4. 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 the following 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**.

5. 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. In the Libraries page, select a **tape library** or **tape drive** in the Devices list.

2. From the **Library commands** list, select **Move Volume (Library | Drive)**.
3. Click **Apply** to accept your selection.
4. 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 the following 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**.
5. In the **Element spec** field, enter the slot to which the volume should be moved. For example, enter **iee2**.
6. Click **Apply**, **OK**, or **Cancel**.

Opening a Door

This command opens the import/export door of s **tape library**.

To open the import/export door:

1. In the Libraries page, select a tape library in the Devices list.
2. From the **Library commands** list, select **Open Door (Library)**.
3. 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. In the Libraries page, select a tape library in the Devices list.
2. From the **Library commands** list, select **Close Door (Library)**.
3. 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. In the Libraries page, select a **tape drive** in the Devices list.
2. From the **Library commands** list, select the **Identify Volume (Drive)** option.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive to be used in the volume identification.

5. 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.

6. In the **Storage element range** field, enter the **storage element** range for the volumes to be identified. For example, enter **1-20**.

7. 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. In the Libraries page, select a tape drive in the Devices list.
2. From the **Library commands** list, select **Load Volume (Drive)**.
3. In the **Drive** list, select the tape drive to contain the loaded volume.
4. Click **Apply** to accept your selection.
5. 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 the following 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**.

6. From the **Load volume options** groups, optionally select one of the following:
   - **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 new 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 already loaded in the tape drive.

7. 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. In the Libraries page, select a **tape drive** in the Devices list.
2. From the **Library commands** list, select **Unload Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive that contains the loaded volume.
5. In the **Source element address** field, enter the element to which the volume should be moved. For example, enter **1**.
6. Click **Apply**, **OK**, or **Cancel**.

Labeling a Volume

This command loads selected volumes and writes a new **volume label** for each **volume**. This command erases all existing data on the selected volumes.

To label a volume:

1. In the Libraries page, select a **tape drive** in the Devices list.
2. From the **Library commands** list, select **Label Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive into which the volume should be loaded.
5. 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 unlabeling a volume.
6. Select the **Barcode** option and enter the barcode for the volume.
7. Enter a **storage element** element range in the **Storage element range** field. For example, enter **1-3**.
8. Click **Apply**, **OK**, or **Cancel**.

Unlabeling a Volume

This command loads selected volumes and physically unlabels them.

To unlabel a **volume**:

1. In the Libraries page, select a **tape drive** in the Devices list.
2. From the **Library commands** list, select **Unlabel Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive into which the volume should be loaded.

5. 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.
6. In the **Storage element range** field, enter a **storage element** range. For example, enter **1-3**.
7. 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. In the Libraries page, select a tape drive in the Devices list.
2. From the **Library commands** list, select **Clean (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive into which the cleaning tape should be loaded.
5. 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.
6. In the **Source element address** field, enter an element address of a **storage element** containing a cleaning tape.
7. 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` right.

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. In the Libraries page, select a tape drive in the Devices list.
2. From the **Library commands** list, select **Borrow (Drive)**.
3. In the **Drive** list, select the tape drive to be borrowed.
4. 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. In the Libraries page, select a tape drive in the Devices list.
2. From the **Library commands** list, select **Return Device (Drive)**.
3. In the **Drive** list, select the tape drive to be returned.

4. Click **Apply**, **OK**, or **Cancel**.

Reusing a Volume

This command loads selected volumes and deletes every **backup image** 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 unlabeling it, but reusing directs Oracle Secure Backup to preserve the existing **volume label**.

To reuse a volume:

1. In the Libraries page, select a **tape drive** in the Devices list.
2. From the **Library commands** list, select **Reuse (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the tape drive to be returned.
5. In the **Storage element range** field, enter a **storage element** range containing the volumes to be reused.
6. Click **Apply**, **OK**, or **Cancel**.

Displaying Library Properties

This section explains how to display properties for a **tape library**.

To view tape library properties:

1. In the Libraries page, select a tape library in the Devices list.
2. Click **Show Properties**.

   The Oracle Secure Backup **Web tool** displays a page with the properties for the tape library you selected.
3. Click **Close** to return to the Libraries page.

Displaying Tape Drive Properties

This section explains how to display properties for a **tape drive**.

To view tape drive properties:

1. In the Libraries page, select a tape drive in the Devices list.
2. Click **Show Properties**.

   The Oracle Secure Backup **Web tool** displays a page with the properties for the tape drive you selected.
3. 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. In the Libraries page, select a tape library in the Devices list.
2. Click **List Volumes**.

   The Oracle Secure Backup **Web tool** displays a page with the volumes for the tape library you selected.

3. Click **Close** to return to the Libraries page.

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. In the Libraries page, select a tape library or tape drive in the Devices list.
2. Select a tape library or tape drive from the **Library Management** list.
3. 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.
4. Optionally, select **Since (date)** and specify a date range for specific error messages.
5. Optionally, select **Read device dump file** and enter the filename and path of the file that you want to read.
6. Choose one of the following:
   - Click **Apply** if you have either specified a date range or entered a filename.
   - Click **Clear** to eliminate error history. New error messages will display from the time of the clear.
   - Click **Close** to return to the Libraries page.

Managing Device Reservations

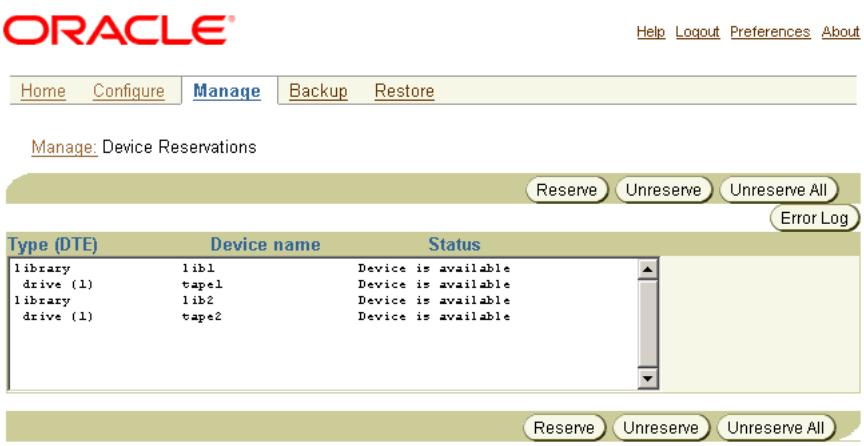
In the normal course of operations, Oracle Secure Backup temporarily assigns exclusive use of shared resources to its processes and jobs. It does so using a built-in resource reservation system managed by the **service daemon** of the **administrative server**.

You might encounter certain situations in which you desire 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. In 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.



2. To reserve a **tape library** or **tape 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.

3. 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.

4. 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.

Automatic Volume Unloading

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 **obtool** `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 on 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, a success message is written to the observiced 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 an error message is written to the observiced log.

8

Performing Maintenance

This chapter describes how to perform maintenance tasks with Oracle Secure Backup.

This chapter contains these sections:

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.

This section contains these topics:

Displaying the Jobs Page

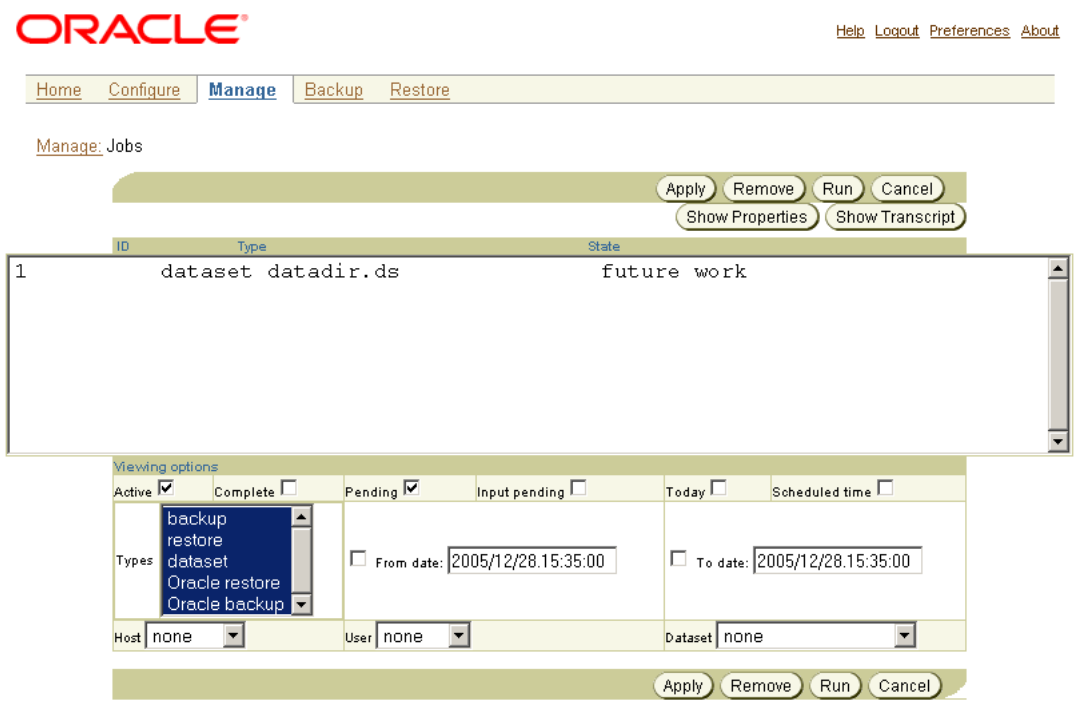
In the Manage page, click **Jobs** to display the page shown in Figure 8–1. You can perform all job-related tasks in this page or in pages to which it provides links.

The central text box contains the following information for each **backup 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 8–1 Jobs Page



Note that you can also monitor and manage jobs from the Oracle Secure Backup Home page, which is shown in Figure 8–2. The Home page contains sections that show failed, active, pending, and completed jobs.

Figure 8–2 Home Page

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.

To display jobs:

1. In the Jobs page, 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.
   - **Complete**

     Select this option to display the status of completed jobs, whether they succeeded or not.
   - **Pending**

     Select this option if you want to view the status of jobs that are pending, but not presently running.
   - **Input pending**

     Select this option to view the status of jobs that are running and requesting input now.
   - **Today**

     Select this option to display the status of each **backup job** scheduled to run today.
   - **Scheduled time**

     Select this option to display jobs scheduled within a time range that you select as follows:
     - Check 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.
     - Check 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, 2005/5/19.12:43.
2. In the **Types** box, select one or more job types.
3. In the **Host** list, optionally select a host to limit the jobs displayed to those pertinent to a specific host.
4. In the **User** list, optionally select an **Oracle Secure Backup user** to limit the jobs displayed to those instantiated by the specified user.
5. In the **Dataset** list, select a **dataset file** to limit the jobs displayed to a particular dataset file or directory. See "File System Backup Types" on page 5-2 to learn about datasets.
6. Click **Apply** to accept your selections.

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. In the Jobs page, select a job from the central text box.
2. Click the **Show Properties** button.

   The Job Properties page appears.
3. 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 on Oracle Secure Backup **rights**

To display a job transcript:

1. In the Jobs page, select a job and click **Show Transcript**.

   The Oracle Secure Backup **Web tool** displays a page with the transcript.
2. Scroll down the page to view more information.

   At the end of the page, you can modify the transcript viewing criteria.
3. 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.
4. 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.
5. Optionally, check **Show line numbers** to prefix each line with its message number.
6. Optionally, select one of the following 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 above 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 above the value you selected.

7. In the **Page refresh (in seconds)** box, optionally enter a number of seconds. The default is 60 seconds.
8. Choose one of the following:
   - 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 8–1.

Table 8–1 Job Transcript Backup Statistics

Statistic	Description
`status`	Overall status of backup. See samples/obexit.h in your Oracle Secure Backup home directory for more information on status codes
`devices`	Name(s) of tape drive(s) used during the backup
`devices`	Number of tape drives 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
`encryption`	Encryption used. Values are `off`, `on`, `transient`, `forcedoff`, or `RMAN`. If the value displayed is `on` or `transient`, then the algorithm used is also shown as `aes128`, `aes192`, or `aes256`.
`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 start_time. It might differ if an archive is being read, in which case the backup_time 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`	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
`mount_points_skipped`	Number of file system entries that were skipped because they were mount points, either local or remote, and obtar 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

Table 8–1 (Cont.) Job Transcript Backup Statistics

Statistic	Description
`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.
`filesys_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 `open()` operation and ending with the `close()` operation
`dev_iorate`	Rate at which data was written to tape
`wrt_iosecs`	Total seconds during which data was being written to tape. This excludes time spent on such activities as positioning the tape and reading labels.
`wrt_iorate`	Rate at which data was written to tape during write operations
`physical_blks_written`	Number of physical blocks written, as reported by the tape drive
`write_errors`	Number of physical blocks that encountered unrecoverable write errors and therefore had to be rewritten to tape
`physical_blks_read`	Number of physical blocks read, as reported by the tape drive
`read_errors`	Number of physical blocks that encountered unrecoverable read errors and therefore had to be reread from tape
`error_rate`	The sum of read errors and write errors divided by the sum of total blocks read and total blocks written
`path` *`path_name`*	Final status of the backup of the path *path_name*. 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" on page 8-7, you can cancel a job and retain its history and transcript.

To remove a job:

1. In the Jobs page, select a job from the central text box.
2. Click the **Remove** button.

   The Oracle Secure Backup **Web tool** prompts you to confirm the job removal.
3. 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 **tape device**. 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 on 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. In the Jobs page, select a job from the central text box.
2. Click **Run**.
3. In the **Devices** list, 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.
4. Optionally select one of the following 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 new 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.
5. Choose 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. In the Jobs page, select a job from the central text box.
2. Click the **Cancel** button.

Browsing 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:

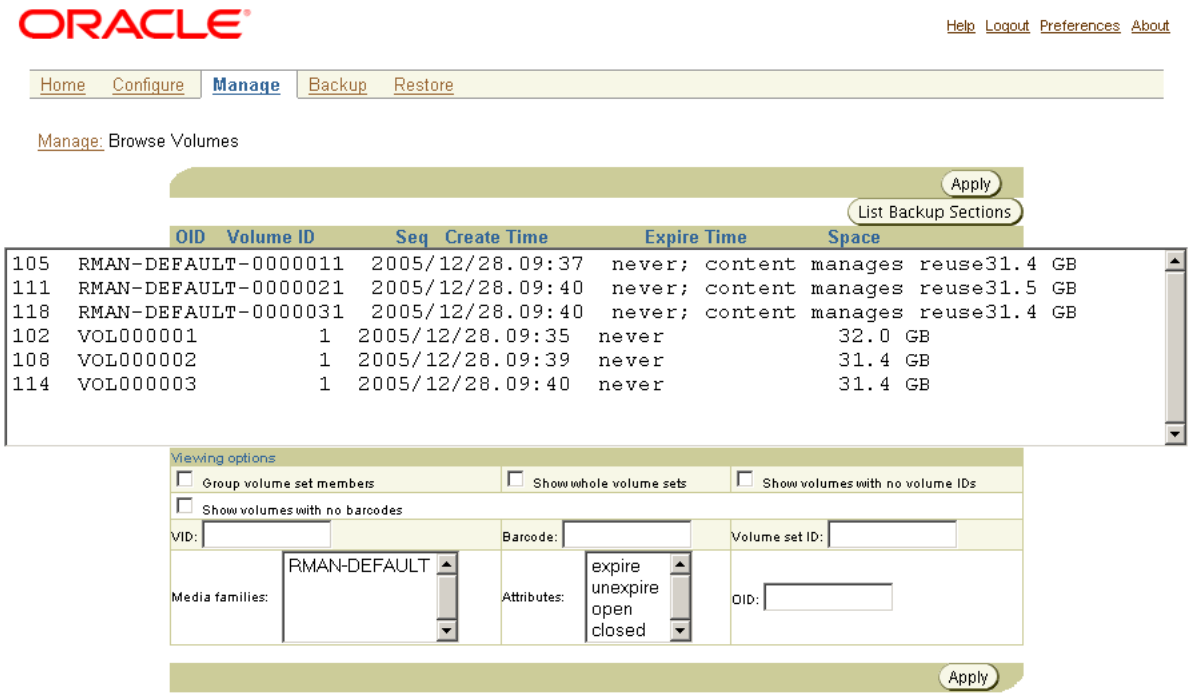
- Displaying the Browse Volumes Page
- Displaying Volumes
- Displaying Backup Sections

Displaying the Browse Volumes Page

In the Manage page, click **Volumes** to display the page shown in Figure 8–3. This page lists every **volume** in the volume **catalog**.

Note: To list volumes in a specified **tape library**, go to the Libraries page described in "Running Library Commands" on page 7-3 and click **List Volumes**.

Figure 8–3 Browse Volumes Page



See Also: *Oracle Secure Backup Reference* to learn about the `lsvol` command in **obtool**

Displaying Volumes

This section describes how to display information about Oracle Secure Backup volumes and media families.

By default, the Browse Volumes page displays the attributes of each volume in the **catalog**.

