Oracle® Secure Backup

Administrator's Guide

Release 10.1

B14234-01

March 2006

Oracle Secure Backup Administrator's Guide, Release 10.1

B14234-01

Contributing Authors: Lance Ashdown, Paul Gavin

Contributors: Tammy Bednar, Michael Chamberlain, Donna Cooksey, Tony Dziedzic, Judy Ferstenberg, George Stabler, Radhika Vullikanti, Joe Wadleigh, Steve Wertheimer

Contents

Part I Oracle Secure Backup Concepts

1 Introduction to Oracle Secure Backup

2 Backup and Restore Concepts

Part IV Managing Operations

9 Managing Devices and Media

10 Performing Maintenance

Part V Advanced Topics

11 Configuring Security: Advanced Topics

12 Using obtar

Preface

This preface contains these topics:

Audience

This book is intended for system administrators and database administrators who perform backup and restore operations. To use this document, you need to be familiar with the operating system environment on which you plan to use Oracle Secure Backup. 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, seven days a week. For TTY support, call 800.446.2398.

Related Documentation

For more information about using Oracle Secure Backup, see the following Oracle resources:

- *Oracle Secure Backup Installation Guide*

  This book explains how to stage and install Oracle Secure Backup.

- *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.

- *Oracle Secure Backup Reference*

This book describes the Oracle Secure Backup command-line interface.

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

- *Oracle Database Backup and Recovery Basics*

  This book provides an overview of backup and recovery and discusses backup and recovery strategies. It provides instructions for basic backup and recovery of your database using Recovery Manager (RMAN).

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

  This guide covers more advanced database backup and recovery topics, including performing user-managed backup and recovery.

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

`http://www.oracle.com/technology/products/backup`

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

`http://www.oracle.com/technology/software`

Conventions

The following conventions are used in this manual:

Convention	Meaning
Bold	Bold typeface indicates components of the Web tool interface, such as buttons, boxes, lists, page names and page subdivisions. Bold typeface also indicates terms that are defined in the text or terms that appear in a glossary, or both.
italic	Italic typeface indicates book titles or emphasis. Italics also indicates variables or placeholders for which you substitute an appropriate value.
`courier`	Courier typeface indicates command line entries, system output display, options and arguments that you enter, executables, filenames, and directory names. When the syntax for a command is given, a bullet offsets the minimal abbreviation for the command, as in `chd•ev`.
[ ]	Brackets enclose optional items from which you can choose one or none.
{}	Required items for which you need to select one of the enclosed values. Each value is separated by a `|`.
|	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options.
. . .	Vertical ellipsis points in an example mean that information not directly related to the example has been omitted.
. . .	Horizontal ellipsis points in statements or commands mean that parts of the statement or command not directly related to the example have been omitted
< >	Angle brackets enclose user-supplied names.

Part I

Oracle Secure Backup Concepts

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

This part contains the following chapters:

1

Introduction to Oracle Secure Backup

This chapter introduces Oracle Secure Backup and describes the basic architecture of an Oracle Secure Backup environment. This chapter contains the following topics:

- What Is Oracle Secure Backup?
- Oracle Secure Backup and NDMP
- Administrative Domains
- Users and Classes

What Is Oracle Secure Backup?

Oracle Secure Backup supplies reliable data protection through file system backup to tape. The Oracle Secure Backup SBT interface enables you to use Recovery Manager (RMAN) to back up Oracle databases. All major tape drives and tape libraries in SAN, Gigabit Ethernet, and SCSI environments are supported.

Oracle Secure Backup Features

Oracle Secure Backup enables you to do the following:

- Centrally manage tape backup and restore operations of distributed, mixed-platform environments (see *Oracle Secure Backup Installation Guide* for supported machine architectures). You can access local and remote file systems and devices from any location in a network without using NFS or CIFS.
- Back up to and restore data from Oracle Cluster File System (OCFS) on Linux and Windows.
- Use wildcards and exclusion lists to specify what you want to back up.
- Perform multilevel incremental backups.
- Duplex database backups so that the same data stream goes to multiple devices. You can specify different media families or devices for each copy of the data.
- Create backups that span multiple volumes.
- Optimize tape resources with automatic 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, SSL is used for authentication and communication between hosts in the administrative domain.

Oracle Secure Backup and Recovery Manager

Recovery Manager (RMAN) is an Oracle Database-specific backup and recovery utility. RMAN is a built-in part of Oracle Database and backs up, restores, and recovers database files regardless of the type of disk storage used for these files.

RMAN knows and applies the complex rules that must be followed to recover Oracle databases. If your database backup strategy needs storage resources other than local disk, then you must use RMAN in conjunction with a general-purpose network backup tool such as Oracle Secure Backup.

Oracle Secure Backup can back up all types of files on the file system. Although Oracle Secure Backup has no specialized knowledge of database backup and recovery algorithms, it can serve as a media management layer for RMAN through the SBT interface. In this capacity, Oracle Secure Backup provides the same services for RMAN as other supported third-party SBT libraries. Oracle Secure Backup is better integrated with Oracle Enterprise Manager, however, than other media managers.

Table 1–1 describes differences between RMAN and Oracle Secure Backup in terms of the type of data backed up and the type of media used for backup storage.

Table 1–1 Differences Between Oracle Secure Backup and RMAN

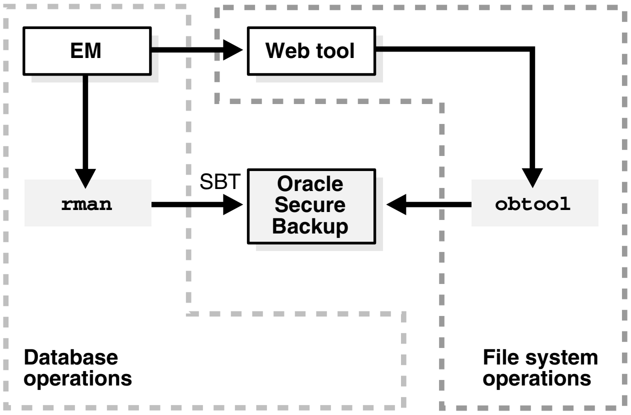
Type of Data	Type of Backup Storage	Oracle Secure Backup Backup and Restore	Recovery Manager Backup and Restore
Oracle datafiles, control files, and archived redo logs	Tape	Yes (only with RMAN)	Yes (only through supported SBT interface)
Oracle datafiles, control files, and archived redo logs	Disk	No	Yes
Non-database files on the file system	Tape	Yes	No
Non-database files on the file system	Disk	No	No

See Also: *Oracle Database Backup and Recovery Basics* to learn about Recovery Manager

Oracle Secure Backup Interfaces

Figure 1–1 shows the interfaces that you can use to access Oracle Secure Backup.

Figure 1–1 Interfaces to Oracle Secure Backup



Users interact with Oracle Secure Backup by means of one of the following tools:

- Oracle Secure Backup Web tool

  The Oracle Secure Backup Web tool is a browser-based GUI that enables you to configure an administrative domain, manage the backup and restore of file system data, and browse the backup catalog.

  The Web tool utilizes an Apache Web server, which runs on the administrative server. As explained in "Using the Web Tool" on page 3-2, you can access the Web tool from any Web browser that can connect to this server.

- Oracle Secure Backup command-line interface (`obtool`)

  Oracle Secure Backup provides a command-line program called `obtool` as an alternative to the Web tool. You can log in to the administrative domain through `obtool` to back up and restore file system data and to perform configuration and administration tasks.

  As explained in "Using obtool" on page 3-8, you can run the `obtool` utility on any host in the administrative domain on which Oracle Secure Backup is installed.

- Oracle Enterprise Manager Database Control and Grid Control

Oracle Enterprise Manager is a set of GUI-based tools for managing the Oracle environment. You can use Enterprise Manager to schedule and perform RMAN backups through the Oracle Secure Backup SBT interface. You can also perform administrative tasks such as managing media and devices within the Oracle Secure Backup administrative domain. The Enterprise Manager console includes a link to the Oracle Secure Backup Web tool.