To restrict display of **volume** and **media family** information:

1. In the Viewing Options section of the Browse Volumes page, optionally check one or more of the following volume display options:
   - **Group volume set members**

     Check this box to group volumes in the same **volume set**.
   - **Show whole volume sets**

     Check this box to display all volume set members for each volume displayed.
   - **Show volumes with no volume IDs**

     Check this box to display volumes with no volume IDs.
   - **Show volumes with no barcodes**

     Check this box to display volumes with no tags.
2. In the Viewing Options section of the Browse Volumes page, optionally enter text in the following boxes to restrict output:
   - **VID**

     Enter a **volume ID** in this box to restrict output to the specified VID. Separate multiple volume IDs with commas.
   - **Barcode**

     Enter a **barcode** in this box to restrict output to the specified barcode. Separate multiple barcodes with commas.
   - **Volume set ID**

     Enter a volume set ID in this box to restrict output to the specified volume set. The set ID represents the volume ID of the first volume in the volume set. Separate multiple volume set IDs with commas.
3. In the Viewing Options section of the Browse Volumes page, optionally select options from the following lists:
   - **Media families**

     Select one or more media families in this list to restrict output to volumes in the specified families.
   - **Attributes**

     Select one of the attributes in this list to restrict output to volumes in the specified families. Valid values for this placeholder are the following:
     - **open**, which means that the volume is open for writing
     - **closed**, which means that the volume is closed for writing
     - **expired**, which means that the volume is expired (see "Volume Expiration Policies" on page 1-17)
     - **unexpired**, which means that the volume is not expired

- **OID**

  Enter a volume catalog identifier in this box to restrict output to the specified volume. Separate multiple volume OIDs with commas.

4. Click **Apply** to accept your selections.

Displaying Backup Sections

This section describes how to display **backup section** information on a **volume**.

To display the backup sections on a value:

1. In the Browse Volumes page, select a volume from the main window.
2. Click **List Backup Sections**.

   The List Sections property page appears. This page displays the file number, section number, and **volume ID** for every backup section on the volume.
3. Click **Close** after you have finished reviewing the information.

Managing Backup Images

The backup of an Oracle database performed with RMAN results in a backup set. The physical files are called backup pieces. When you use Oracle Secure Backup to store database backups on tape, each **backup piece** is created as one **backup image**.

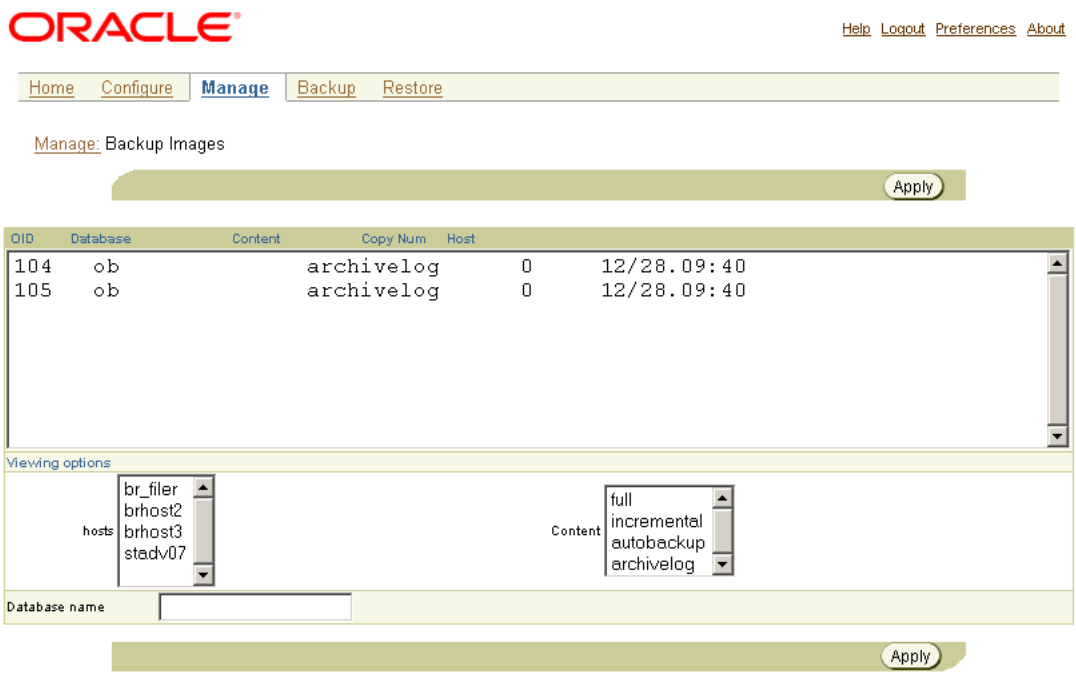
This section includes these topics:

- Displaying the Backup Images Page
- Displaying Backup Images

Displaying the Backup Images Page

In the Manage page, click **Backup Images** to display the page shown in Figure 8–4. This page lists the backup images generated by RMAN.

Figure 8–4 Backup Images Page



See Also: *Oracle Secure Backup Reference* to learn about the `lspiece` command in **obtool**

Displaying Backup Images

This section describes how to display information about RMAN backup images. By default, the main box in the Backup Images page displays each **backup image** recorded in the **catalog**.

To restrict display of backup images:

1. In the Viewing Options section of the Backup Images page, you can restrict the display as follows:
   - **hosts**

     Select one or more hosts in the list to show only the backup images of databases on the selected hosts.
   - **Content**

     Select a content type to restrict the display to **full**, **incremental**, **autobackup**, or **archivelog**.
   - **Database name**

     Enter a database name to restrict the display to backups of the specified database.
2. Click **Apply** to accept your selections.

Managing Backup Sections

A **backup section** is the part of a **backup image** that fits on one tape. If a single backup image spans multiple tapes, then the portion of the image on each tape is a separate section.

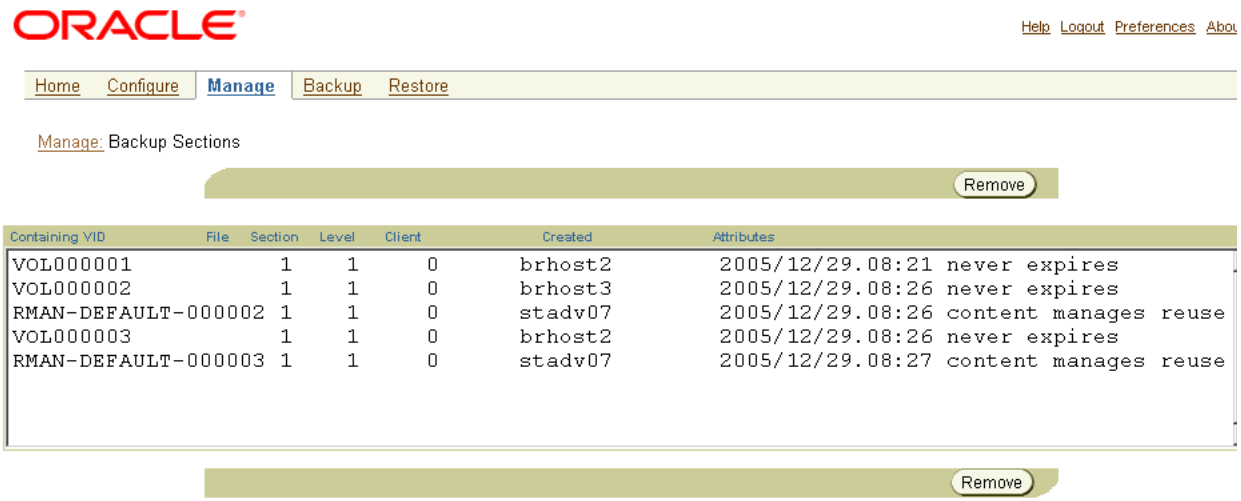
This section includes these topics:

- Displaying the Backup Sections Page
- Updating the Catalog After Deletion of Backup Sections

Displaying the Backup Sections Page

In the Manage page, click **Backup Sections** to display the page shown in Figure 8–5. This page lists every **backup section** recorded in the **catalog**.

Figure 8–5 Backup Sections Page



See Also: *Oracle Secure Backup Reference* to learn about the `lssection` command in **obtool**

Updating the Catalog After Deletion of Backup Sections

This section describes how to update the Oracle Secure Backup to reflect backup sections that have been deleted. This action is meaningful only for a content-managed **volume**.

When you click **Remove**, 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 click **Remove** 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.

To update the catalog concerning deleted backup sections:

1. In the main box of the Backup Sections page, select the backup sections that have been deleted.
2. Click **Remove**.

   A confirmation page appears.

3. Click **Yes** to confirm the deletion.

   The Backup Sections page appears. The deleted backup section no longer appears in the main box.

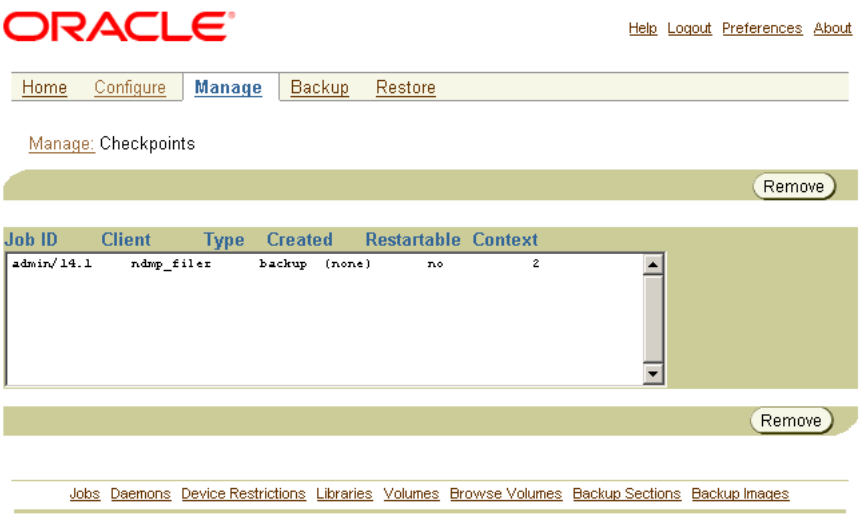
Managing Checkpoints

You can restart some **filer** backups from a mid-point if they fail before completing. A checkpoint is a collection of state information that describes a specific mid-point in a **backup job** and how to restart from it. Some information for each checkpoint resides on the Oracle Secure Backup **administrative server**; the remainder resides on the **client**.

Displaying the Checkpoints Page

In the Manage page, click **Checkpoints** to display the page shown in Figure 8–6. This page displays all checkpoints for hosts in the **administrative domain**.

Figure 8–6 Manage Checkpoints Page



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. In the main box, select the job whose checkpoint you want to remove.

2. Click **Remove**.

   A confirmation page appears.

3. 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: "Oracle Secure Backup Daemons" on page 1-3

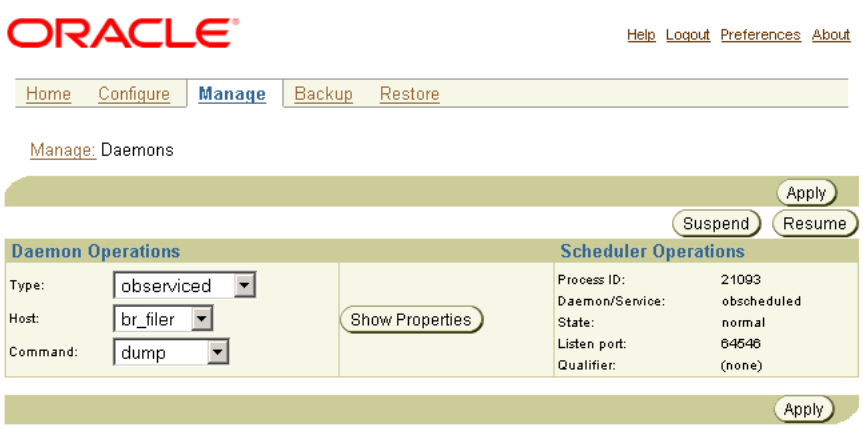
This section contains these topics:

- Displaying the Daemons Page
- Performing Daemon Operations
- Viewing Daemon Properties
- Suspending and Resuming Job Dispatching

Displaying the Daemons Page

In the Manage page, click **Daemons** to display the page shown in Figure 8–7. This page enables you to manage the Oracle Secure Backup **daemons**.

Figure 8–7 Daemons Page



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: "Oracle Secure Backup Daemons" on page 1-3

To send a command to a daemon:

1. In the **Type** list, select the daemon that you want to control.
2. In the **Host** list, select the host on which the daemon runs.
3. In the **Command** list, select one of the following 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.
4. 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:** "Oracle Secure Backup Daemons" on page 1-3

To view daemon properties:

1. In the **Type** list, select the daemon that you want to control.
2. In the **Host** list, select the host on which the daemon runs.
3. 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 will be allowed to complete, but the **scheduler** will start no new jobs.

The scheduler resumes job dispatching for suspended jobs when you click **Resume** or restart Oracle Secure Backup on the **administrative server**.

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 already 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:

9

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 both optional, and they are independent of one another. You can enable both of them simultaneously, either of them by itself, or neither. You can also enable either of them for some volumes, leaving the movement and/or duplication of other volumes unmanaged by Oracle Secure Backup.

This chapter contains these sections:

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 New Vaulting Environment" on page 9-5.

This section contains these topics:

- Volume Duplication Schedules
- Volume Duplication Jobs
- Volume Duplication Windows

Locations

The Oracle Secure Backup vaulting feature enables you to organize your volumes as they move from location to location in your environment. Locations are physical places where a volume can reside. Oracle Secure Backup recognizes two location types:

- Active locations

  Active locations are 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 on 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 can be used for volumes at the end of their rotation cycle. You can create as many additional storage locations as you want. Storage location examples include fireproof closets, off-site data warehouses and third-party storage vendors such as Iron Mountain.

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 will move to is a storage closet.

  Oracle Secure Backup will know about the storage closet, because you will have configured it following the procedure in "Adding Locations" on page 9-6.

- 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 will then be moved to the media recycle bin.

Location Scans

After you have created both active and storage locations, you can specify the days and times that Oracle Secure Backup does location scans. During a location 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 location scan can scan one or more locations.

Setting up one or more location scans is a necessary part of creating a vaulting environment. If there are no location scans, then Oracle Secure Backup creates no media movement jobs. If there are no media movement jobs, then rotation policies are not enforced.

You want to schedule the location scans to finish shortly before the times you have set aside for media movement jobs, because the media movement jobs are based on volume events and durations at the time of the scans. If there is a long lag between location scans and media movement jobs, then media movement will be based on stale information.

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 location scans are not run automatically. They are created in a pending state and require action by an operator to complete.

Reports

Oracle Secure Backup produces the following reports to assist you in the movement of volumes from location to location:

- 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 will be 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.

- Distribution report

  Oracle Secure Backup creates a distribution report when it creates a media movement job. It lists all volumes being sent to a particular location as the result of a media movement job. For each volume, it shows the number of the associated

media movement job and the customer ID (if any) that was assigned to the next location. You can think of it as a packing list to be included in the shipment of volumes to a location.

- Pick report

  The pick report lists all volumes to be picked for distribution to another location. For each volume, it shows the number of the associated media movement job but not the customer ID 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.

- 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 will appear in the exception report for that tape library.

The Vaulting Process

After you have set up storage locations, rotation policies, and location scan schedules, managing the movement of your volumes through their respective life cycles becomes routine. At intervals defined by the location scan schedule, Oracle Secure Backup 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, and creates pick and distribution reports to facilitate the movement of volumes from old to new locations. The only operator involvement is running the media movement jobs, extracting the volumes from their present active or storage locations with the help of pick reports, packing them with their distribution reports, and transporting them to their new locations.

If you want a greater margin of safety for your backup data, or if you want to use different media families for on-site backups and off-site storage, then you can combine the Oracle Secure Backup vaulting process with automatic volume duplication.

About Volume Duplication

Volume duplication can safeguard critical data. Having multiple copies of a volume to store in different geographic locations, for example, protects against data loss caused by 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 in compressed format, then the duplicate volume is also in compressed format. The volume label for the original volume differs from the volume label for the duplicate volume, because volume labels contain the volume **Universal Unique Identifier (UUID)**, which is unique for each volume.

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.

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.

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 location 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.

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.

You can also run on-demand volume duplication jobs with the obtool `dupvol` command.

> **See Also:** *Oracle Secure Backup Reference* for complete `dupvol` syntax and semantics

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.

Setting Up a New Vaulting Environment

This section contains step-by-step instructions for configuring a new vaulting environment.

This section contains these topics:

- Adding Locations
- Adding Rotation Policies

- Associating Rotation Policies with Media Families
- Adding a Location Scan Schedule
- Running Media Movement Jobs
- Viewing Location Reports
- Recalling a Volume
- Viewing Job 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

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 Oracle Secure Backup **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 using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. 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. It also lists a storage location called Media_Recycle_Bin generated by Oracle Secure Backup.

3. Click **Add**.

   The Configure: Locations > New Locations page appears.

4. Enter a name for the storage location in the **Location** field.

   This is the name you will use for this storage location when you create rotation policies. This name will also appear in the reports that are generated in the vaulting process.

   See Also:

   - "Adding Rotation Policies" on page 9-8
   - "Viewing Location Reports" on page 9-21
   - "Viewing Job Reports" on page 9-25

   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.

5. 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 will appear in all distribution reports created for media movement jobs for this location, it will accompany all volumes that are moved at the location.

   This step is optional.

6. 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 that it requires 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 that are 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 Job Reports" on page 9-25 for more information on pick and distribution reports

7. 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. An e-mail system must be operational on the **administrative server** for this feature to operate. Separate multiple entries with commas.

8. 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 Oracle Secure Backup administrative domain. This setting can be used to determine whether to fail an RMAN-initiated restore request that requires use of tape volumes that cannot be supplied within the specified resource wait time period. If there are duplicate volumes, then this value is used to determine which of the duplicate volume has the shortest recall time. That volume is used for the restore operation.

9. Enter a description of the storage site or other information in the **Comments** field.

10. Click **OK**.

    The Configure: Locations page displays a success message, and your new 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. It 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 be constrained or unconstrained. A constrained rotation policy names a specific **tape drive** or **tape library** where volumes controlled by the policy begin their life cycle. A backup will adhere to the constraints of this policy. The backup will use only the resources defined by this constraint. It does not apply to volumes that begin their life cycle in any other active location. An unconstrained rotation policy specifies a wild card (*) as its first location. It can apply to volumes that begin their life cycle at any active location.

To add a rotation policy with the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. 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 will be empty because Oracle Secure Backup does not automatically generate any rotation policies.

3. Click **Add**.

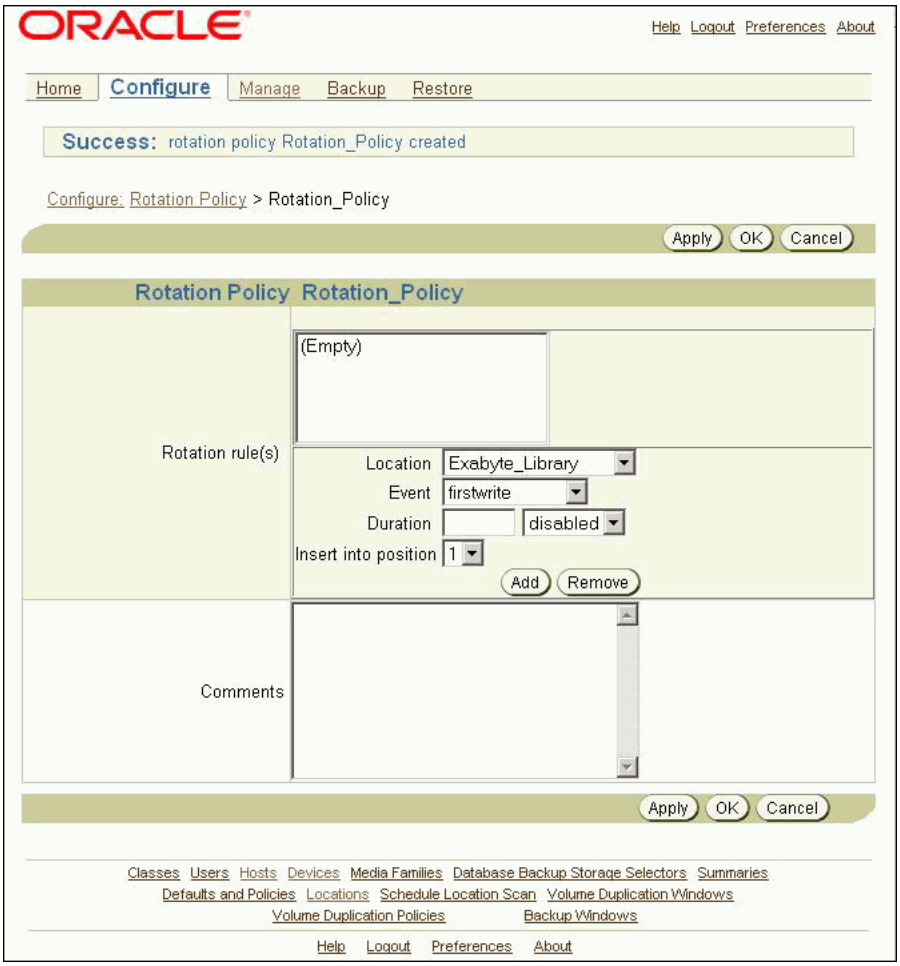
   The Configure: Rotation Policies > New Rotation Policy page appears.

4. 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 new rotation policy was created successfully.



5. Although your new 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 of time 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 6.

---

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.

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 new rotation rule appears in the Rotation rule(s) field.

6. 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. The next location will default to the Media_Recycle_Bin. Specifying additional rotation rules enables you to 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 5. 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. This event is applicable only to volumes with a **time-managed expiration policy**.

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 new rotation rule appears in the Rotation rule(s) field.

7. Add a buffer location rotation rule.

   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 are the final stops in the media life cycle. They can be specified only as the final location in a rotation policy.

   Buffer locations do not have durations. Volumes in buffer locations remain there until they are inserted into a tape device to begin a new 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.

8. When you are finished adding rotation rules, click **OK**.

   The Configure: Rotation Policies page appears with your new rotation policy in the Rotation Policies list.

Associating Rotation Policies with Media Families

A volume is a 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 that media 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 that media family will 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 any restrictions on the choice of drives within a library. To restrict backups to particular drives within a library, you must configure device restrictions for the schedule or backup. Note, however, that Oracle Secure Backup does not permit configuration of device restrictions that can conflict with a constrained rotation policy.

Suppose for example, that you use a constrained rotation policy to restrict media family mymf to tape library qualstar1. This means that 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.
```

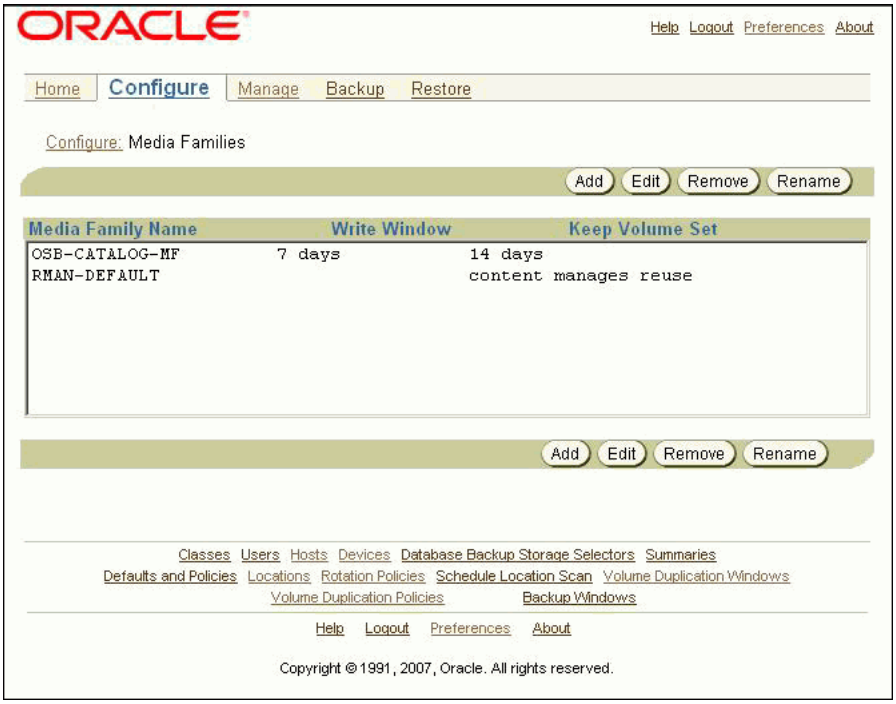
To associate a rotation policy with a media family using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

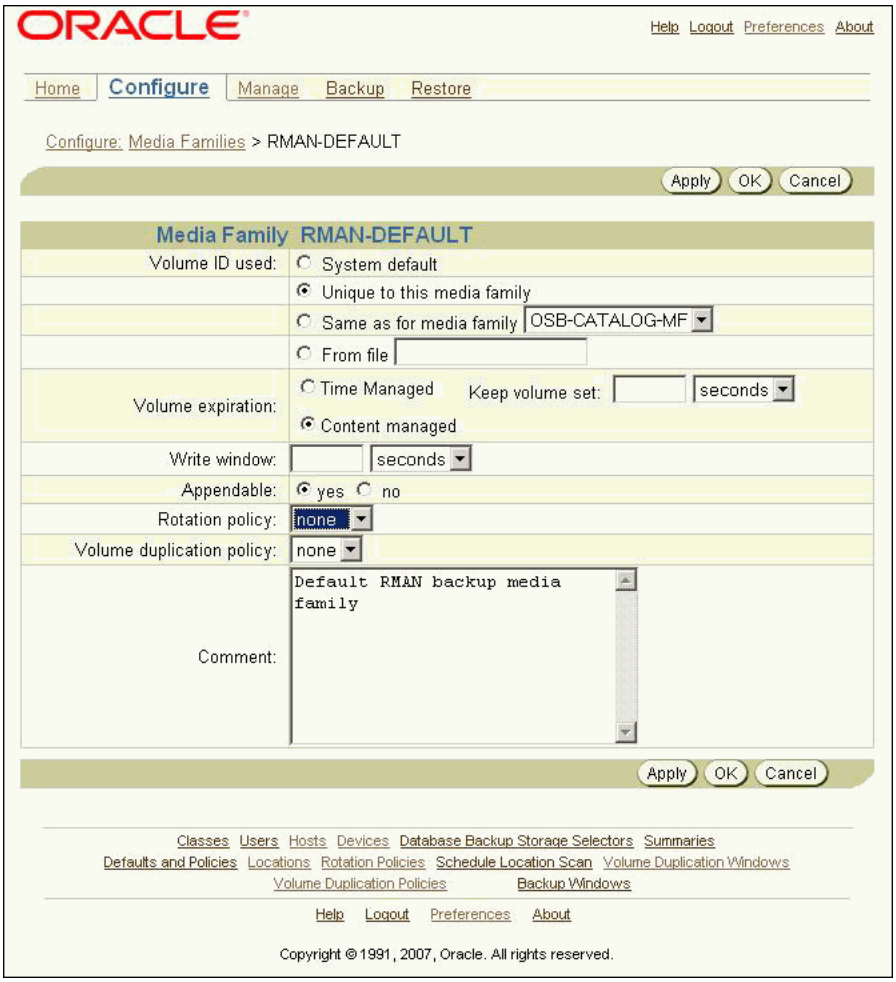
2. In the Basic section, click **Media Families**.

   The Configure: Media Families page appears.



3. Select the media family you want to associate with a rotation policy and click **Edit**.

   The Configure: Media Families > *family_name* page appears.



4. Select a rotation policy from the **Rotation policy** list and click **OK**.

   The Configure: Media Families page displays a success message.

Adding a Location Scan Schedule

During a location 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.

See Also: "Running Volume Duplication Jobs" on page 9-34

If you use a rotation policy, then you must create either one location scan schedule for the entire administrative domain or individual location scan schedules for each location in the rotation policy. Without the location scan, Oracle Secure Backup cannot select eligible volumes to be moved.

To schedule a location scan using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

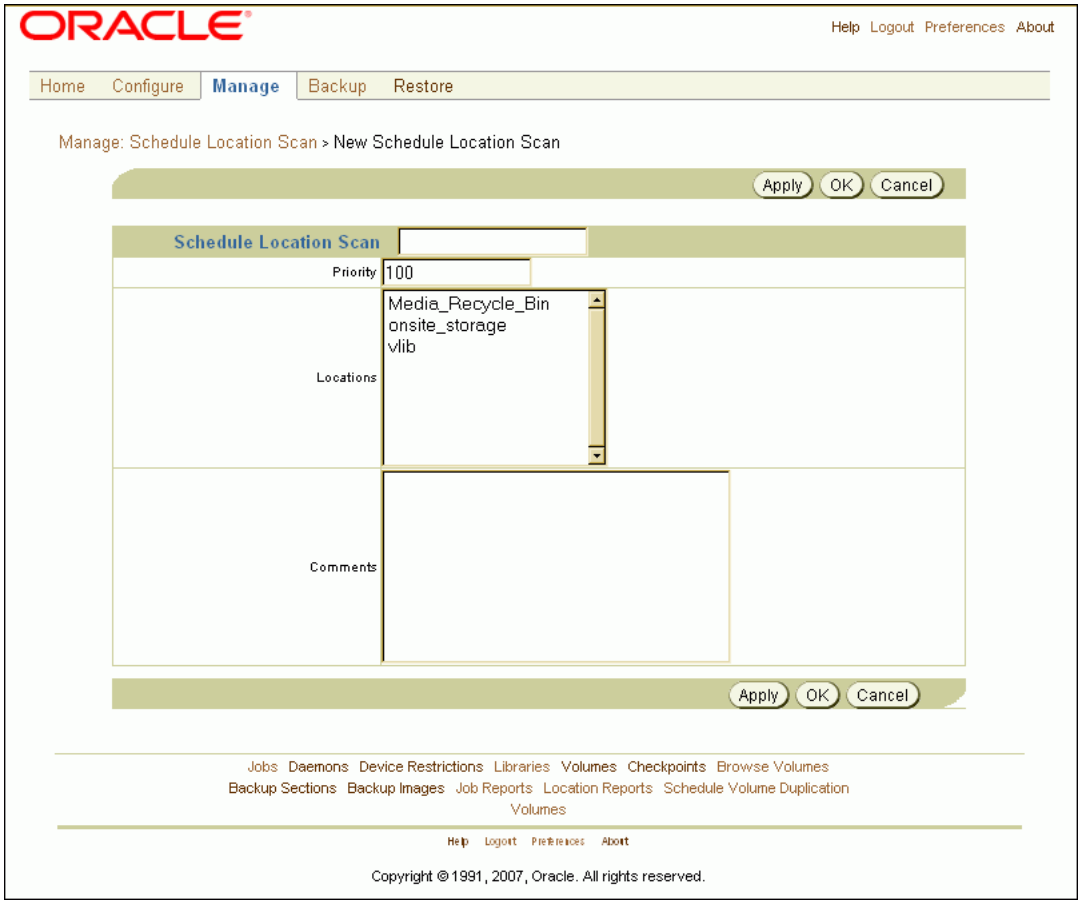
   The Manage page appears.

2. In the Media Life Cycle section, click **Schedule Location Scan**.

   The Manage: Schedule Location Scan page appears.

3. Click **Add**.

   The Manage: Schedule Location Scan > New Schedule Location Scan page appears.



4. Enter a name for the location scan schedule in the **Schedule Location 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.

5. 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.

6. Select at least one **location** in the **Locations** list.

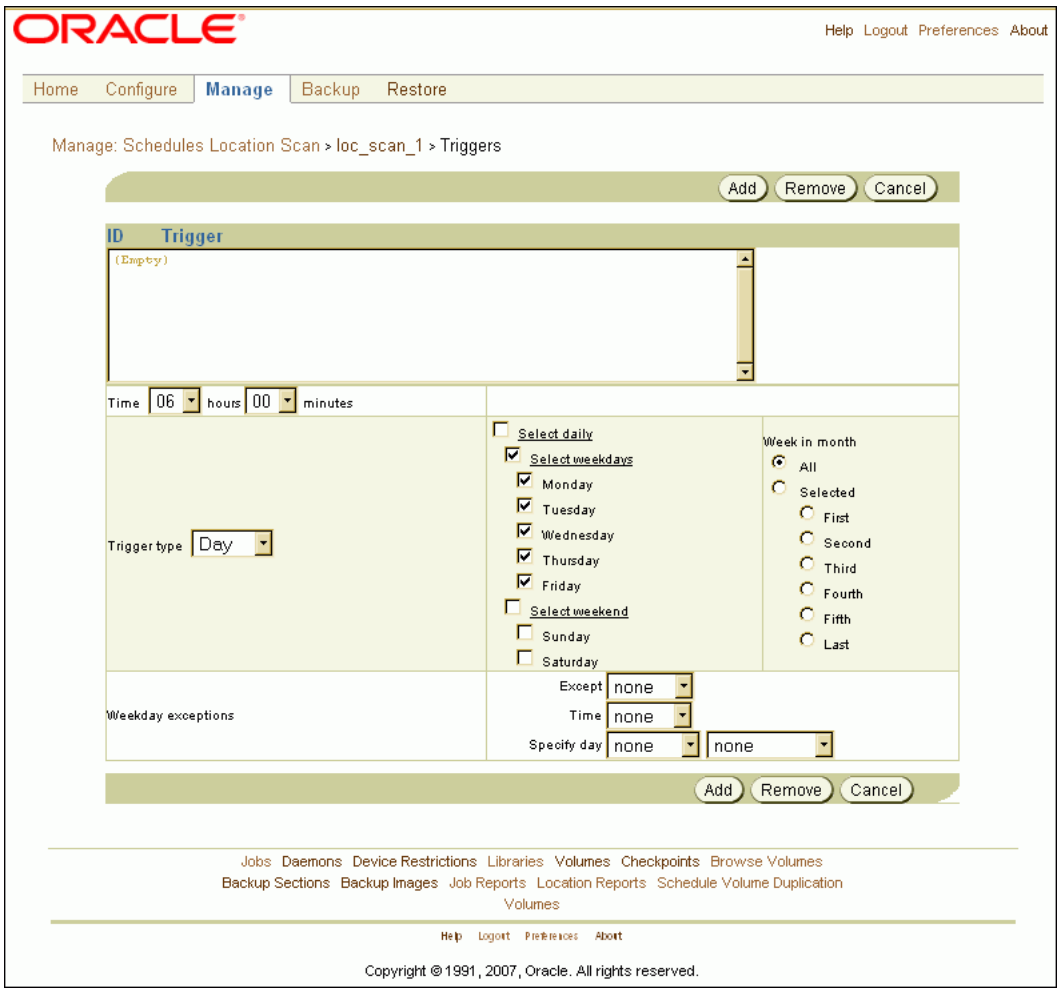
   You can use control-click to select more than one location or shift-click to select a range of locations.

7. Click **Apply**.

The Manage: Schedule Location Scan > *schedule_name* page appears.

8. Click **Triggers**.

   The Manage: Schedule Location Scan > *schedule_name* > Triggers page appears.



9. In the Time section, select a **trigger** time from the **hours** and **minutes** lists.
10. Select a trigger type from the **Trigger type** list.
11. If you selected trigger type **Day**, then do the following:
    a. Select the days you want the location scan to run:
       - **Select daily**

         This option produces a daily location scan, seven days a week.
       - **Select weekdays**

         This option produces a daily location scan, Monday through Friday.
       - **Select weekend**

         This option produces a location scan only on Saturday and Sunday.
       - Select one or more days of the week
    b. Select the week in the month you want the location scan to run.

       The default is all weeks.

c. In the Weekday exceptions section, you can specify days you do not want the location 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.

12. If you selected trigger type **Month**, then select an option in the **Day in month** section.
13. Click **Add**.
14. If you want to add another trigger, then go back to step 9.

    When you are done adding triggers, click **Schedule Location Scan** in the breadcrumbs at the top of the page.

    The Manage: Schedule Location Scans page appears with the new location scan schedule in the list of schedules.

Running Media Movement Jobs

Vaulting in a typical large organization could be organized something like this: 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. For each scheduled media movement job that appears in the list, the backup operator prints any reports needed to accompany the volumes that are to be moved. Pick and distribution reports are created for every media movement job.

The backup operator runs the media movement jobs and removes ejected volumes from the containing libraries. The pick report can be used to verify the volumes that are ejected. Ejected volumes are packed for transport, and a copy of the distribution report should be included with the volumes. The ejection type for the library determines what the operator must actually do to eject the volumes.

> **See Also:** "Ejection Type" on page 9-20

Volumes that are scheduled to return to the local data center from storage locations are listed on a distribution report that is provided to storage location operators, who might be off-site storage vendors. Returned volumes are placed directly into a tape library or into some buffer location until they are needed to restock a tape library. The media movement job created for returning volumes should be run only after the volumes have been received and verified.

At smaller sites the Oracle Secure Backup administrator typically performs all of the preceding tasks.

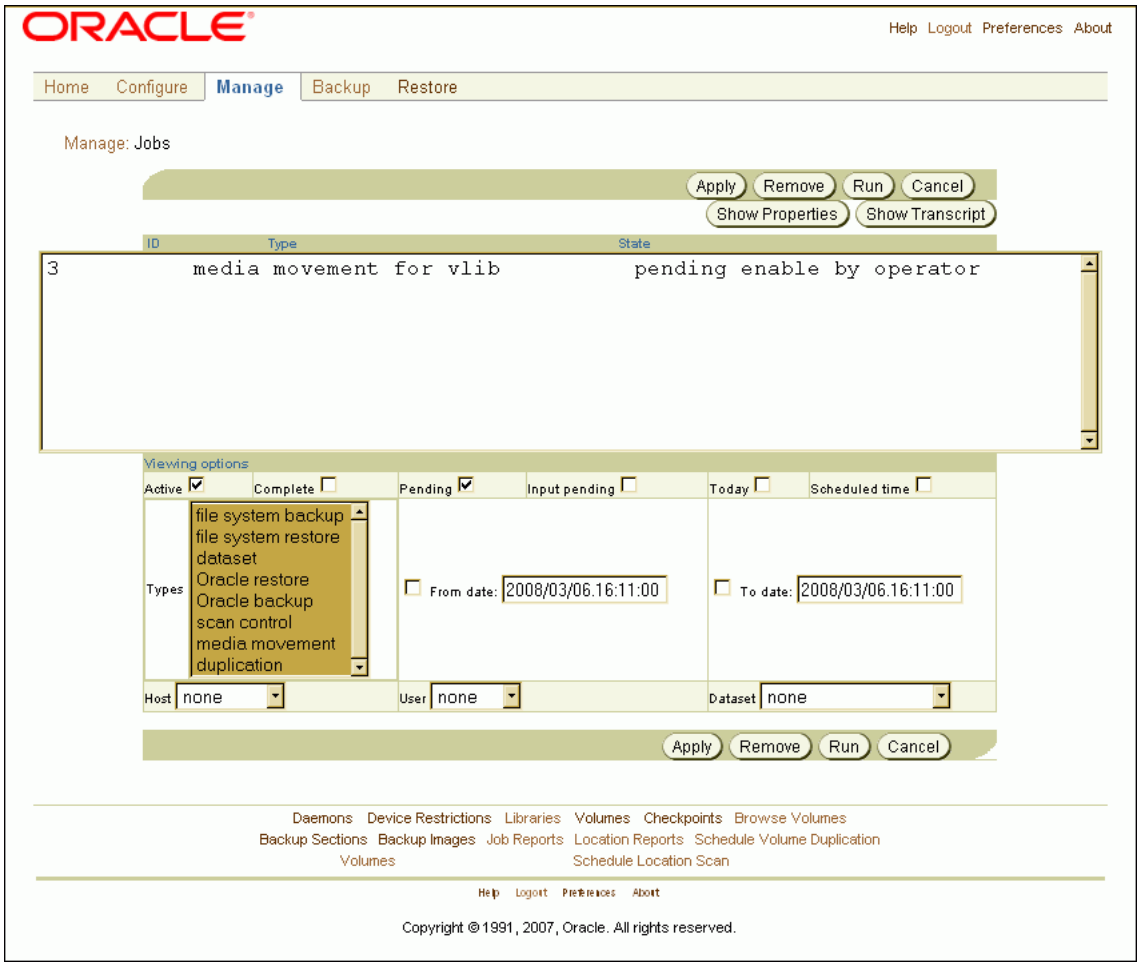
> **See Also:** "Viewing Job Reports" on page 9-25 for more information on distribution and pick reports

To run a media movement job using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.
2. In the Maintenance section, click **Jobs**.

   The Manage: Jobs page appears.



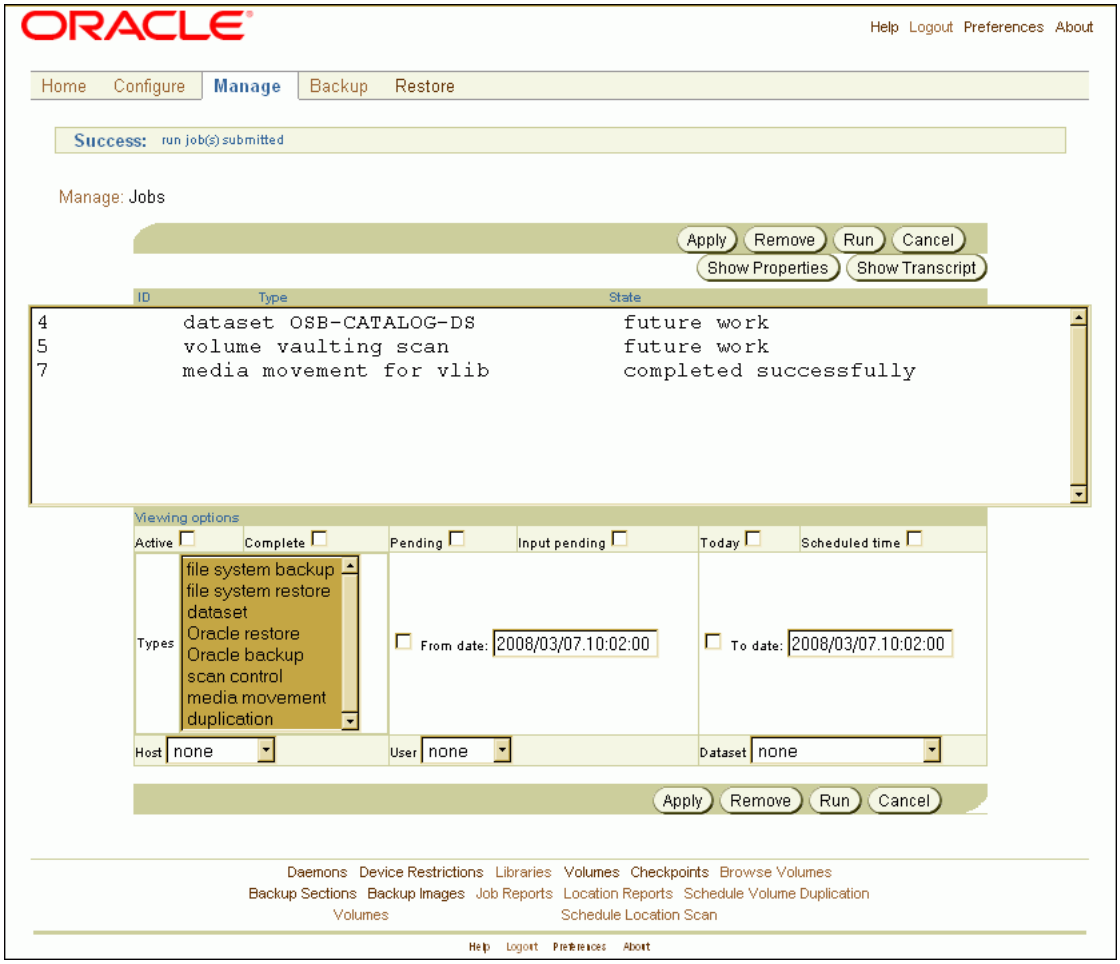
3. Select a media movement job and click **Run**.

   A new page appears.

4. Select the **Now** and **Media movement** options.

5. Leave the Devices list set to **none**.
6. 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.



7. 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
```