As explained in "Using Oracle Enterprise Manager" on page 3-8, you can use Enterprise Manager Database Control to back up a database on the administrative server. You can run Enterprise Manager Grid Control on any database host within the administrative domain and use this interface to manage all database backup and restore operations.

- Recovery Manager command-line interface (`rman`)

  You can use the RMAN command-line interface to configure and initiate backup and restore operations that use the Oracle Secure Backup SBT interface. The RMAN utility is located in the `bin` subdirectory of an Oracle home.

  As explained in "Interfaces for Managing Database Backup and Recovery" on page 6-2, you can run the RMAN command-line client on any database host so long as it can connect to the target database. For RMAN to make backups to Oracle Secure Backup, the Oracle Secure Backup SBT library must reside on the same host as the target database.

See Also:

- Chapter 3, "Getting Started" for an orientation to the interfaces to Oracle Secure Backup
- *Oracle Enterprise Manager Administrator's Guide* and the Enterprise Manager online help to learn how to use Enterprise Manager
- *Oracle Secure Backup Reference* to learn about `obtool` commands
- *Oracle Database Backup and Recovery Basics* to learn about the Recovery Manager command-line interface

Oracle Secure Backup and NDMP

The Network Data Management Protocol (NDMP) defines a common architecture for backups of file servers on a network. NDMP specifies the format and means of transmission of messages and payload data. NDMP is an open standard protocol that is promoted and supported by industry vendors.

NDMP enables a centralized backup application, which is called the Data Management Application (DMA), to back up and restore file servers that run on different platforms. NDMP is commonly used by Network Attached Storage (NAS) devices, also known as filers, to perform backup and restore operations without requiring backup software to be installed. This model is different from the classical backup model, which requires the installation of backup software on each host.

The DMA manages backup and restore operations by establishing a TCP/IP-based control connection with an NDMP server. An NDMP server provides NDMP services, which are the NDMP interfaces to the storage devices. The data service transfers data to and from the primary disk storage, whereas the tape service transfers data to and from secondary storage such as a tape drive.

With NDMP, network congestion is minimized because the data path and control path are separated. Data transfer can occur locally—from file servers directly to and from tape drives—while management occurs centrally.

Oracle Secure Backup uses NDMP for data transfer and remote control of tape drives and tape libraries. Thus, Oracle Secure Backup supports devices connected to Windows, Linux, and UNIX hosts with Oracle Secure Backup's internal NDMP server. While Oracle Secure Backup leverages NDMP, it is transparent to users except when backing up a NAS device that requires NDMP for optimal backup operations.

In addition to Windows, Linux, and UNIX hosts, Oracle Secure Backup supports special-purpose appliances such as Network Appliance filers, Mirapoint message servers, and DinoStor tape appliances. These appliances can be backed up locally or remotely, but cannot perform the role of Oracle Secure Backup administrative server because backup software cannot be installed on them.

Although Oracle Secure Backup uses NDMP, specific NAS devices utilizing NDMP must still be tested and supported by Oracle Secure Backup. Refer to the device matrix at the following URL for a list of supported NAS devices:

`http://www.oracle.com/technology/products/backup/`

See Also:

- `http://www.ndmp.org` to learn more about NDMP
- Appendix A, "NDMP Usage Notes"

Administrative Domains

An administrative domain is a network of hosts that you manage as a common unit to perform backup and restore operations. To configure Oracle Secure Backup, you need to assign roles to each host in the domain. A single host can have one or more of the following roles:

- Administrative server

  You can assign this role to a host in your administrative domain that contains a copy of Oracle Secure Backup software. The administrative server maintains the configuration data and catalogs for the domain (see "Administrative Data" on page 1-7). An administrative domain has one and only one administrative server.

  The administrative server runs the Oracle Secure Backup scheduler, which starts and monitors backup and restore jobs within the administrative domain. You choose your administrative server when you install Oracle Secure Backup. Note that the administrative server can co-reside on a host with other applications or function as a dedicated, single-purpose server.

- Media server

  You can assign this role to a host that has one or more secondary storage devices, such as tape libraries or tape drives, connected to it. An administrative domain has one or more media servers.

- Client

  You can assign this role to a host whose locally-accessed data is backed up by Oracle Secure Backup. An administrative domain has one or more client hosts. Most hosts defined within the administrative domain are clients.

Figure 1–2 illustrates a sample Oracle Secure Backup administrative domain. In this scenario, the domain includes five hosts: an administrative server, a media server with attached tape library, and three clients. Two of the clients run Oracle databases; the other client is a NAS appliance.

Figure 1–2 Administrative Domain with Five Hosts

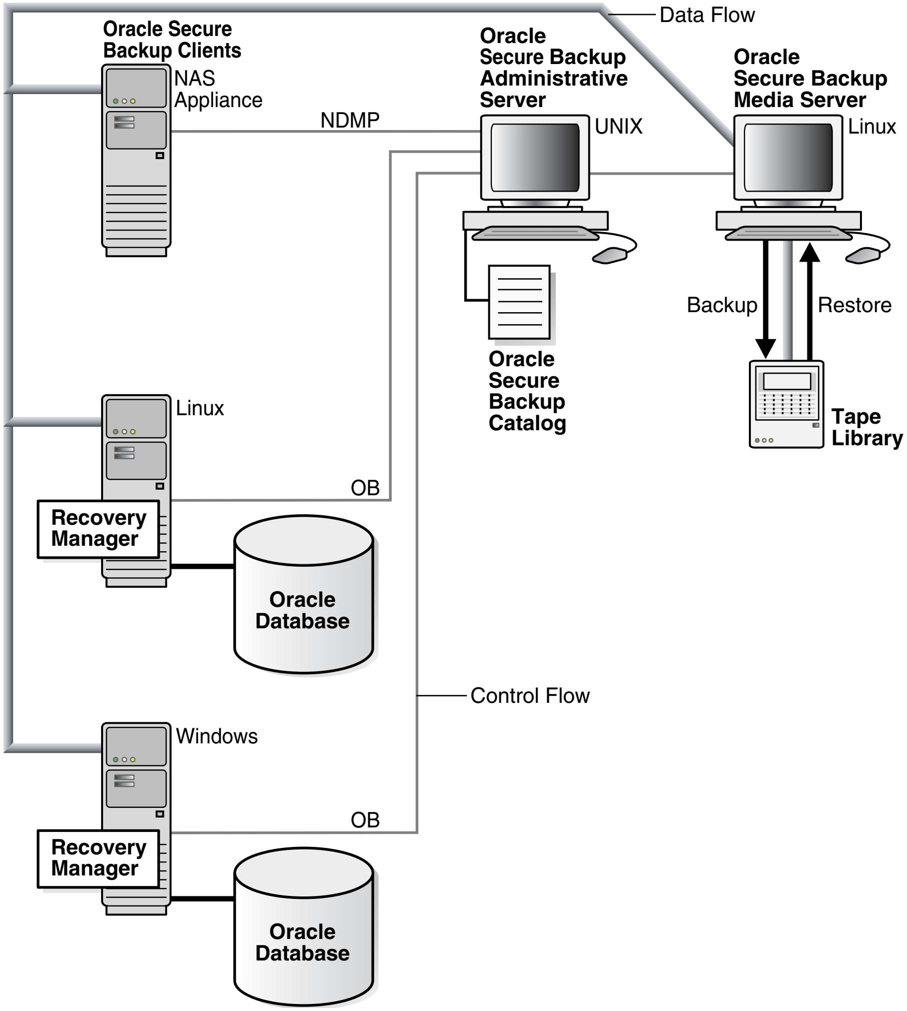
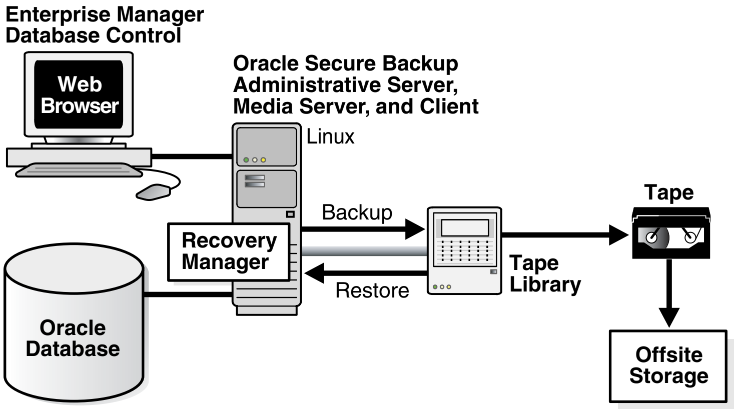


Figure 1–3 illustrates a different Oracle Secure Backup administrative domain that contains a single Linux host. This host assumes the roles of administrative server, media server, and client. The host runs an Oracle database and has a tape library locally attached.

Figure 1–3 Administrative Domain with One Host


Enterprise Manager Database Control
Web Browser
Oracle Secure Backup Administrative Server, Media Server, and Client
Linux
Backup
Recovery Manager
Restore
Tape
Tape Library
Oracle Database
Offsite Storage

Host Access Modes

Communications with a host in an administrative domain occur through one of the following access modes:

- Primary

  In primary access mode, Oracle Secure Backup is installed on a host. The programming components of Oracle Secure Backup are running in the background as daemons. The daemons actively participate in managing backup and restore operations. Typically, an Oracle database resides on a host accessed through this mode.

- NDMP

  An NDMP host is a storage appliance from third-party vendors such as Network Appliance, Mirapoint, or DinoStor. An NDMP host uses a vendor-specific implementation of the NDMP protocol to back up and restore file systems. Oracle Secure Backup software is not installed on an NDMP host, but is accessible to Oracle Secure Backup through NDMP.

In Example 1–1, the `lshost` command in `obtool` displays the hosts in an administrative domain. The command indicates the access mode of each host—NDMP or primary (`ob`)—in parentheses.

Example 1–1 Host Access Modes

```
ob> lshost
br_filer        client                      (via NDMP) in service
stadv07         admin,mediaserver,client    (via OB)   in service
```

As explained in "Oracle Secure Backup and NDMP" on page 1-4, Oracle Secure Backup uses NDMP for data transfer among hosts regardless of whether a host is accessed through the primary or NDMP modes. For example, a Windows administrative server uses NDMP to exchange data with a NetApp filer and a Linux client.

See Also:

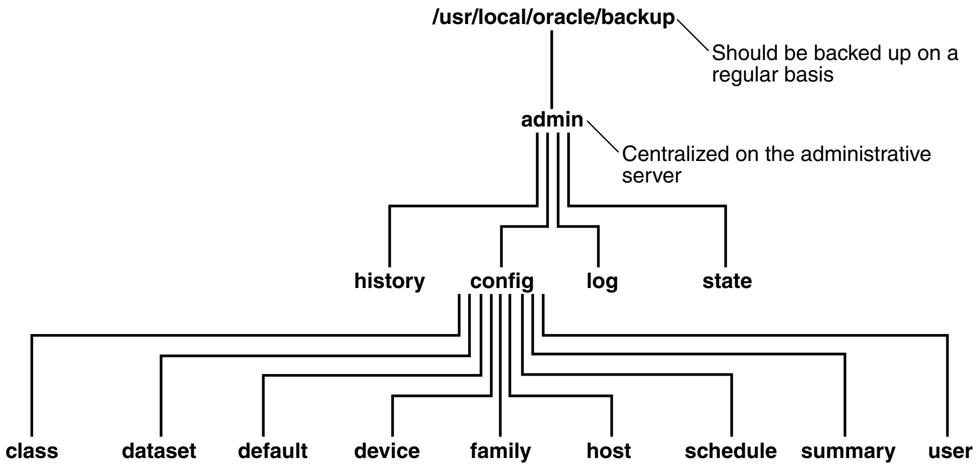
- "Configuring Hosts" on page 4-6
- *Oracle Secure Backup Reference* to learn about the `obtool` host commands

Administrative Data

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 1–4 shows the directory structure of an Oracle Secure Backup home. This directory structure is the same for all platforms, but the default home is `/usr/local/oracle/backup` for UNIX and Linux and `C:\Program Files\Oracle\Backup` for Windows.

Figure 1–4 Directories on the Administrative Server



The administrative data includes configuration data about domain-wide entities such as classes, devices, media families, and so on. As shown in Figure 1–4, `config` 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 also maintains backup sections, backup pieces, and volumes catalogs in the `admin/state/general` subdirectory.

The Web tool and `obtool` are the interfaces by which you access catalogs and configuration data. Only in exceptional circumstances do you access the administrative data directly on the file system.

> **See Also:** *Oracle Secure Backup Installation Guide* to learn more about the files and directories in the Oracle Secure Backup home

Users and Classes

This section explains the concept of an Oracle Secure Backup user, which is a domain-wide identity. A class is a named collection of rights assigned to this user.

Oracle Secure Backup Users and Passwords

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

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

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 muthu, and if an Oracle Secure Backup user in the domain is named muthu, these accounts are separately managed even though the name is the same. For convenience, you may 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 UNIX and Windows accounts. These accounts are used for unprivileged backup, that is, backups that do not run with root privileges. In contrast, privileged backup and restore operations run on a client with root (UNIX) or Local System (Windows) permissions.

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 domain, the jobs run 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.

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

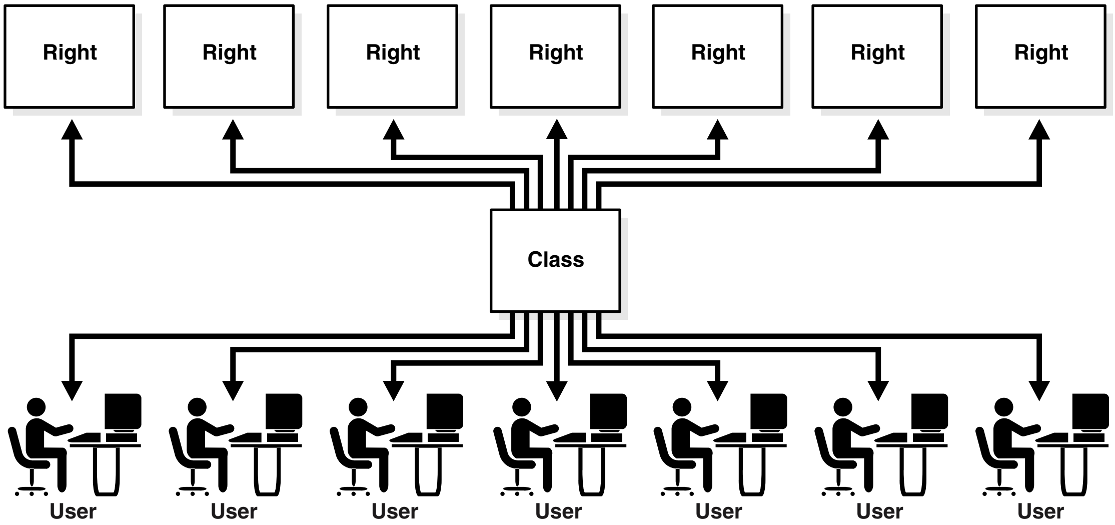
You can configure user access to NDMP hosts when setting up an Oracle Secure Backup user account. Passwords for NDMP hosts are associated with the host instead of the user. You can configure the host to use the default NDMP password, a user-defined text password, or a null password. You can also configure a password authentication method such as text or MD5-encrypted.

See Also: "Adding a Host" on page 4-8 to learn how to add an NDMP host to an administrative domain

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 UNIX group, but it defines a finer granularity of access rights tailored to the needs of Oracle Secure Backup. As shown in Figure 1–5, you can assign multiple users to a class, each of whom is a member of only one class.

Figure 1–5 Classes and Rights



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

- `admin`

  This class is used for overall administration of a domain. The `admin` class has all the rights needed to modify 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 user to query the state of all primary and secondary storage devices and to control the state of these devices.

- `oracle`

  This class, which is similar to the `operator` class, has rights enabling users to modify Oracle database configuration settings as well as to perform Oracle database backups. Typically, class members are Oracle Secure Backup users that are mapped to operating system accounts of Oracle database installations.

- `user`

  This class is assigned to specific users and gives them permission to interact in a limited way with their domains. This class is reserved for users who need to browse their own data within the Oracle Secure Backup catalog and perform user-based restore operations.