   To provide operator assistance:

   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 and click **Apply**.

Ejection Type

The need for operator assistance in a media movement job depends in part on the ejection type you specified when configuring a tape library for use with Oracle Secure Backup. The options are:

- Automatic

  Whenever a volume becomes eligible to be ejected from the tape library, Oracle Secure Backup moves that volume to an export element and notifies the backup operator that it is available there. If no export elements are available, then Oracle Secure Backup requests operator assistance.

- On demand

  Whenever a volume becomes eligible to be ejected from the tape library, Oracle Secure Backup marks the volume to that effect. A media movement job will then wait for the operator to reply to the job. The operator replies to the job through the job transcript. When the operator replies to the job to continue, Oracle Secure Backup ejects all such volumes through export elements.

- Manual

  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 tape library has no import/export slots.

> **See Also:** *Oracle Secure Backup Installation and Configuration Guide* for more information on configuring a tape library for use with Oracle Secure Backup

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 non-zero, and if the number of writable volumes in that tape library has fallen below 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 location scan job transcript that volumes have been moved early, as shown in the following example:

```
ob> catxcr -l0 1
2007/09/05.20:42:44 ____________________________________________________________
2007/09/05.20:42:44
2007/09/05.20:42:44 Transcript for job 1 running on stacr12
2007/09/05.20:42:44
2007/09/05.20:42:44 Processing location vlibminwrt
2007/09/05.20:42:44 Checking volume mf1-000001
2007/09/05.20:42:44 Volume mf1-000001 added to full volume list
2007/09/05.20:42:44 Checking volume mf1-000002
2007/09/05.20:42:44 Volume mf1-000002 added to full volume list
2007/09/05.20:42:44 Checking volume mf1-000003
```

```
2007/09/05.20:42:44 Volume mf1-000003 added to full volume list
2007/09/05.20:42:44 Checking volume mf1-000004
2007/09/05.20:42:44 Checking volume mf2-000001
2007/09/05.20:42:44 Full volume mf1-000001 added to volume movement list
2007/09/05.20:42:44 Full volume mf1-000002 added to volume movement list
2007/09/05.20:42:44 Full volume mf1-000003 added to volume movement list
2007/09/05.20:42:44 Created media movement request 1
2007/09/05.20:42:44 Done processing location vlibminwrt
2007/09/05.20:42:44 Media movement request 1 submitted; job id is 2
```

The location scan job identified volumes mf1-000001, mf1-000002, mf1-00003 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

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 will be 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 will appear 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.

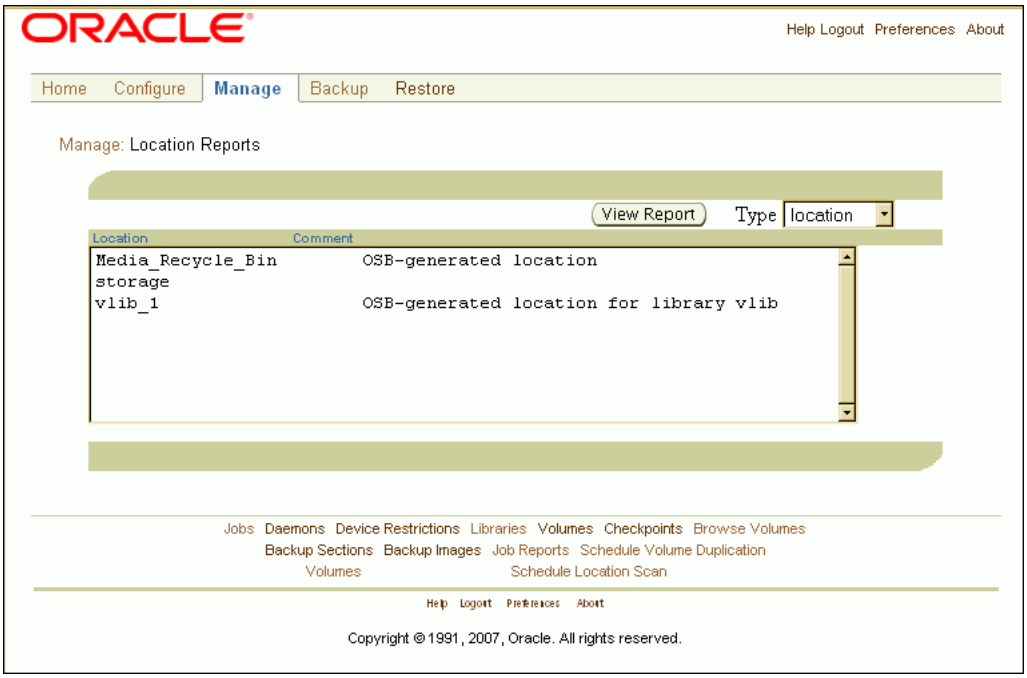
To view a location report using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Location Reports**.

   The Manage: Location Reports page appears.



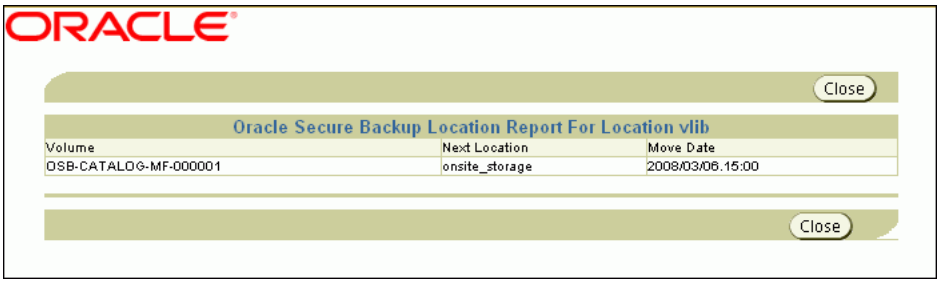
3. Select a location from the list of locations.

   The location report page lists all configured locations within the administrative domain.

4. Select **location** from the Type list.

5. Click **View Report**.

   A new 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 a 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 generates a volume recall request. The backup operator must explicitly enable this media movement job before the volume can be recalled.

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.

See Also: "Running Media Movement Jobs" on page 9-17

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 as part of your vaulting environment, then multiple copies of a backup volume might be available. Oracle Secure Backup first looks in its volumes catalog for all available duplicate volumes, determines their locations, and identifies the volume with the lowest recall time. If that volume is not at an active location, then Oracle Secure Backup schedules a media movement request for it.

See Also:

- "Configuring Defaults and Policies" on page 2-5
- *Oracle Secure Backup Reference* for more information on the `autovolumerelease` policy

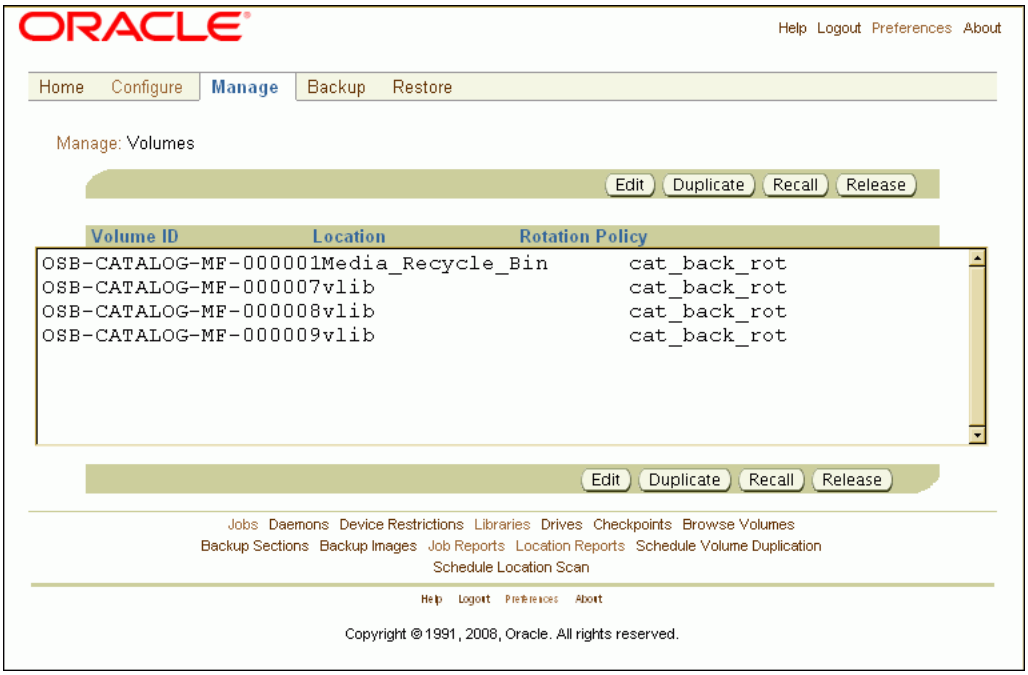
To recall a volume using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

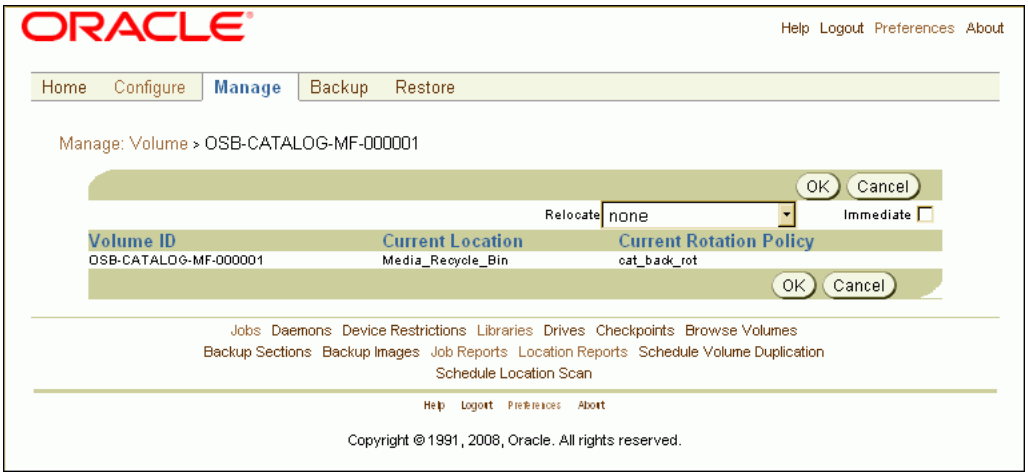
2. In the Media Life Cycle section, click **Volumes**.