- `reader`

  This class enables Oracle Secure Backup users to browse the catalog. Readers are only permitted to modify the given name and password for their Oracle Secure Backup user accounts.

See Also:

- "Configuring Classes" on page 4-24 for a detailed description of the rights available to each class
- *Oracle Secure Backup Reference* to learn about the `obtool` user and class commands
- *Oracle Secure Backup Reference* to learn about the rights in the default classes

2

Backup and Restore Concepts

This chapter explains the fundamental concepts involved in Oracle Secure Backup backup and restore operations. This chapter contains the following topics:

- File System Backup and Restore
- Database Backup and Recovery
- Jobs and Requests
- Tape Devices
- Backup Images and Media
- Daemons and Services
- Defaults and Policies
- Network Backup Security

> **See Also:** *Oracle Secure Backup Reference* for details on using the Oracle Secure Backup command-line interface

File System Backup and Restore

This section describes how Oracle Secure Backup can back up and restore the file system. It contains the following sections:

- File System Backups
- Backup Datasets
- Scheduled and On-Demand Backups
- Restartable Backups
- Backup Catalog
- File System Restore Operations

File System Backups

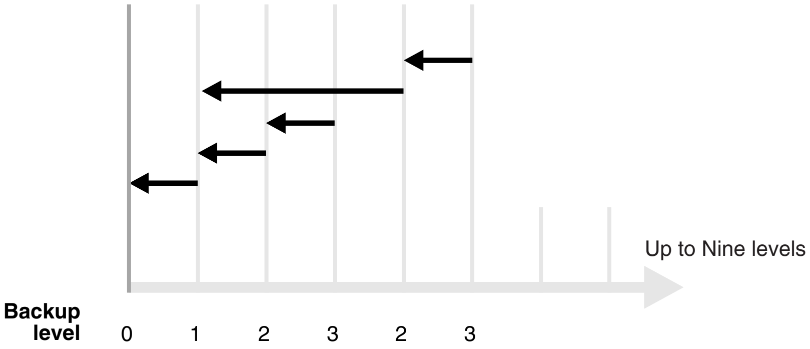
File system data can be defined as the collection of files and file management structures on physical or logical storage. Oracle Secure Backup can back up all types of files on the file system to tape. For example, you can use Oracle Secure Backup to back up the root directory on a host or an Oracle Database home. Backups that you initiate through Oracle Secure Backup are called file system backups.

Full and Incremental File System Backups

A full backup backs up all specified files, regardless of when they were last backed up. This option is the same as an incremental backup at level 0. You can use a level 0 backup as the base of an incremental backup strategy.

Oracle Secure Backup supports 9 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 lower (numerical) 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 2–1 shows a series of cumulative backups.

Figure 2–1 Cumulative Incremental Backups



In a differential incremental backup, Oracle Secure Backup back 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 NAS devices such as Network Appliance filers.

Oracle Secure Backup includes an offsite 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 offsite storage without disturbing your schedule of incremental backups.

See Also:

- "Choosing a Backup Schedule" on page 7-3
- *Oracle Secure Backup Reference* for a description of the obtool backup commands

Backup Datasets

A dataset file defines the file system data that Oracle Secure Backup should include in and exclude 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 2–1 instructs Oracle Secure Backup to back up the directory /usr1/home on brhost2 (except for the directories /usr1/home/temp and /usr1/home/oldfiles) and the directory /usr2/home.

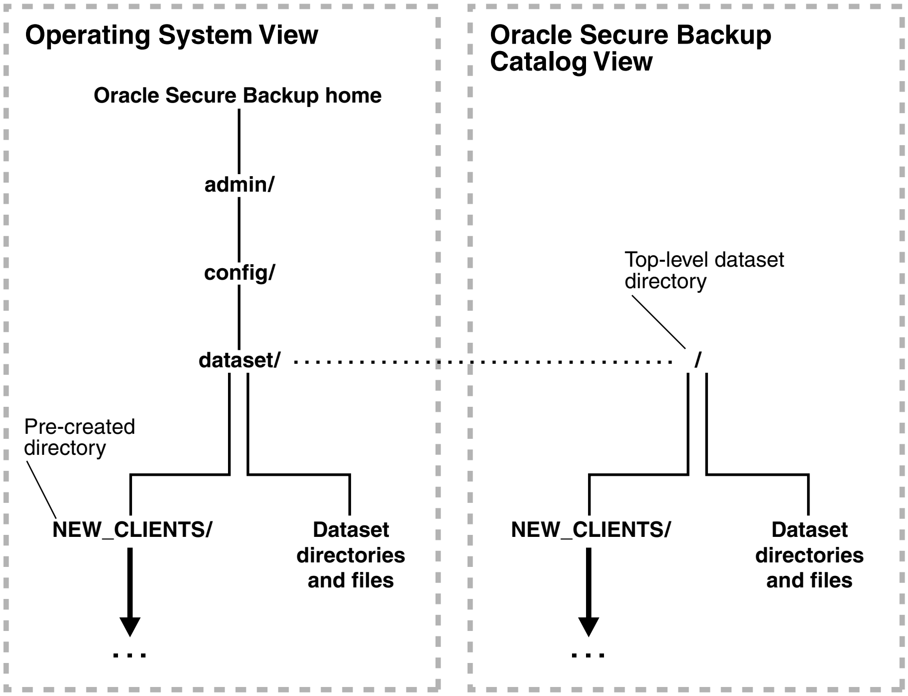
Example 2–1 Sample Dataset File

```
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 2–2, you can view this structure from the perspective of the operating system or the Oracle Secure Backup catalog.

Figure 2–2 Dataset Directories and Files


Operating System View
Oracle Secure Backup home
admin/
config/
dataset/
Pre-created directory
NEW_CLIENTS/
Dataset directories and files
. . .
Oracle Secure Backup Catalog View
Top-level dataset directory
/
NEW_CLIENTS/
Dataset directories and files
. . .

From the operating system point of view, the 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 2–2, the `NEW_CLIENTS` directory is automatically created during installation. You can use this directory to store your dataset files.

With either `obtool` or the Web tool, you can execute commands to manage dataset files and directories. You can create your own dataset directories and files and organize them into a tree-like structure. As shown in Figure 2–2, the `admin/config/dataset/` subdirectory on the operating system corresponds to the top-level dataset directory in the Oracle Secure Backup catalog.

See Also:

- *Oracle Secure Backup Reference* for a description of the Oracle Secure Backup dataset language
- *Oracle Secure Backup Reference* for a description of the `obtool` dataset commands

Scheduled and On-Demand Backups

You can create the following types of file system backup requests with Oracle Secure Backup:

- Scheduled

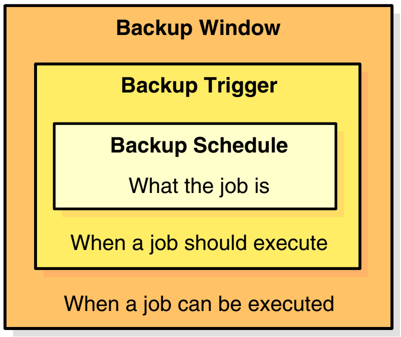
  In backups of this type, you instruct Oracle Secure Backup to make backups according to a backup schedule, which specifies the datasets for the backup. A trigger defined in the schedule specifies when the job should execute. For example, you can instruct Oracle Secure Backup to back up the `/home` directory on client host `brhost2` every Sunday. Note that jobs scheduled from different time zones will be synchronized with one another.

- On-demand

In backups of this type, you instruct Oracle Secure Backup to perform an ad hoc or one-time-only backup of the specified data. For example, you may instruct Oracle Secure Backup to back up the Oracle home on client host `brhost2`.

As shown in Figure 2–3, the execution of scheduled backup jobs 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 2–3 Backup Windows and Scheduled Backups



A single backup window can apply to all days of the week or only to specific days or dates. If the backup window is closed, or if no backup window is defined, then scheduled backups will not run, although you can still run on-demand backups.

> **Note:** If a job is running when the backup window closes, then it will continue to completion.

The default backup window is daily 00:00-24:00. For an example of how backup windows affect scheduled backups, assume that your only backup window opens daily from midnight to 2 a.m. If the backup schedule trigger fires at 3 a.m., then the backup will never run.

> **See Also:** "On-Demand Backup Work Flow" on page 7-21 and "About Backup Schedules" on page 7-12

Privileged and Unprivileged Backups

When you use the Web tool or the `backup` command in `obtool` to initiate an on-demand backup, the backup runs in unprivileged or privileged mode.

As explained in "Oracle Secure Backup Users and Passwords" on page 1-8, an unprivileged backup runs under the Linux/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/UNIX or Windows account.

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.

If you create a scheduled backup job, then it runs with the privileges of the Oracle Secure Backup scheduler, that is, as `root` on Linux and UNIX and as `Local System` on Windows.

Restartable Backups

If a file system backup fails due to an unexpected event like a network failure, power outage, unexpected system shutdown, tape media error, and so on, 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 is meets the following conditions:

- The backup client is a Network Appliance filer running Data ONTAP 6.4 or later.
- The backup image is saved to a tape drive controlled by a server that uses NDMP version 3 or later.
- The `restartablebackups` policy in the `operations` class is enabled (the default).
- 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 at least 1 GB of free space.

At the beginning of each backup job, Oracle Secure Backup automatically determines whether the backup can be restarted from a midpoint. If so, it 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. Upon finding a restartable job, the scheduler restarts it and uses the same volume and drive in the same library in use when the interruption occurred.

See Also: "Managing Checkpoints" on page 10-12

Backup Catalog

As explained in "Administrative Data" on page 1-7, the administrative server maintains a catalog in which it stores metadata relating to backup and restore operations for the administrative domain. You can use `obtool` or the Web tool to browse the catalog to determine what you have backed up.

> **Note:** The Oracle Secure Backup catalog is integrated to share backup metadata with RMAN, but is separate from the RMAN recovery catalog. The recovery catalog is stored in an Oracle database and is maintained independently by RMAN.

When Oracle Secure Backup performs a file system backup or a database backup through the SBT interface (see "Database Backups" on page 2-10), it records the name and attributes of the objects it backs up. It writes this data to the catalog stored on the administrative server.

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 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. "Oracle Secure Backup Classes and Rights" on page 1-9 explains 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.

Note the following features of the catalog super-directory:

- On UNIX and Linux systems, it usually contains only the root directory, / (slash).
- On Windows systems, it contains each top-level file system—identified by a drive letter and a colon—that you backed up.

The Oracle Secure Backup catalog contains a record of each file system object saved in each backup. So, what you would normally consider a two-dimensional representation of a file system—the inverted naming tree—now includes a third dimension, time.

Directory contents change over time; in fact, the very existence of directories is transient. The name of an object backed up yesterday as a directory may, in today's backup, refer to a file, and in tomorrow's backup, a symbolic link. 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: the data selector and the view mode.

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 2–1. The data selector describes, either explicitly or by inference, the identity of each backup image section containing the data of interest. "Backup Images and Media" on page 2-18 explains backup images and sections.

Table 2–1 Data Selectors

Selector	Description
latest	Shows most recent file system objects.
earliest	Shows least recent file system objects.
all	Shows all instances of file system objects.
backup-id	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	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 explanation of data selectors

Using Data Selectors: Example 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 2–2 shows the files that are backed up as well as the volume and image file to which they are written.

Table 2–2 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

In Table 2–2, the May 3 backup filled a tape while writing `file2.dat`. Oracle Secure Backup continued the backup on volume `FULL-04` by writing the remainder of `file2.dat`, followed by `file4.dat`. Table 2–3 describes the effect of various data selectors on the file system object references.

Table 2–3 Data Selectors for Backups of the /numbers Directory

This data selector	and this reference	selects the data backed up in these backup image sections (backup ids)
latest	`/numbers/file4.dat`	FULL-04, file 3, section 2 (46)
	`/numbers/file2.dat`	FULL-03, file 3, section 1 (40) and FULL-04, file 3, section 2 (46)
	`/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)
	`/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)
	`/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)
	`/numbers`	FULL-02, file 5 (20) and FULL-02, file 9 (30)
05/05	`/numbers/file1.dat`	(none)
	`/numbers`	FULL-02, file 9 (30)
05/04-05/05	`/numbers/file4.dat`	(none)
	`/numbers/file1.dat`	FULL-02, file 5 (20)
	`/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 and exact.

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, in "Using Data Selectors: Example" on page 2-8, a listing of the `/numbers` directory 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

When you browse a directory in exact mode, you display only the contents of a directory identified by the data selector. Assume that in "Using Data Selectors: Example" on page 2-8 you set the view mode to exact. In this case, the `latest` setting in Table 2–3 would display only `file1.dat`, `file2.dat`, and `file4.dat`.

File System Restore Operations

Restoring to the file system with Oracle Secure Backup is essentially the reverse of backing up to the file system. Normally, restore operations are additive. In other words, each file and directory restored from a full or an incremental backup is added to its destination directory.

Note the following differences between backup and restore operations:

- Whereas file system backups are either scheduled or on-demand (see "Scheduled and On-Demand Backups" on page 2-4), all restore operations are on-demand.
- Whereas some file system backups are restartable (see "Restartable Backups" on page 2-6), no restore operations are restartable.