   The Manage: Volumes page appears.



3. Select the volume you want to recall and click **Recall**.

   The Manage: Volume > *volume_name* page appears.

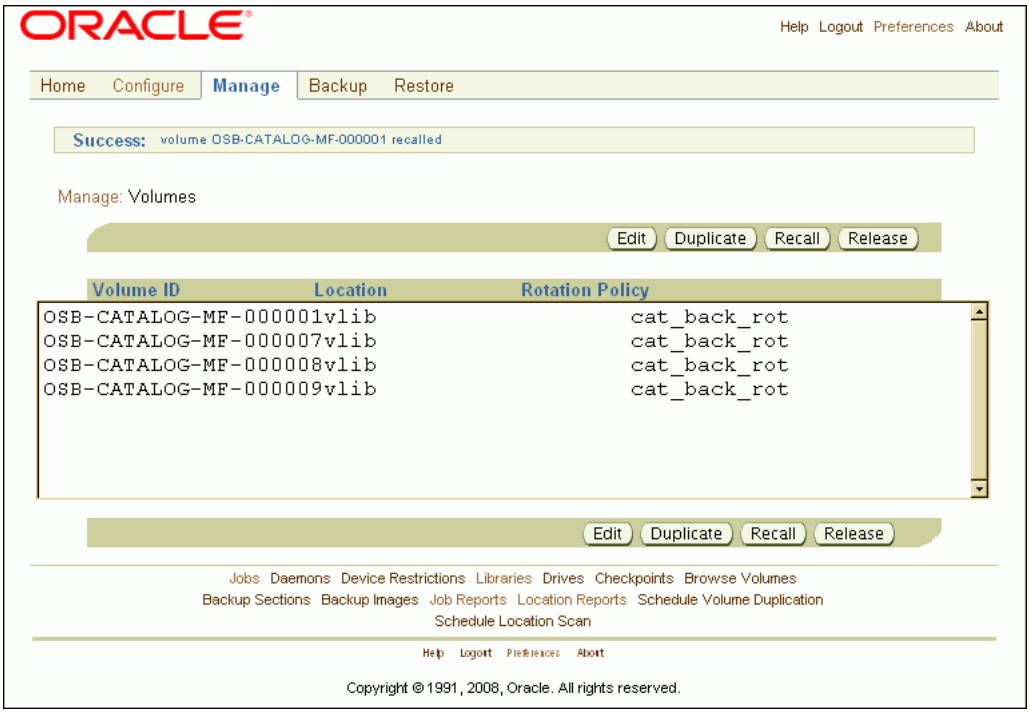


4. Select the location to which you want to recall the volume from the **Relocate** list.
5. Select the **Immediate** option to recall the volume immediately.

   If the Immediate option is not selected, then Oracle Secure Backup creates a media movement job in a pending state. This job will not run until an Oracle Secure Backup operator explicitly runs it.
6. Click **OK**.

   The Manage: Volumes page displays a success message, and the recalled volume appears in the list with its new location. Oracle Secure Backup has created an active or pending media movement job to move the recalled volume to its new location.

See Also: "Running Media Movement Jobs" on page 9-17



To release a volume using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Volumes**.

   The Manage: Volumes page appears.

3. Select the volume you want to release and click **Release**.

   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" on page 9-17

Viewing Job Reports

The following two job reports are generated automatically when you run a media movement job:

- 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.

- 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.

In each case the report name includes the media movement job number. Distribution and pick reports contain identical lists of volumes. The only difference between the

two reports is that the distribution report also contains the customer ID (if any) that was assigned to the next location.

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" on page 9-6 for more information on Iron Mountain FTP notification

To view distribution and pick lists using the Oracle Secure Backup Web tool:

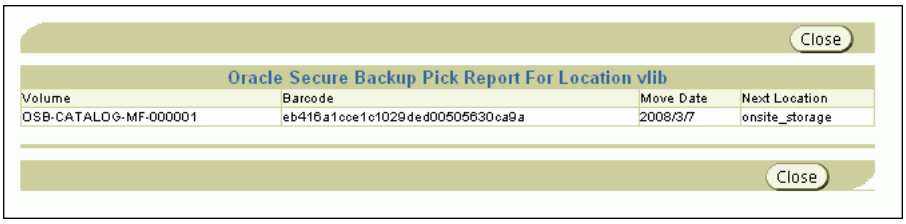
1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Job Reports**.

   The Manage: Job Reports page appears.

3. 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. If you want to duplicate a duplicate volume, then you must use an on-demand duplication.

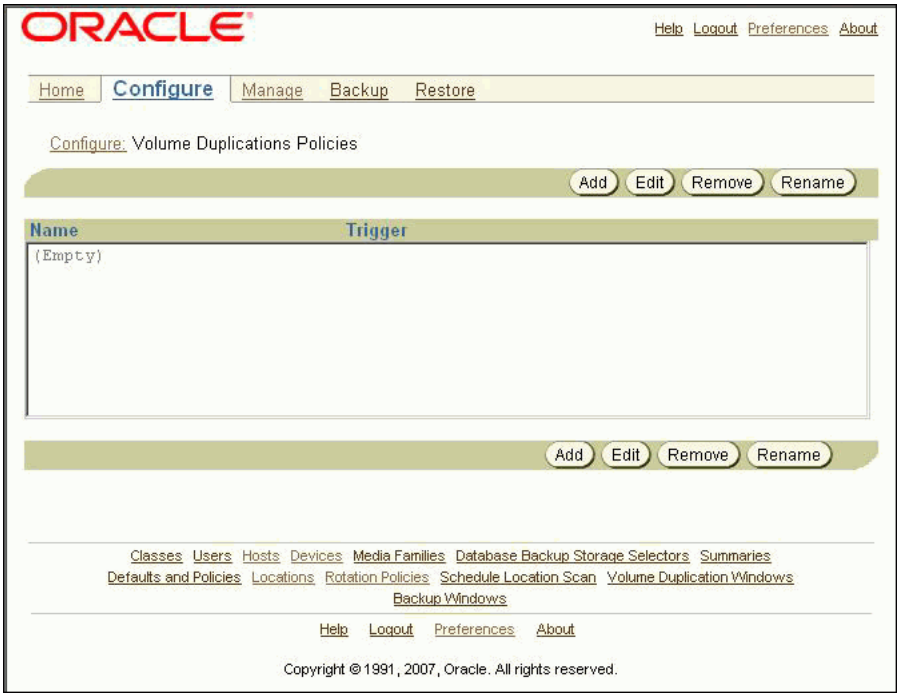
To add a duplication policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

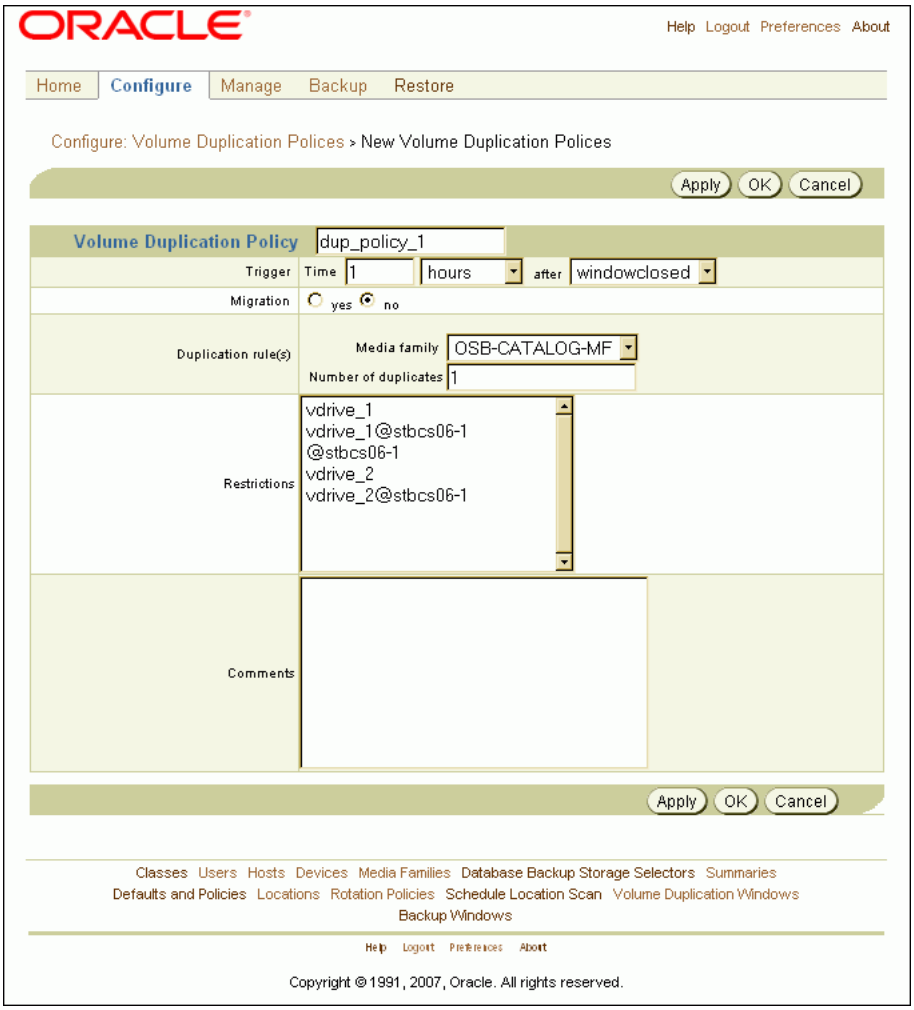
2. In the Media Life Cycle section, click **Volume Duplication Policies**.

   The Configure: Volume Duplication Policies page appears.



3. Click **Add**.

   The Configure: Volume Duplication Policies > New Volume Duplication Policies page appears.



4. 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.

5. 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 the following:

      – `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 of time 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.

For example, if you selected `1 day`, and `windowclosed`, then volume 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.

6. 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.

7. 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.

8. Enter the number of duplicates you want to make in the **Number of duplicates** field.

   The default is one duplicate.

9. 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.

10. Enter a description of this duplication policy in the **Comments** field.

    This step is optional.

11. Click **OK**.

    The Configure: Volume Duplication Policies page displays a success message, and your new 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. If you want to duplicate a duplicate volume, then you must use an on-demand duplication.

See Also: "On-Demand Volume Duplication" on page 9-36

To associate a volume duplication policy with a media family using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

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

   The Configure: Media Families page appears.

3. Select the media family you want to associate with a volume duplication policy and click **Edit**.

   The Configure: Media Families > *family_name* page appears.

4. 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" on page 9-12 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.

Oracle recommends 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 duplication window interval, then it is allowed to continue to run until the duplication process is finished. If any subordinate jobs or retry jobs are submitted by this job due

to a duplication failure, then the newly created jobs are scheduled in the next duplication window.

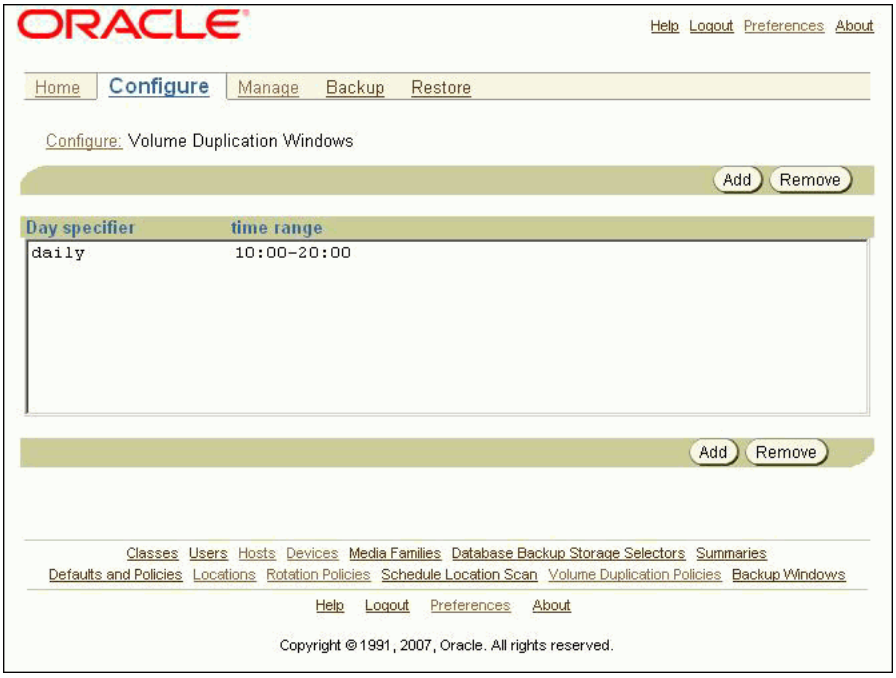
To add a duplication window using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Advanced section, click **Volume Duplication Windows**.

   The Configure: Volume Duplication Windows page appears.



3. 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**.

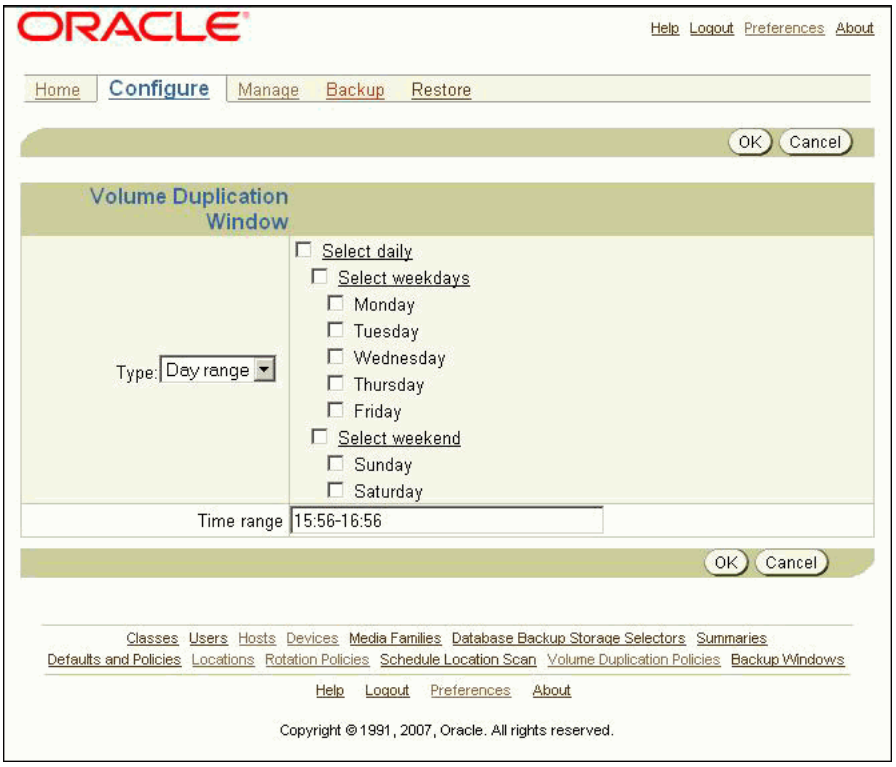
   A confirmation page appears.

4. 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.

5. Click **Add**.

   A new page appears.



6. Select a volume duplication window type from the **Type** list.
7. If you selected **Date** in step 6, then select a month, day, and year from the **Month**, **Day**, and **Year** lists.
8. If you selected **Day range** in step 6, 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
9. 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.
10. Click OK.

    The Configure: Volume Duplication Windows page displays a success message, and your new 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 location 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" on page 9-30

To add a volume duplication schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Schedule Volume Duplication**.

   The Manage: Schedule Volume Duplication page appears.

3. Click **Add**.

   The Manage: Schedule Volume Duplication > New Schedule Volume Duplication page appears.

4. Enter a name for the volume duplication schedule in the **Schedule Volume Duplication** field.

5. 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.

6. Select at least one location in the **Locations** list.

   You can use control-click to select more than one location or shift-click to select a range of locations. Only active locations can be specified in a volume duplication schedule.

7. Click **Apply**.

   The Manage: Schedule Volume Duplication > *schedule_name* page appears.

8. Click **Triggers**.

   The Manage: Schedule Volume Duplication > *schedule_name* > Triggers page appears.

9. In the Time section, select a **trigger** time from the **hours** and **minutes** lists.

10. Select a trigger type from the **Trigger type** list.

11. If you selected trigger type **Day** in step 10, 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.

12. If you selected trigger type **Month** in step 10, then select an option in the **Day in month** section.

13. Click **Add**.

The Manage: Schedule Volume Duplication > schedule_name > Triggers page displays a success message, and the trigger appears in the Trigger list.