- File system backups use datasets to specify data (see "Backup Datasets" on page 2-3), whereas restore operations use one of the methods described in the following section.

File System Restore Methods

With Oracle Secure Backup, you can restore data in the following ways:

- Catalog-based restore operation

  In this type of restore operation, you browse the catalog for the file system objects to be restored. When you have located their names and selected the instances, you can restore the objects.

  "Performing a Catalog-Based Restore Operation" on page 8-3 explains how to restore data with a catalog.

- Raw restore operation

  In this type of restore operation, you must have independent knowledge of the secondary storage location (volume ID and backup image file number) of a backup. You can either restore all data in the backup or specify an individual file or directory.

  "Performing a Raw Restore Operation" on page 8-8 explains how to restore data without using a catalog.

- `obtar` restore operation

  You can use the obtar command-line interface to operate directly on tape drives, outside the purview of the Oracle Secure Backup scheduler. The `obtar` utility is intended for advanced users only.

  See Also:

  - "Backup Catalog" on page 2-6 for an overview of the Oracle Secure Backup catalog
  - "Volumes" on page 2-20 for an explanation of volume IDs and backup images
  - Chapter 12, "Using obtar" to learn how to use `obtar`

Database Backup and Recovery

This section describes concepts relating to restore operations in Oracle Secure Backup.

Database Backups

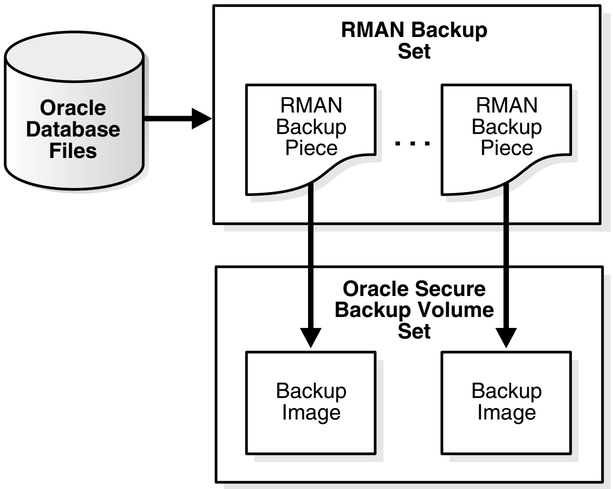
RMAN is a database utility that enables you to back up an Oracle database. Oracle Secure Backup supplies an SBT interface that RMAN can use to back up database files to tape. An SBT backup initiated by RMAN is distinct from a file system backup, which is a scheduled or on-demand backup of any files on the file system (not just database files) initiated by Oracle Secure Backup.

Backup Sets and Backup Images

The backup of an Oracle database performed with RMAN results in a backup set, which is a logical grouping of backup pieces. Backup pieces are physical files.

When you use Oracle Secure Backup to store database backups on tape, each backup piece is created as one backup image. Figure 2–4 illustrates the relationship between pieces and images. As explained in "Volume Sets" on page 2-21, a single backup image can span multiple tapes.

Figure 2–4 Backup Sets and Backup Images



Oracle Secure Backup can mix RMAN backup pieces and file system backup sections within the same volume set and even on the same volume.

Database Backup Storage Selectors

Oracle Secure Backup uses information encapsulated in database backup storage selectors to interact with RMAN when performing backup and restore operations. Oracle Secure Backup maintains storage selectors in the `admin/ssel` subdirectory of the Oracle Secure Backup home on the administrative server.

Database backup storage selectors contain backup and restore attributes that describe an Oracle database. For example, the storage selector identifies a database by name or DBID (unique numerical identifier), the host on which it resides, and the media family to use when backing it up. Storage selectors act as a layer between RMAN, which backs up and restore the database, and the Oracle Secure Backup software, which manages the underlying media.

When performing an Oracle database backup to devices and media managed by Oracle Secure Backup, 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 informs Oracle Secure Backup what devices, if any, to restrict this backup to and which media family (if any) to use.

See Also:

- "Creating a Database Backup Storage Selector" on page 6-12
- *Oracle Secure Backup Reference* to learn about database backup storage selector commands in `obtool`

Database Restore and Recovery

Restore operations that you initiate through RMAN are called Oracle Database restore operations. You can use the Oracle Secure Backup SBT interface in conjunction with RMAN to restore database files to tape. As explained in "Database Backup Storage Selectors" on page 2-11, Oracle Secure Backup uses information encapsulated in storage selectors to interact with RMAN when performing restore operations.

See Also:

- "Performing Recovery with RMAN and Oracle Secure Backup" on page 6-16
- *Oracle Secure Backup Reference* to learn about the `obtool` host commands

Jobs and Requests

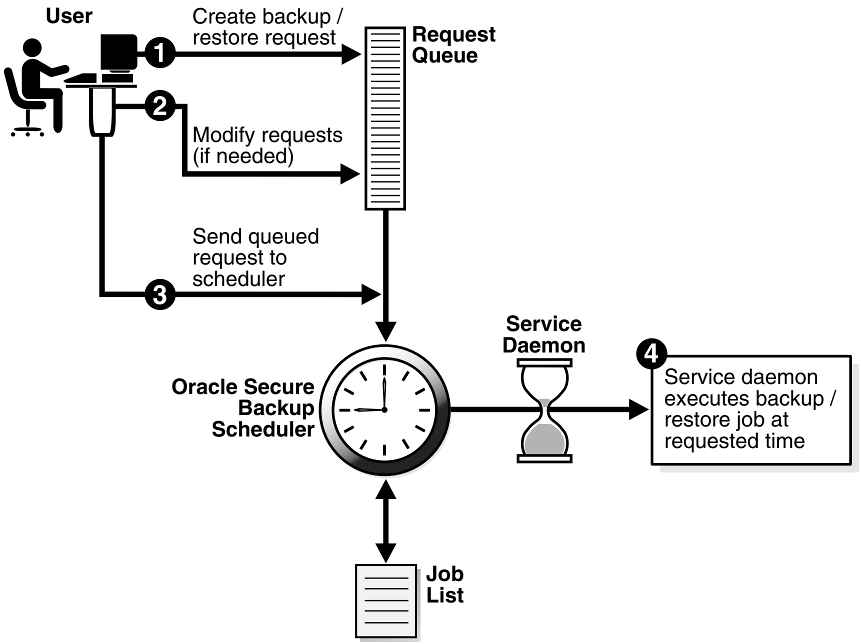
In Oracle Secure Backup, a backup or restore request is distinct from a job. A request is a locally-stored specification of a backup or restore operation that is not yet eligible to run. A job is a request that has been forwarded to the Oracle Secure Backup scheduler and is eligible to be run.

The scheduler policies, which are described in "Defaults and Policies" on page 2-30, 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 6-5.

Figure 2–5 shows the process by which a user can create an on-demand backup or restore job. "Scheduled and On-Demand Backups" on page 2-4 explains the difference between on-demand and scheduled backups.

Figure 2–5 Backup and Restore Requests and Jobs


User
1
Create backup / restore request
Request Queue
2
Modify requests (if needed)
3
Send queued request to scheduler
Service Daemon
4
Service daemon executes backup / restore job at requested time
Oracle Secure Backup Scheduler
Job List

The steps in the process illustrated in Figure 2–5 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 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 executes 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:

- At the beginning of the day, Oracle Secure Backup inspects the triggers defined in each backup schedule. Schedules and triggers are described in "Scheduled and

On-Demand Backups" on page 2-4. For each trigger that fires that day, Oracle Secure Backup creates one new job for each dataset listed in the schedule.

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 use the **Go** button or 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 user who executes 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 use the **Go** button or 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 execute a job has arrived, the foremost decision criterion that the scheduler uses to execute 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 execution, then Oracle Secure Backup executes the job with the lowest numeric schedule priority.

See Also: "Performing On-Demand File System Backups" on page 7-20 and "Configuring Backup Schedules" on page 7-12

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 Web tool and `obtool`.

See Also: "Displaying Job Properties" on page 10-4

Job Transcripts

Oracle Secure Backup maintains a running transcript for each job. The transcript describes the details of the job's operation. Oracle Secure Backup creates this transcript when dispatching the job for the first time and updates it as the job progresses. When a job requires operator assistance, Oracle Secure Backup prompts for assistance using the transcript.

See Also: "Displaying Job Transcripts" on page 10-4

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 emailed
- 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 5-8

Tape Devices

Oracle Secure Backup maintains information about tape libraries and tape drives so that you can use them for local and network backup and restore operations. You can configure devices during installation or add a new device to an existing administrative domain. When configuring devices, the basic task is to inform Oracle Secure Backup about the existence of a device and then specify which media server can communicate with this device.

This section contains the following topics:

- Tape Drives
- Tape Libraries
- Device Names and Attachments

Tape Drives

A tape drive is a device that uses precisely-controlled motors to wind a tape from one reel to the other. The tape passes a read/write head as it winds. Most magnetic tape systems use small reels that are fixed inside a cartridge to protect the tape and make handling of the tape easier.

A magnetic cassette or tape is sequential-access storage. It has a beginning and an end, which means that to access data in the middle of the tape, a device must read through the beginning part of the tape until it locates the desired data. Data must be read in this way because the tape heads are stationary.

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

Every tape drive supports a specific tape format. Common tape formats include the following:

- 8mm
- 4mm, or Digital Audio Tape (DAT)
- Advanced Intelligent Tape (AIT)
- Digital Data Storage (DDS)
- Digital Linear Tape (DLT) and Super DLT (SDLT)
- Linear Tape-Open (LTO), an open alternative to the proprietary DLT format

Oracle Secure Backup supports a number of different tape devices. Refer to the following URL for a list of supported tape drives and libraries:

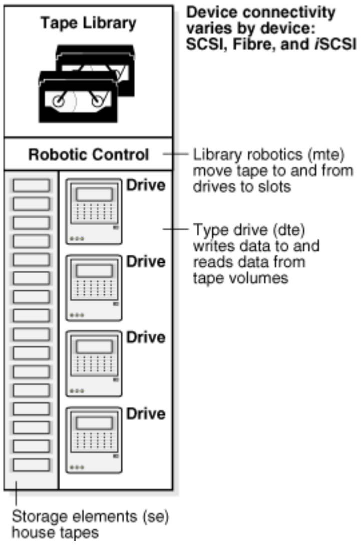
http://www.oracle.com/technology/products/backup

Tape Libraries

A tape library is a robotic storage device that accepts SCSI commands to move media between storage locations and tape drives. A library is often referred to as a robotic tape device, autochanger, or medium changer.

A library contains one or more tape drives, a number of slots to hold tape cartridges, and an automated method for loading tapes. Figure 2–6 illustrates a tape library that contains four tape drives.

Figure 2–6 Tape Library


Tape Library
Device connectivity varies by device: SCSI, Fibre, and *i*SCSI
Robotic Control
Library robotics (mte) move tape to and from drives to slots
Drive
Type drive (dte) writes data to and reads data from tape volumes
Drive
Drive
Drive
Storage elements (se) house tapes