14. If you want to add another trigger, then go back to step 9.

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 new 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.

> **See Also:** *Oracle Secure Backup Reference* for more information on the `duplicationjobpriority` policy

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 more than one tape drive 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.

> **See Also:** *Oracle Secure Backup Reference* for more information on duplication over networked tape devices

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 makes use of 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.

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" on page 9-17 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. A new 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 obtool `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.

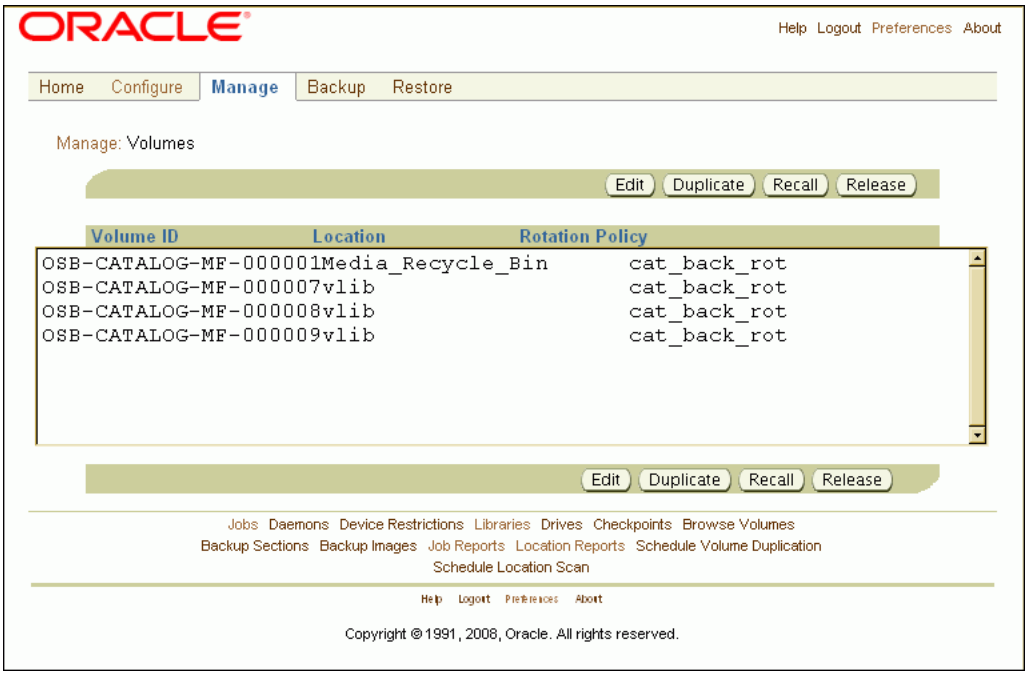
To manually duplicate a volume using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

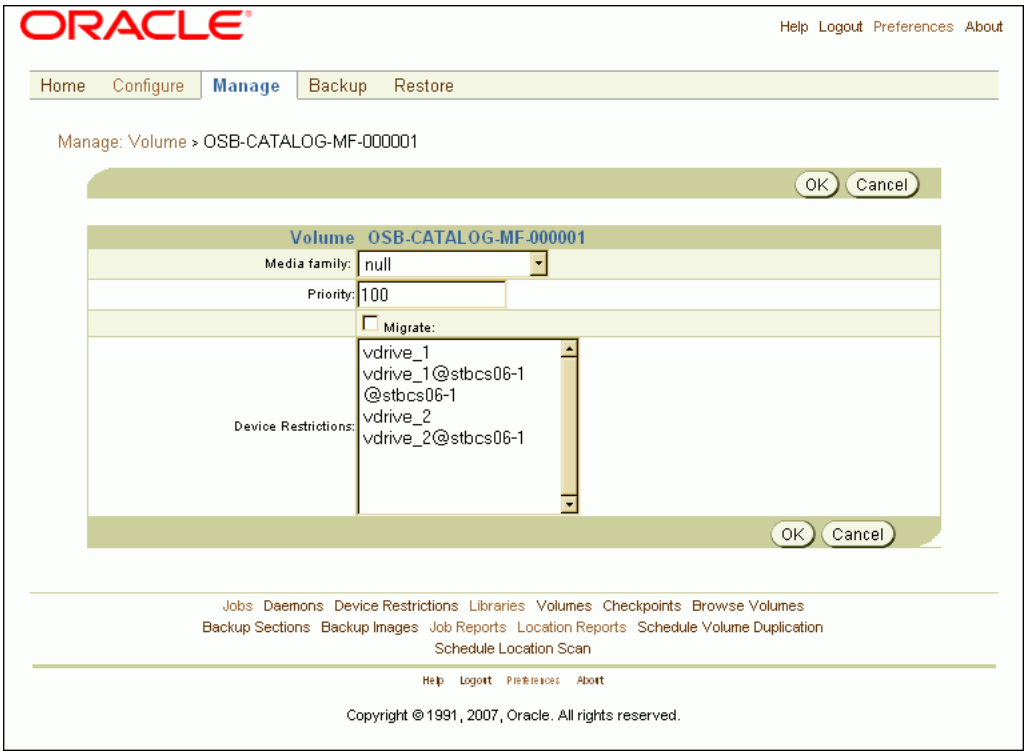
2. In the Media Life Cycle section, click **Volumes**.

   The Manage: Volumes page appears.



3. Select the volume you want to recall and click **Duplicate**.

   The Manage: Volume > *volume_name* page appears.



4. Select the media family you want the duplicate volume to belong to from the **Media family** list.
5. Enter a priority for this volume duplication 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.
6. Select the **Migrate** option if you want the duplicate volume to replace the original volume.

   If you select the Migrate option, 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 term 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.
7. If you want to restrict this volume duplication to a particular tape device or set of tape devices, then select those devices in the **Device Restrictions** list.

   If you do not select a restriction, then this volume duplication can use any available **tape device** on any **media server**, at the discretion of the Oracle Secure Backup scheduling system.
8. Click OK.

The Manage: Volumes page reports that the volume duplication job was submitted. When the volume duplication is completed, the Manage: Volumes page will display the duplicate volume.

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.

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 9–1 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 New Vaulting Environment" on page 9-5. 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 location scan for both `library` and `onsite_storage` at 0600.

Table 9–1 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 OSB-CATALOG-MF-000001.
1	0600	An Oracle Secure Backup location scan starts. Because 6 hours have elapsed since the first write to OSB-CATALOG-MF-000001, 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 OSB-CATALOG-MF-000001. The operator runs the job.
1	0815	The operator goes to the Web tool Manage: Job Reports page and reviews the distribution report for OSB-CATALOG-MF-000001.
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 location 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: Job 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 location 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.

Table 9–1 (Cont.) Inauguration of a Simple Vaulting Environment

Day	Time	Event
9	0815	The operator goes to the Web tool Manage: Job 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 Volumes
- Managing Locations
- Managing Rotation Policies
- Managing Rotation Policy/Media Family Associations
- Managing Location Scan Schedules
- Managing Volume Duplication Policies
- Managing Volume Duplication Policy/Media Family Associations
- Managing Volume Duplication Windows
- Managing Volume Duplication Schedules
- Changing Global Vaulting Policies
- Changing Global Volume Duplication Policies

Managing Volumes

This section provides step-by-step instructions for manually moving a volume from one location to another or changing its rotation policy.

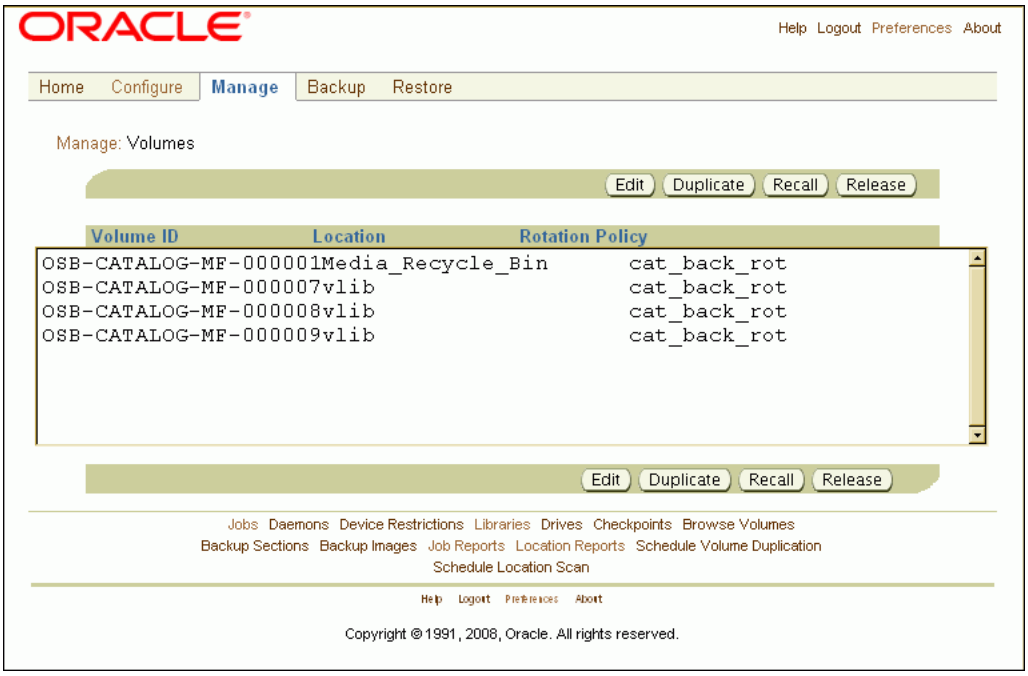
To change the location or rotation policy for a volume using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

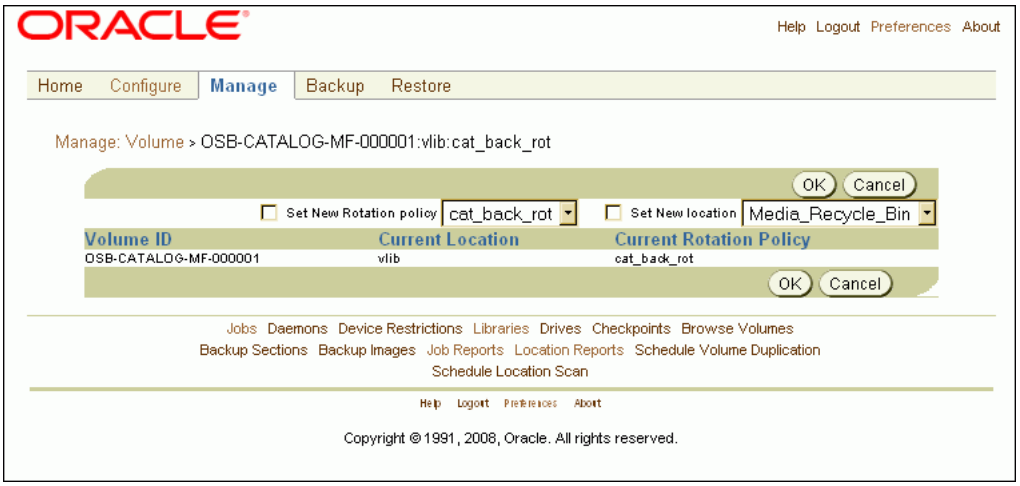
2. In the Media Life Cycle section, click **Volumes**.

   The Manage: Volumes page appears.



3. Select the volume whose location and/or rotation policy you want to change, and click **Edit**.

   The Manage: Volume > *volume_name:location:rotation_policy* page appears.



4. To change the rotation policy for the volume, select the **Set New Rotation policy** option and select a new rotation policy from the adjacent list.

   If you specify a new rotation policy but not a new location, and if the new rotation policy does not include the current location of the volume, then Oracle Secure Backup changes the rotation policy but warns you that the volume is stranded.

5. To change the location of a volume, select the **Set New location** option and select a new location from the adjacent list.

   If you selected a new rotation policy in the previous step, then the new location must be in the new rotation policy. If you did not select a new rotation policy, then the new location must be in the current rotation policy. Either way, Oracle Secure

Backup does not allow you to move a volume to a location that is not in the rotation policy that applies to the volume.

6. Click **OK**.

   The Manage: Volumes page displays a success message, and the recalled volume appears in the list with its new rotation policy, location, or both.

   If you selected a new location for the volume, then Oracle Secure Backup created a pending media movement job for the move. This media movement job must be run by an Oracle Secure Backup operator to move the volume to its new location.

   See Also: "Running Media Movement Jobs" on page 9-17

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 on 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. It a vaulting vendor adds support for Iron Mountain FTP notification, for example, you would want to edit your storage location to change its notification type.

To edit or view storage location properties using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Locations**.

   The Configure: Locations page appears.

3. Select a storage location whose properties you want to edit or view and click **Edit**.

   The Configure: Locations > *location_name* page appears.

4. Make whatever changes you want.

5. Click **OK**.

   The Configure: Locations page displays a success message.

Removing a Storage Location

To remove a storage location with the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Locations**.

The Configure: Locations page appears.

3. Select the storage location you want to remove and click **Remove**.

   A location that is 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.

   > **See Also:** "Managing Rotation Policies" on page 9-44 for instructions on removing a storage location from a rotation rule

   A location that contains volumes managed by Oracle Secure Backup cannot be deleted. Those volumes must be relocated before the location can be deleted.

   A confirmation page appears.

4. 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

To rename a storage location with the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Locations**.

   The Configure: Locations page appears.

3. Select a storage location whose name you want to change and click **Rename**.

   Storage locations can be renamed without consequence. Oracle Secure Backup assigns a **Universal Unique Identifier (UUID)** to each location object, and all internal references use the UUID rather than the location name. If the name of the location is changed, then all rotation policies that reference that name will be updated.

   A new page appears.

4. Enter the new 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 new 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

To edit or view the properties of an existing rotation policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Rotation Policies**.

   The Configure: Rotation Policies page appears.

3. Select the rotation policy whose properties you want to view or edit and click **Edit**.

   The Configure: Rotation Policy > *policy_name* page appears.

4. To add a new 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" on page 9-8 for more information on rotation rules

5. 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 as long as no volumes are currently at that location.

6. To add a descriptive comment to the selected rotation policy, enter text in the **Comments** field and click **Apply**.

Removing a Rotation Policy

To remove an existing rotation policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Rotation Policies**.

   The Configure: Rotation Policies page appears.

3. Select the rotation policy you want to remove and click **Remove**.

   A confirmation page appears.

4. 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

To rename an existing rotation policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Rotation Policies**.

   The Configure: Rotation Policies page appears.

3. Select the rotation policy you want to rename and click **Rename**.

   A new page appears.

4. Enter the new 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 new 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 new rotation policy. The rotation policy of volumes associated with the media family will be changed as well. Only those volumes still in their originating location will have their rotation policy changed. The rotation policy of volumes that have moved out of their originating location will not be changed.

To remove or change the rotation policy associated with a media family using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

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

   The Configure: Media Families page appears.

3. Select the media family whose rotation policy you want to remove or change and click **Edit**.

   The Configure: Media Families > *family_name* page appears.

4. 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.

5. To replace the existing rotation policy, select a new rotation policy from the **Rotation policy** list and click **OK**.

   The Configure: Media Families page displays a success message.

Managing Location Scan Schedules

This section provides step-by-step instructions for editing, removing, and renaming an existing location scan schedule.

This section contains these topics:

- Editing or Viewing the Properties of a Location Scan Schedule
- Removing a Location Scan Schedule
- Renaming a Location Scan Schedule

Editing or Viewing the Properties of a Location Scan Schedule

To edit or view the properties of an existing location scan schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

The Manage page appears.

2. Click **Schedule Location Scan**.

   The Manage: Schedule Location Scan page appears.

3. Select the location scan schedule you want to edit or view and click **Edit**.

   The Manage: Schedule Location Scan > *schedule_name* page appears.

4. Make whatever changes you want to the location scan schedule priority, locations, or comments.

   Click **Triggers** to add or remove a location scan schedule **trigger**.

5. Click **OK** to accept the changes.

   The Manage: Schedule Location Scan page displays a success message, and the edited schedule appears in the list of schedules.

6. Click **Cancel** to return to the Manage: Schedule Location Scan page without changing anything.

Removing a Location Scan Schedule

To remove an existing location scan schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. Click **Schedule Location Scan**.

   The Manage: Schedule Location Scan page appears.

3. Select the location scan schedule you want to remove and click **Remove**.

   A confirmation page appears.

4. Click **Yes**.

   The Manage: Schedule Location Scan page displays a success message, and the selected schedule no longer appears in the list of schedules.

Renaming a Location Scan Schedule

To rename an existing location scan schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. Click **Schedule Location Scan**.

   The Manage: Schedule Location Scan page appears.

3. Select the location scan schedule you want to rename and click **Rename**.

   A new page appears.

4. Enter the new name for the schedule in the **Rename *schedule_name* to** field and click **Yes**.

   The Manage: Schedule Location Scan page displays a success message, and the selected schedule appears in the list of schedules with its new 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 duplicates already created.

To edit or view the properties of an existing volume duplication policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Volume Duplication Policies**.

   The Configure: Volume Duplication Policies page appears.

3. Select the volume duplication policy you want to edit or view and click **Edit**.

   The Configure: Volume Duplication Policies > *policy_name* page appears.

4. 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 using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Volume Duplication Policies**.

   The Configure: Volume Duplication Policies page appears.

3. Select the duplication policy you want to remove and click **Remove**.

   A confirmation page appears.

4. 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

To rename an existing volume duplication policy using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Media Life Cycle section, click **Volume Duplication Policies**.

   The Configure: Volume Duplication Policies page appears.

3. Select the duplication policy you want to rename and click **Rename**.

   A new page appears.