Oracle Secure Backup automates the management of tape libraries, thereby enabling efficient and reliable use of their capabilities. Oracle Secure Backup controls the library robotics so that tapes can be managed easily.

Oracle Secure Backup supports the following features of tape libraries:

- Automatic loading and unloading of volumes

  When you add a tape library to your administrative domain, the device is configured in automount mode by default. In this mode, Oracle Secure Backup sends commands to the robotic arm of the library to mount tapes for backup and restore operations. When a new volume is needed, Oracle Secure Backup scans the volumes in the library until it finds a suitable volume. If sufficient eligible tapes are contained in the library storage elements, then no operator intervention is required to load the volumes needed to store the complete backup image.

- Barcode readers

  A barcode is a symbol code that is physically applied to volumes for identification purposes. Some libraries have an automated barcode reader. Oracle Secure Backup can use barcodes to identify tapes in a tape library.

- Automatically cleaning tape drives in a tape library

  Oracle Secure Backup checks for cleaning requirements when a tape is loaded into or unloaded from a tape drive. If a cleaning is required, then Oracle Secure Backup loads a cleaning cartridge, waits for the cleaning cycle to complete, replaces the cleaning cartridge in its original storage element, and continues with the requested load or unload. You can also schedule a cleaning interval.

Library Elements

As shown in Figure 2–6, a library consists of a set of addressable elements, each of which can contain a tape or can be used to move a tape. Libraries can contain the following types of elements:

- Storage Element (SE)

  This element is an internal slot in a library in which a tape cartridge can reside.

- Data Transfer Element (DTE)

  This element represents a device capable of reading or writing the physical volume. Typically, a DTE is a tape drive used to backup or restore data on a tape.

- Medium Transport Element (MTE)

  This element represents the robotics mechanism used to move media between other elements in the library. Typically, an MTE is a robot arm that moves tape cartridges from library slots to tape drives.

- Import/Export Element (IEE)

  This is an element by which media can be imported to and exported from the library. Typically, an IEE is a door-like mechanism that operators use to transfer tapes into and out of the library. After the door is closed, the robotic arm transfers cartridges to internal slots in the library. Because the library itself is not opened during this procedure, a re-inventory is not required.

Many of the Oracle Secure Backup library commands require you to specify one or more library elements, in particular, storage elements and import/export elements. Except in the inventory display, media transport elements are never referenced. Data transfer elements are referenced only in the inventory display and indirectly by the drive (if any) that you select for an operation.

Oracle Secure Backup refers to elements by their abbreviation (`mte`, `se`, `iee`, or `dte`) followed by the number of the element, for example, `se5`, `iee2`, `dte1`. When there is more than one element of a particular type, element numbering starts at 1. When there is only one element of a type, the number can be omitted: `iee1` and `iee` both refer to the first and only import export element. If the abbreviation is omitted, then a storage element is assumed. For example, `se4` and `4` both refer to the fourth storage element. For some commands, you can specify a range of storage elements, for example, `1-5`.

Library Operations

Oracle Secure Backup supports a number of library operations. The following operations are the most basic:

- Inserting and extracting volumes

  If you manually place volumes into library storage elements, then use the `insertvol` command to notify Oracle Secure Backup of these volumes, their locations and their properties. Similarly, you can use the `extractvol` command to indicate that you are removing a volume manually from the library.

- Loading and unloading volumes

  You can use the `loadvol` command to instruct the tape library to load a volume from a storage element into a tape drive in preparation for a backup. For example, you can instruct the library to load the tape in slot 3 into the drive named `tape1`. You can also use the `unloadvol` command to instruct the tape library to unload a volume from a tape drive to a particular storage element.

- Moving volumes

  You can use the `movevol` command to move a volume from one storage element to another storage element. For example, you can instruct the library to move a tape from storage element 3 to 1.

- Importing and exporting volumes

  If the tape library has an import/export element and supports the `opendoor` command to open the import/export door of a tape library, then you can use this method to transfer tapes into and out of the tape library. You can use the `importvol` command to move volumes to internal slots in the library and the `exportvol` command to move volumes out of the tape library.

See Also:

- "Executing Library Commands" on page 9-5 for a complete list of supported library commands
- *Oracle Secure Backup Reference* for a description of the library commands that you can execute in `obtool`

Device Names and Attachments

Each tape device is uniquely identified within Oracle Secure Backup by a user-defined name. Because Oracle Secure Backup manages tape drive operations, it must be able to identify the drive as well as determine whether the drive is housed in a library. Oracle Secure Backup must further determine which storage elements are available for storing tapes while not in use by the drive.

Oracle Secure Backup distinguishes a device and the means by which the device is connected to a host. To be usable by Oracle Secure Backup, each device must have at least one attachment, which describes a data path between a host and the device itself. Typically, an attachment includes the identity of a host plus a UNIX device special file name, a Windows device name, or NAS device name. In rare cases, additional information is needed for the attachment definition.

SAN-attached devices often have multiple attachments, one for each host with local access to the device through its Fibre Channel interface. SAN-attached devices are also distinguished by a World Wide Name (WWN), an internal identifier that uniquely names the device on the SAN. Systems such as Network Appliance filers permit access to SAN-attached devices through their WWN; for such systems, Oracle Secure Backup includes a reference to the WWN in the device attachment's raw device name.

Devices such as certain Quantum and SpectraLogic tape libraries appear to be connected directly to an Ethernet LAN segment and accessed through NDMP. In fact, Oracle Secure Backup views these devices as having two discrete components:

- A host, which defines the IP address and which you configure through the Web tool Hosts page or the `obtool mkhost` command
- A device, which has one attachment to the single-purpose host that serves as the front end for the device

Devices such as DinoStor TapeServer use a single host to service multiple devices.

For NDMP servers that run version 2, other data may be required to define SCSI parameters needed to access the device. These parameters are sent in an NDMP message called `NDMP_SCSI_SET_TARGET`. Oracle Secure Backup NDMP servers do not use this data or this message.

See Also:

- "Configuring Tape Devices" on page 4-14 to learn how to configure devices
- The description of the `mkdev` command *aspec* placeholder, which describes the syntax and naming conventions for device attachments

Backup Images and Media

To understand Oracle Secure Backup, you need to understand the relationship between the physical backup files and the media on which those files are stored.

Figure 2–7 provides a graphical illustration of how backup files are related to volumes. The concepts are as follows:

- 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.
- A volume is a single unit of media, such as an 8mm tape.

Figure 2–7 Backup Images, Backup Sections, and Volumes

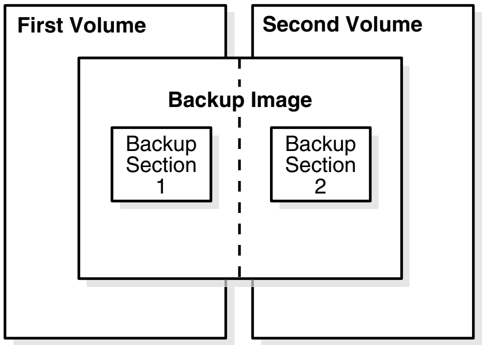
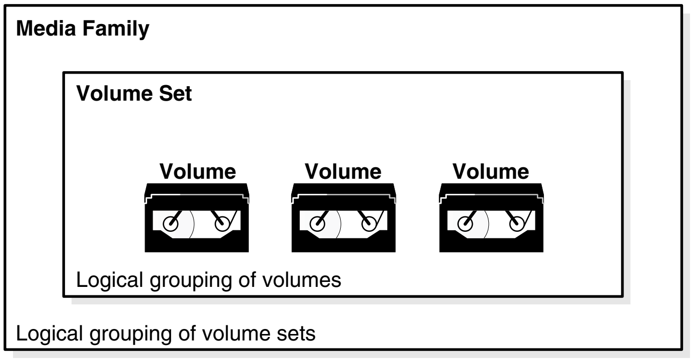


Figure 2–8 provides a graphical illustration of how a volume set is related to a media family. The concepts are as follows:

- A volume set is a logical grouping of one or more physical volumes spanned by a backup image. As shown in Figure 2–7, a backup section is the part of a backup image that fits on a single volume.
- 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 2–8 Volumes, Volume Sets, and Media Families

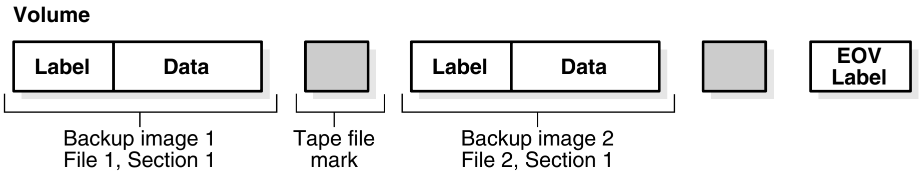


When you back up files with Oracle Secure Backup, you generate a volume set that has some common characteristics defined by the corresponding media family associated with your backup.

Backup Images and Sections

When you execute a backup in Oracle Secure Backup, you generate a backup image on tape. As shown in Figure 2–9, a backup image is a file that consists of one or more backup sections.

Figure 2–9 Backup Images and Backup Sections



Backup images are unique identified in the Oracle Secure Backup catalog by their backup IDs. Similarly, backup sections are uniquely identified in the catalog by their backup section IDs. Example 2–2 shows output from the `lsbu` command for a backup with the ID of `1`.

Example 2–2 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 2–3 shows output from the `lssection` command for the backup section belonging to the backup shown in Example 2–2.

Example 2–3 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
```