4. Enter the new name in the **Rename *policy_name* to** field and click **Yes**.

   The Configure: Volume Duplication Policies page displays a success message, and the selected duplication policy appears in the list of policies with its new name.

Managing Volume Duplication Policy/Media Family Associations

To remove or change the rotation policy associated with a media family using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

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

   The Configure: Media Families page appears.

3. 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.

4. 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.

5. To replace the existing volume duplication policy, select a new 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" on page 9-30.

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 new time range appended to the existing volume duplication window.

To remove a volume duplication window with the Oracle Secure Backup **Web tool**:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

   The Configure page appears.

2. In the Advanced section, click **Volume Duplication Windows**.

   The Configure: Volume Duplication Windows page appears.

3. Select the volume duplication window you want to remove and click **Remove**.

   A confirmation page appears.

4. 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

To edit or view the properties of a volume duplication schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Schedule Volume Duplication**.

   The Manage: Schedule Volume Duplication page appears.

3. Select the volume duplication schedule you want to edit or view and click **Edit**.

   The Manage: Schedule Volume Duplication > *schedule_name* page appears.

4. Make whatever changes you want to the volume duplication policy and click **OK**.

The Manage: Schedule Volume Duplication page displays a success message, and the edited volume duplication schedule appears in the list.

Removing a Volume Duplication Schedule

To remove a volume duplication schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Schedule Volume Duplication**.

   The Manage: Schedule Volume Duplication page appears.

3. Select the volume duplication schedule you want to remove and click **Remove**.

   A confirmation page appears.

4. 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

To rename a volume duplication schedule using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Schedule Volume Duplication**.

   The Manage: Schedule Volume Duplication page appears.

3. Select the volume duplication schedule you want to rename and click **Rename**.

   A new page appears.

4. Enter the new 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 new 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.

- `minwritablevolumes`

Use the `minwritablevolumes` policy to specify the minimum number of writable volumes that must be available in each tape library at all times. If the number of writable volumes in a tape library drops below 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 using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

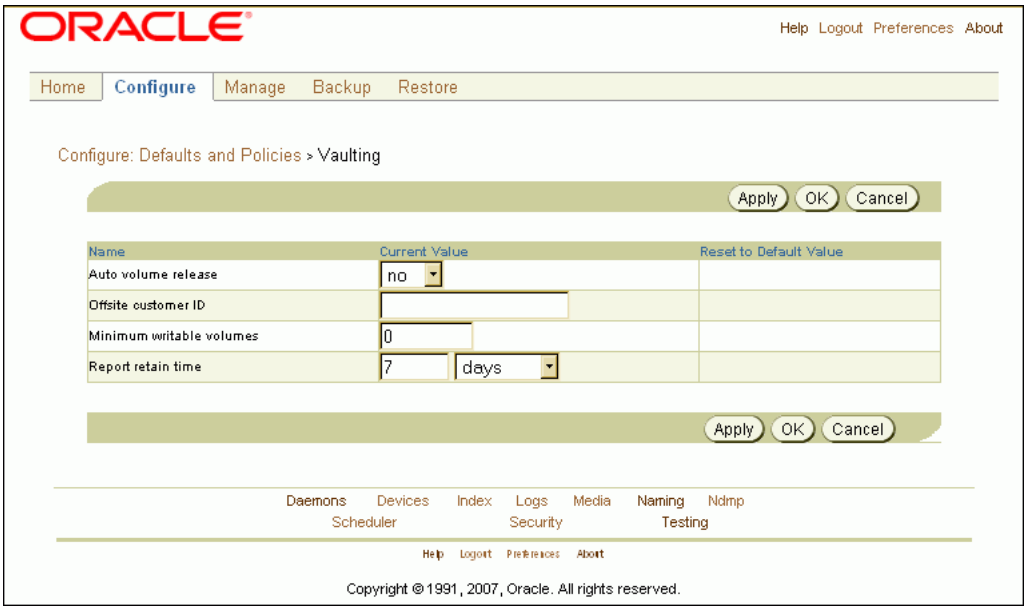
   The Configure page appears.

2. In the Advanced section, click **Defaults and Policies**.

   The Configure: Defaults and Policies page appears.

3. In the Policy column, click **vaulting**.

   The Configure: Defaults and Policies > Vaulting page appears.



4. Make whatever vaulting policy changes you want and click **OK**.
5. 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 using the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Configure**.

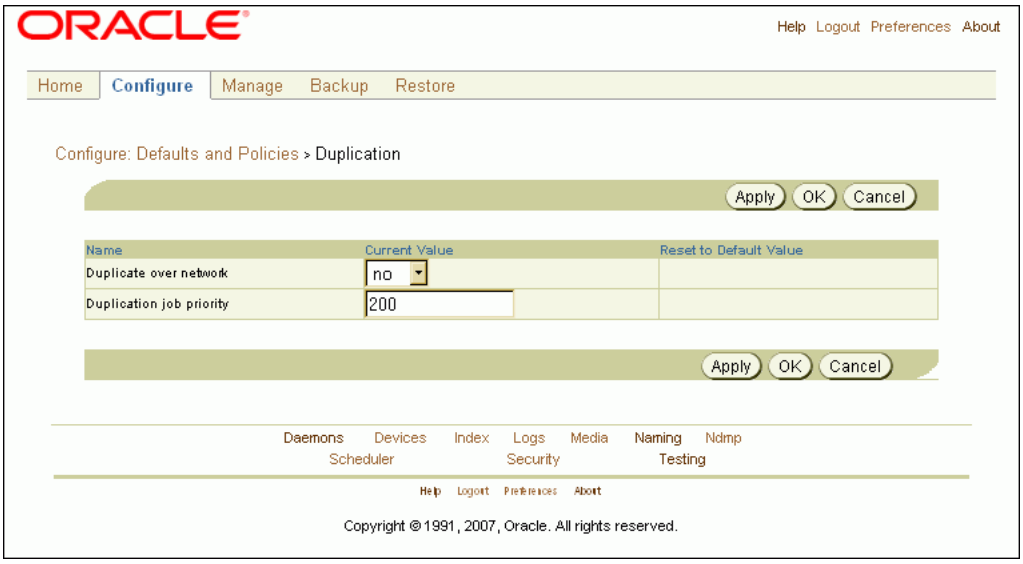
   The Configure page appears.

2. In the Advanced section, click **Defaults and Policies**.

   The Configure: Defaults and Policies page appears.

3. In the Policy column, click **duplication**.

   The Configure: Defaults and Policies > Duplication page appears.



4. Make whatever volume duplication policy changes you want and click **OK**.

5. 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 10*g* release 2 (10.2) and later **Recovery Manager (RMAN)** `restore database preview` and `restore database preview recall` commands. In Oracle Database 10*g* release 2 (10.2) and later, an RMAN restore will fail 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=/ade/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: TAG20070810T150035
RMAN-06355:         Handle: 05ip1s0j_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 /ade/jfersten_tstvw1/oracle/dbs/t_db1.f
RMAN-06338:   2       Full 308037     10-AUG-07 /ade/jfersten_tstvw1/oracle/dbs/t_ax1.f

RMAN-08607: List of remote backup files
RMAN-06320: ============================
RMAN-06355:         Handle: 05ip1s0j_1_1   Media:
rmanvltfam-001,rmanvltfam-002,rmanvltfam-003,rmanvltfam-004
RMAN-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.

See Also: "Recalling a Volume" on page 9-22

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=/ade/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: TAG20070
810T150035
RMAN-06355:         Handle: 05ip1s0j_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 /ade/jfersten_tstvw1/oracle/dbs/t_db1.f
RMAN-06338:   2       Full 308037     10-AUG-07 /ade/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. That job is in a pending state and must be run the Oracle Secure Backup operator. An obtool `lsjob` command returns the following information about this media movement job:

```
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
```

An obtool `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 2007/8/10    vlibrman
rmanvltfam-002  b22b696a29f5102ad52000cf1ce8d3a 2007/8/10    vlibrman
rmanvltfam-003  b26873be29f5102ad52000cf1ce8d3a 2007/8/10    vlibrman
rmanvltfam-004  b39fbf9429f5102a9f0000cf1ce8d3a 2007/8/10    vlibrman
```

The media movement job is in a pending state. The operator can run the media movement job with an obtool `runjob` command:

```
ob> runjob --mediamovement --now 17
```

In releases before Oracle Database 10*g* 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" on page 9-22.

See Also:

- "Adding Locations" on page 9-6 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 at the same time, their distribution lists are interchanged, and they are all 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 will not flag it as misplaced. The Oracle Secure Backup catalog will still show it as residing in its former location. Its misplaced status will not be 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 a physical search.

If the wrong volume is returned from a storage location, then two volumes are misplaced simultaneously. Suppose, for example, that 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 will show `vol00001` in the Media_Recycle_Bin when it is really still at the storage location. Worse, it will show `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 that is misplaced en route to a storage location is arguably the worst case. The volume is no longer in your administrative domain, and you will 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 worst case by generating two distribution reports for each media movement job: one distribution report accompanies the volume to the storage location, and 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 Job Reports" on page 9-25

Volumes Outside Their Rotation Policies

Volumes are associated with rotation policies. Volumes inherit their rotation policies from their media families. If you change the rotation policy associated with a media family, then the new policy applies to all volumes that belong to the media family and that have not yet left their originating locations. The new rotation policy does not apply to volumes that belong to the media family but are no longer at their originating location.

See Also: "Associating Rotation Policies with Media Families" on page 9-12

Note: A volume can also be assigned to a new rotation policy with the obtool `chvol --rotationpolicy` option.

If the new rotation policy includes all locations included in the old policy, then there is no problem with volumes that have already left their originating locations. But if the new 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 will not create media movement jobs for these volumes, because it will not look for them in the omitted locations.

Stranded volumes must be moved to a location specified in the new rotation policy with the Oracle Secure Backup Web tool Manage: Volumes page. These stranded volumes appear in the volume exception report.

Viewing Exception Reports

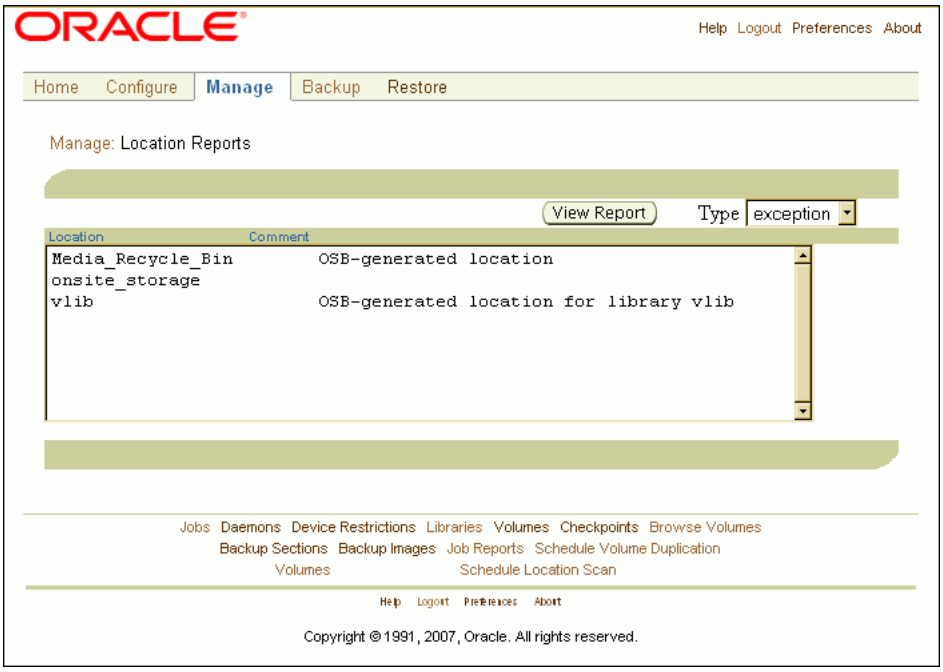
To generate an exception report with the Oracle Secure Backup Web tool:

1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Media Life Cycle section, click **Location Reports**.

   The Manage: Location Reports page appears.



3. 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.

10

Managing Backup Encryption

The security of your backup tapes is extremely important, because they typically contain your most important data stored in one localized, compact, and easily transportable medium. You can have the most secure set of protection policies, a **firewall**, passwords, and retina scanners to protect access to data. But if your data is backed up on a portable storage medium in an unencrypted fashion, and if that storage medium leaves the security of your media room, then your security model breaks down.

Backup Encryption is an optional and highly configurable Oracle Secure Backup mechanism that ensures that data stored on tape is safe from prying eyes. Backup encryption is fully integrated with Oracle Secure Backup and is ready to use as soon as Oracle Secure Backup is installed. Backup encryption applies to both file system data and **Recovery Manager (RMAN)** generated backups.

> **Note:** Encryption is not supported for volume duplication, volume migration, or media management. For more information on these topics, see Chapter 9, "Vaulting".

Backup encryption provides the backup administrator with the means to ensure that all **client** data that is written to tape is encrypted. It is not intended to enable an individual user to decide which of their data is encrypted or how it is encrypted. Nor is it meant to protect one user's data from another user. If you must encrypt data for individual users at the hard drive level, then Oracle recommends you use an operating system that provides built in encryption at the file system level, such as that provided by Windows with Encrypted File System (EFS), or a product such as PGP.

This chapter contains these sections:

Enabling Backup Encryption

Backup encryption is designed to be easy to implement. At its simplest the backup administrator is required to change just one global policy, and all data from each **client** is encrypted. For larger enterprises and for those backup administrators who wish to optimize their backup domain, backup encryption offers a large degree of configuration flexibility.

For **file system backup**, encryption can be selected for the entire **administrative domain**, a specific client, or even a specific **backup job**. The hierarchy of decisions going from highest precedence to lowest precedence for the encryption setting is global, client, job. If backup encryption is enabled at the global level, then the data coming from all clients and all jobs is encrypted. If the global policy does not enforce encryption, then the client encryption setting determines if encryption is performed. If the client does not require encryption, then the decision for encryption is deferred to the job level.

The global and client encryption policies have two possible settings:

- `required`

  All data coming from this backup domain or this client must be encrypted.

- `allowed`

  The decision to encrypt is deferred to the next lower priority item.

In general, encryption of **Recovery Manager (RMAN)** data follows the same rules as that of file systems. One difference is if the RMAN data coming out of the **SBT interface** is encrypted, then there is no further encryption. Another difference is that you cannot turn encryption on for one RMAN backup, because the job is created on the fly.

Note: If a host is configured for encryption `required`, and if RMAN backup encryption is not enabled, then Oracle Secure Backup encrypts the RMAN backups using Oracle Secure Backup encryption based on the host encryption configuration. However, if RMAN backup encryption is enabled, then Oracle Secure Backup is aware that the backup is encrypted. This RMAN encryption satisfies the `required` encryption policy for this host, and no other host encryption settings are honored by Oracle Secure Backup. Oracle Secure Backup specifically does *not* honor rekey duration, encryption algorithm or key generation settings in this situation.

You can disable Oracle Secure Backup encryption with RMAN parameter `OB_ENCRYPTION_FORCED_OFF`.

See Also: *Oracle Database Backup and Recovery User's Guide* for more information

Backup Encryption Options

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

> **Note:** The backup encryption algorithm cannot be selected at the job level.

A client `rekeyfrequency` policy defines when a new key is generated. For example, the policy might require that a new 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.

Backup Encryption Keys

Keys can be generated either automatically 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 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 new 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 case where a key is not automatically added to the **wallet**. Keys for transient backups are effectively one-use keys and are not usually stored in the wallet. The backup administrator can override this behavior through a command line option. See "Transient Backups" on page 10-4 for more information on transient backups.

When a key expires, a new key is automatically generated. For passphrase generated keys, on the other hand, 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.

Backup Encryption Security

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 **Secure Sockets Layer (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. It is a best practices task for the backup administrator to ensure that the encrypted key stores are backed up. This should be easy to accomplish, because the encrypted key stores reside within a file system branch that should already be backed up as a best practices task. 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 the administrative data were encrypted with a automatically generated key, and if the **administrative server** were destroyed, then there would be no way to get back the decryption key used to encrypt the encryption keys. A backup of the administrative server tree should be done using a transient backup.

Encrypting Data

Data is encrypted at the **client** level. Each client has its own set of keys. One key is the active key used for encrypting new 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 **Network Attached Storage (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, **Network Data Management Protocol (NDMP)** is used for backup and restore operations.

Transient Backups

There might be times when the backup administrator must back up a set of data from backup domain Site A and restore it at another backup domain Site B. The backup set might contain backup files for several clients. Each of these **client** backup files is encrypted to a client-specific encryption key, which was most likely used in recent backups at Site A. In order for Site B to decrypt the data, the backup administrator would have to collect all keys used in encrypting the data at Site A and then ship those keys to Site B.

This 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 this 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.

> **See Also:** *Oracle Secure Backup Reference* for complete syntax and semantics of the **obtool** `backup` command

One-Time Unencrypted Backups

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 the new 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_FORCED_OFF` variable from within RMAN.

> **See Also:** *Oracle Secure Backup Reference* for complete syntax and semantics of the **obtool** `backup` command

Day-to-Day Backup Encryption Example

By default the initial global and **client** backup encryption policy settings are `allowed`. Encryptions keys are generated automatically with a default AES192 encryption algorithm. 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.

In this more complicated enterprise, there are three classes of hosts that need differing types 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 new encryption key each week.

- CEO

  This client requires all data to be encrypted using a passphrase-generated key.

There are no options that must be changed for developer clients. The backup administrator instead updates the **backup job** for the sourcecode dataset that is used

to back up the developer computers. If the **backup schedule** does not yet exist, then the backup administrator creates a new backup schedule with a `mkhost` command:

```
mksched --dataset sourcecode --type backup --encryption yes SourceCode
```

If the backup schedule already 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 can make these changes with a `chhost` command:

```
chhost -algorithm aes256 -encryption required -rekeyfrequency 1week Payroll
```

This will ensure that all data from the payroll client is always encrypted to the AES256 algorithm with a new key encryption key each week.

The default encryption is sufficient for the CEO client, but the backup administrator must change the encryption key type to passphrase-generated. This can be done with another `chhost` command:

```
chhost --keytype passphrase -passphrase "What's my password?" TheBoss
```

Once the initial configuration has been performed there is minimal additional overhead managing backup encryption.

The encryption state is displayed as part of the job transcript during a backup operation for both file system and RMAN backups.

11

Oracle Secure Backup Catalog Recovery

The computers we use to back up our data can themselves fail. To guard against such failures Oracle Secure Backup protects its own **catalog** and settings data, without which all the other backups it has performed are just so many assorted tapes. If the catalog data is lost, then Oracle Secure Backup can restore these data to the state they were in before the failure.

When Oracle Secure Backup is first installed on your **administrative server**, a scheduled job is set up by the installer to back up the catalog data every day at midnight.

Oracle Secure Backup catalog recovery does not impose any burden on the backup administrator unless there is an actual failure. No configuration is required, but Oracle Secure Backup catalog recovery can be extended and customized by the backup administrator.

Oracle Secure Backup catalog recovery protects only the catalog and settings on an Oracle Secure Backup **administrative server**. The operating system and other installed software are not automatically backed up.

This chapter contains these sections:

Catalog Recovery Concepts

Oracle Secure Backup **catalog** recovery creates four reserved objects:

These reserved objects cannot be deleted, and some of their properties cannot be changed. The idea is to prevent catalog backups from being disabled or given settings which make them useless by accident.

Catalog Recovery Schedule Object

This object drives the **catalog** recovery backup process. It 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 the characteristics of the resulting 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

Catalog backups can be disabled by removing the trigger from this reserved schedule object. The associated dataset cannot be changed, and only non-encrypted full backups are permitted. An **incremental backup** of the catalog data is disallowed. It adds complexity during the restore process, which must be kept simple because it is done in the absence of catalog data.

> **Note:** A backup using an automatically generated encryption key would be useless without the on-disk key store, which would be lost if the **administrative server** were destroyed.

Catalog Recovery Media Family Object

A **catalog** recovery **media family** object describes the tape volumes which 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. Oracle recommends rotating backups across 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**
- 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 of file system data cannot be content-managed.

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 without storage encryption, regardless of the encryption policy.

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 will report 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 database 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

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 summary report is generated with a `--catalog` option which causes Oracle Secure Backup to include extended information about catalog recovery backups. When a summary report is generated with the `--catalog` option, 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 will be mixed with the other backup jobs. The `--catalog` option is intended to make it easier for a backup administrator to check the status of catalog backups separately from other backup jobs.

Modifying Catalog Recovery Objects

All reserved **catalog** recovery objects are just 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.

To modify catalog recovery objects, you can use **obtool** commands `chsched`, `chmf`, `chsum`, and `edds`. You can also use the Oracle Secure Backup **Web tool** or Oracle Enterprise Manager equivalents. The interface does not allow some things to be changed, but for everything else the reserved objects act just like normal objects.

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 in the usual way.

> **See Also:** "Transient Backups" on page 10-4 for more information on transient passphrase encryption

Catalog Recovery Procedure

This section describes the basic procedure for restoring the admin directory in the event of media failure or loss of the **administrative server**. Catalog restore operations are needed when some grave misfortune has befallen the catalog on the administrative server.

Oracle highly recommends that you maintain a record of Oracle Secure Backup device attachments (especially for the devices you intend to use in the case of disaster recovery), because it will be invaluable when reinstalling Oracle Secure Backup in the event of a disaster. Otherwise you must add/install/configure all media servers and their tape devices in the new administrative domain, and then examine the volumes in your inventory one-by-one to locate the required Oracle Secure Backup catalog backup.

The best way to prepare for a catalog recovery emergency is to:

- Retain a copy of your obtool `lsd -l` output.

- Note the attachment information listed.
- Retain 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.

To restore your Oracle Secure Backup administrative server:

1. Perform a fresh install of Oracle Secure Backup on the administrative server.

   Note: To complete the process of restoring the original administrative server, you must have the password that was used to create the original encryption wallet. The encryption wallet created during the fresh install of Oracle Secure Backup is used only during the restore of the original administrative server. It will be replaced with the original encryption wallet.

   See Also: *Oracle Secure Backup Installation and Configuration Guide* for instructions on installing Oracle Secure Backup on Windows and Linux or UNIX

2. Add a **media server** to your newly created **administrative domain** and re-create your tape devices.

   If your administrative server does not have an attached **tape device**, then you must add a remote media server host from the previous Oracle Secure Backup administrative domain to this new administrative domain. This media server host should also have access to the library containing the most recent catalog backup and a tape drive. Alternatively, if you can locate the volume by its label, then the volume can be manually loaded into the most convenient tape drive. In either case, you must configure a tape device through the Oracle Secure Backup Web tool or obtool to be used for restoring the catalog data.

   If you do not have a media server local to the administrative host and need to add a remote media server that was part of the Oracle Secure Backup administrative domain before the administrative server failed in order to perform disaster recovery, then Oracle Secure Backup will try to add it with a different **Universal Unique Identifier (UUID)**. The new UUID will cause media server operations to fail, because it will not match the **identity certificate** residing on the media server.

   The workaround is to decertify the media server by running `obcm decertify` on the media server (as root) before running the obtool `mkhost` command on the administrative server. The `obcm` utility is located in $OSB_HOME/bin.

   You must repeat this step after the catalog is restored, and then you must do the following on the Oracle Secure Backup administrative server to recertify the remote media server and complete the process:

```
cd OSB_HOME/admin/history/host
mv media_server media_server_save
ob> rmhost --nocomm media_server
remove host media_server? (a, n, q, y, ?) [n]: y
ob> mkhost media_server
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
ob> lsh -l media_server
media_server:
    Access mode:            OB
    TCP/IP buffer size:     not set (global policy)
```

```
    Algorithm:              aes192
    Encryption policy:      allowed
    Rekey frequency:        1 month (system default)
    Key type:               transparent
    In service:             yes
    Roles:                  client
    Trusted host:           no
    Certificate key size:   1024
    UUID:                   50d97a76-0500-102b-a4bb-080020a0a249
ob> pinghost media_server
media_server:     Oracle Secure Backup and NDMP services are available
```

After you have recertified the remote media server, you can move the saved catalog directory back into place:

```
cd OSB_HOME/admin/history/host
mv media_server_save media_server
```

This first example configures a tape library and tape drive attached to the administrative host jfersten-sun:

```
jfersten-sun# obtool
Oracle Secure Backup 10.2.0.2.0.
login: admin
ob> chhost --addrole mediaserver jfersten-sun
ob> mkdev -t library -a jfersten-sun:/dev/obl0 jflib
ob> mkd -t tape -a jfersten-sun:/dev/obt0 -d 1 -l jflib jftape
ob> lshost
 jfersten-sun        admin,mediaserver,client (via OB)   in service
```

This second example configures a remote media server and its devices from the administrative host jfersten-sun:

```
ob> mkhost storabck04
Info: waiting for host to update certification status...
ob> chhost --addrole mediaserver storabck04
ob> mkdev -t lib --attach storabck04:/dev/sg4 stbk4lib
ob> mkdev -t tape -l stbk4lib -d 1 --attach storabck04:/dev/sg5 stbk4tape
```

Note: Before running `mkhost` on the Oracle Secure Backup administrative server, be sure to run `$OSB_HOME/bin/obcm decertify` on the remote media server.

---

3. Locate the volume that contains your most recent OSB_CATALOG backup and load it into the drive. It will be helpful if you have saved a record of your catalog backups so that the tape is easier to locate. The job summary for a catalog backup provides the volume ID, bar code, and file number for the catalog backup. If you do not have this information but know that the volume is in your library, then run obtool `inventory` and `identifyvol` commands on the library.

   The following example shows a job summary for a catalog backup:

```
Job ID      Scheduled At        Completed At       Content
  Backup Size  File #   Volume ID (Bar Code)
admin/1.1   2008/03/26.11:48    2008/03/26.11:49   *catalog jfersten-sun
  455 KB         1      OSB-CATALOG-MF-000002 (e744f09c4eeb4dabf3ac02ae2d332c0)
```

Note: It will be necessary to run an initial inventory on the library before using it for the first time even if you know which volume contains your OSB_CATALOG backup.

```
ob> inv -L jflib
ob> lsvol -L jflib
Inventory of library jflib:
    in    3:             occupied
    in    4:             unlabeled
    in    5:             unlabeled
    in    6:             unlabeled
    in    7:             unlabeled
    in    8:             unlabeled
    in    9:             unlabeled
```

Run the `identifyvol` command only if you do not know which volume contains your catalog backup. If you do know which volume contains your catalog backup, then simply load that volume into the drive and skip to the obtar command shown in step 5.

```
ob> identifyvol --import -D jftape 3-9

Seq       Volume              Volume    Archive     Client      Backup
 #         ID                  Tag     File Sect     Host        Level
 1    OSB-CATALOG-MF-000002              1   1    jfersten-sun     0
Archive Create
 Date & Time
2008/03/23 10:39:54s

ob> lsvol -L jflib
Inventory of library jflib:
   in    3:             volume OSB-CATALOG-MF-000002, 6891336 kb remaining,
expires 2008/04/13.10:39
```

4. If you are restoring a Linux or UNIX Oracle Secure Backup administrative server, then go to steps 5 and 6.

   If you are restoring a Windows administrative server, then the procedure described in steps 5 and 6 for extracting the admin and db directories is not applicable. Use the procedure described in steps 7, 8, and 9 instead.

5. This step applies only to Linux and UNIX administrative servers.

   Load your OSB-CATALOG-MF backup volume into the drive and re-create an Oracle Secure Backup catalog from the volume using the `obtar -Gtf` *`drive_name`* `-F` *`file_number`* command:

```
# obtar -Gtf jftape -F 1
Volume label:
    Volume UUID:        4cfe75d8-db47-102a-9d77-080020a0a249
    Volume ID:          OSB-CATALOG-MF-000002
    Volume sequence:    1
    Volume set owner:   root
    Volume set created: Sun Mar 23 10:39:54 2008
    Volume set closes:  Sun Mar 30 10:39:54 2008 (no writes after this time)
    Volume set expires: Sun Apr 13 11:39:54 2008
    Media family:       OSB-CATALOG-MF
    Original UUID:      4cfe75d8-db47-102a-9d77-080020a0a249
Archive label:
```

```
File number:        1
File section:       1
Owner:              root
Client host:        jfersten-sun
Backup level:       0
S/w compression:    no
Archive created:    Sun Mar 23 10:39:54 2008
Encryption:         off
```

Note: There might be more than one file on the volume. Be sure you are using the correct file number in your restore. In the preceding example, there is only one and it corresponds to the `File Sect` listed. The file number information can also be found in your catalog summary report. Use this file number with the `-F` switch in the `obtar -Gtf` command.

6. This step applies only to Linux and UNIX administrative servers.

   Use either obtool or the Oracle Secure Backup Web tool to browse the newly re-created catalog and restore the items to an alternate directory:

```
ob> set host jfersten-sun
ob> cd /usr/local/oracle/backup
ob> restore admin --aspath /tmp/admin.restored
ob> cd /usr/etc/
ob> restore ob --aspath /tmp/ob.restored
ob> restore -go
Info: 2 catalog restore request items submitted; job id is admin/45.
```

   Note: You absolutely *must* restore the catalog backup to an *alternate* directory. Restoring the catalog backup to its *original* location will leave Oracle Secure Backup configuration in an inconsistent state.

7. This step applies only to Windows administrative servers.

   Load your OSB_CATALOG-MF backup volume into the drive. Ensure you have the correct catalog recovery volume and file number by indexing the tape with obtar, checking the output to confirm that your Oracle Secure Backup catalog data is present on the tape, and checking that you have the correct file number:

```
C:\ >obtar -tf drive_name -F 1 > output_file

C:\ >more output_file
C:/osb/backup/admin/
C:/osb/backup/admin/config/
C:/osb/backup/admin/config/class/
C:/osb/backup/admin/config/class/admin
.
.
.
C:/osb/backup/db/xcr/syssbt@98.1
C:/osb/backup/db/xcr/syssbt@99.1
```

8. This step applies only to Windows administrative servers.

Extract the backup directory to an alternate location:

```
C:\>obtar -xf tape_device -F 1 -s,C:/osb/backup,C:/osb/backup-restored,
```

Caution: The path substitution syntax for obtar (`-s ,P,R,`) replaces prefix P with string R. It is *crucial* that you use a substitution path and restore your catalog recovery files to an alternate directory to avoid overwriting the existing files in your current admin directory. Overwriting the existing files would leave Oracle Secure Backup in an indeterminate state and render it unusable.

9. This step applies only to Windows administrative servers.

   Confirm that your Catalog Recovery files have been properly restored:

```
C:\>cd osb

C:\osb>ls
backup           backup-restored

C:\osb>cd backup-restored

C:\osb\backup-restored>ls
admin  db
```

10. Terminate the observiced process.

    a. On Linux or UNIX, run the following command:

```
# /etc/init.d/observiced stop
```

       Confirm that all `ob` processes have stopped by running the following command:

```
# ps -auwx | grep ob
```

    b. On Windows, run the following command:

```
net stop observiced
```

11. Move the newly restored admin and ob directories into place and re-create the **obfuscated wallet** before restarting observiced. Although the restore process also restores the password-protected encryption **wallet** to the administrative server, for security reasons the obfuscated wallet is not backed up. You must re-create it manually after a restore operation. You must re-create the wallet with the password that was used to create the original encryption wallet. To manually re-create the wallet use the `mkow` command.

    Note: You must know your original keystore password in order to accomplish this task.

    a. On Linux or UNIX:

```
cd /usr/local/oracle/backup
mv admin admin.orig
mv /tmp/admin.restored admin
cd /usr/etc
mv ob ob.orig
```

```
mv /tmp/ob.restored ob
$OSB_HOME/bin/obcm mkow -k  -p wallet_password
Obfuscated wallet has been re-created
/etc/init.d/observiced -start
```

Note: The default OSB_HOME is /usr/local/oracle/backup.

b. On Windows:

```
C:\Program Files\Oracle\Backup> ren admin admin.orig
C:\Program Files\Oracle\Backup> move C:\tmp\admin .
C:\Program Files\Oracle\Backup> ren db db.orig
C:\Program Files\Oracle\Backup> move C:\tmp\db
C:\Program Files\Oracle\Backup\bin\obcm mkow -k -p wallet_password
net start observiced
```

12. The Oracle Secure Backup Web tool is not going to work after the catalog restore operation, and the apache password must be reset. Run the following command to reset the apache webpass:

```
obtool setp daemons/webpass default
```

13. Stop and restart the Oracle Secure Backup daemons.

Your environment is now restored to the point of your last backup of the admin directory. You can use obtool or the Oracle Secure Backup Web tool to review your administrative domain configuration.

A

NDMP Special Characteristics

As an **Oracle Secure Backup user**, you do not have to be aware of **Network Data Management Protocol (NDMP)** in any substantive way except when you use third-party NDMP-enabled appliances. If you use Windows, Linux, or UNIX hosts with secondary storage connected through **Small Computer System Interface (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 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 **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 in which data travels) of a **tape device** to a host in the **administrative domain**.

backup image

The product of a **backup operation**. A single backup image can span more than one **volume** in a **volume set**. The part of a backup image that fits on a single volume is called a **backup section**.

backup image file

The logical container of a **backup image**. A backup image consists of one file. One backup image consists of one or more **backup section**s.

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** by means of 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 in conjunction with **Recovery Manager (RMAN)** to back up the database to tape.

backup piece

A backup file generated by **Recovery Manager (RMAN)**. Backup pieces are stored in a logical container called a backup set.

backup request

An **on-demand backup** that is held locally in **obtool** until you run the `backup` command with the `--go` option. At this point Oracle Secure Backup forwards the requests to the **scheduler**, at which time 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 specific 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 backup**s, 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 is described in a **dataset file**. 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 together 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 that you want 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 as well as permissions 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 in conjunction with some platforms, including NAS devices such as a Network Appliance **filer**.

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 **tape 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 or not they have changed since the last backup.

host

An addressable computer in the network under a specific role.

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 certificate**s, 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**.

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 level**s 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 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** connected to it. A media server is responsible for transferring data to or from the tape devices that are attached to it.

mount mode

The mode indicates the way in which Oracle Secure Backup can use a **volume** physically loaded into a **tape drive**. Valid values are read-only, write/append, overwrite, and not mounted.

NAS

See **Network Attached Storage (NAS)**

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. 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/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 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.

original volume

The **volume** from which a duplicate is made.

originating location

A **location** where a **volume** was first written.

overwrite

The process of replacing a file on your system by restoring a file that has the same file name.

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. Private keys can be used to compute signatures and decrypt data.

privileged backup

File system **backup operation**s 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 in conjunction 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.

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 (observiced) 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 more than one **tape device** 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 backup**s 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)**.

Universal Unique Identifier (UUID)

An identifier used for tagging objects across an Oracle Secure Backup **administrative domain**.

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.

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 single unit of media, such as an 8mm tape. A volume can contain more than one **backup image**.

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 **certificate**s and their associated **public key**/**private key** pair. The contents of the wallet are only available after the wallet password has been supplied, although in the case of 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 of time for which a **volume set** remains open for updates, usually by appending additional **backup image**s. 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

B

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

V

W