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 ways described in "Volumes in a Media Family" on page 2-26.

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 the backup images it contains in the catalog.

Backup Image and Volume Labels

A label contains data that Oracle Secure Backup uses to identify a volume or a backup image. The first block of the first backup image on a volume is referred to as the volume label. It contains the volume ID, owner name, and date and time for the volume creation. The first block of a backup image is referred to as a backup image label. It contains the backup image's file and section numbers and owner.

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.

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.

Note: All the backup images on a volume need to be either labeled or unlabeled. You cannot mix labeled and unlabeled backup images on a volume.

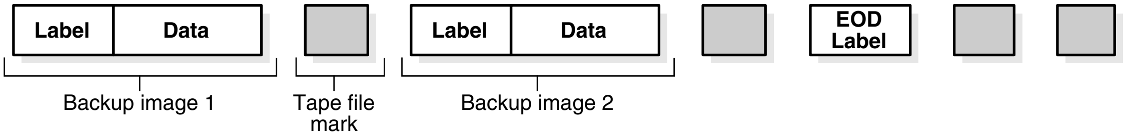
For volumes generated by the Oracle Secure Backup scheduling system, you might see entries such as media family and volume expiration.

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.

As shown in Figure 2–10, 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 2–10 illustrates the format of a volume that contains two backup images. This figure shows the position of the labels and tape file marks.

Figure 2–10 Two Backup Images on a Volume



Assume that the volume shown in Figure 2–10 is the first volume in the set. The volume label for the first backup image could look like the one in Example 2–4.

Example 2–4 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 2–5.

Example 2–5 Backup Image 2

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

After you create a backup image, Oracle Secure Backup 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 you read a backup image, the volume is positioned after the tape file mark following the backup image that you just read and before the volume label of the next backup image.

Volume Sets

Oracle Secure Backup enables a single backup image to span multiple volumes. 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. You can also make efficient use of media by packing backup images onto volumes.

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

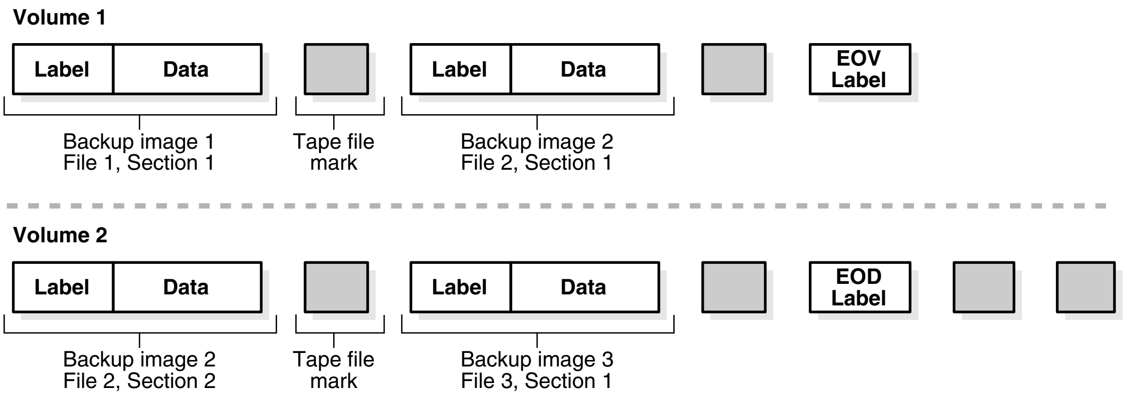
  A sequence number, which is recorded in the volume label, indicates the order of volumes in a volume set. The first volume in a set has sequence number `1`.

- 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.

Figure 2–11 illustrates a volume set that contains three backup images. Backup image 2 spans two volumes.

Figure 2–11 A Single Backup Image on Multiple Volumes



A partial volume label for the first backup image could look like the one shown in Example 2–6.

Example 2–6 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 2–7.

Example 2–7 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 2–8.

Example 2–8 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 2–9.

Example 2–9 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 media families to typical backup operations. For example, you could create media families specifically for onsite backups, offsite backups, and incremental backups.

Media Family Attributes

Volumes in a media family share 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 policies: 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.

Although a volume may 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.

- Write window

  The beginning of the write window is the time at which Oracle Secure Backup first writes to a volume in the volume set. The write window is a user-specified period of time that applies to all volumes in the set. Oracle Secure Backup continues to append backups to the volume set until the end of this period.

  When the write window closes, Oracle Secure Backup does not allow further updates to the volume set until it expires or is relabeled, reused, unlabeled, or overwritten. Note that if a backup is writing to a tape when the write window closes, the backup completes but no further backups are written to the volume.

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.

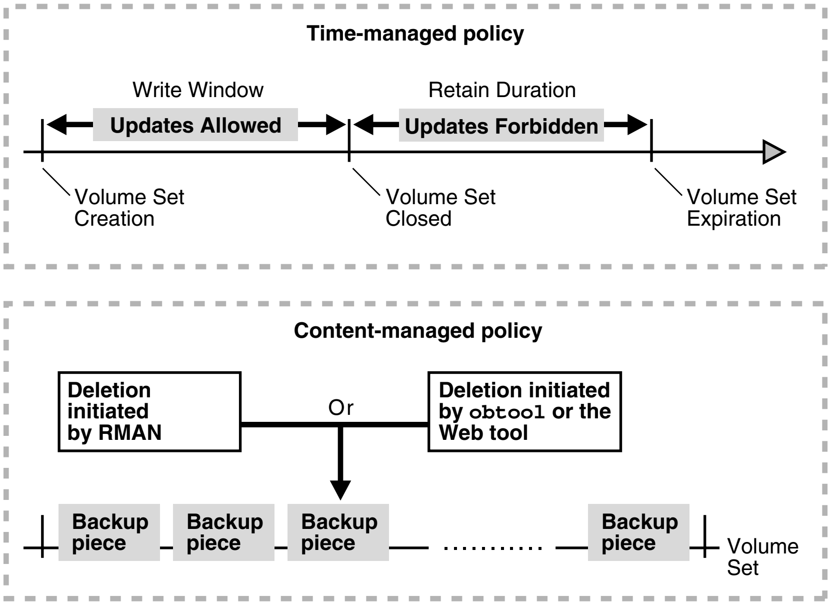
See Also:

- "Configuring Media Families" on page 5-2 to learn how to create media families
- *Oracle Secure Backup Reference* for a description of the media family 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 expired, that is, eligible to be overwritten and recycled. As shown in Figure 2–12, volumes in a media family use either a content-managed expiration policy or time-managed expiration policy.

Figure 2–12 Volume Expiration Policies



Content-Managed Expiration Policies You can make RMAN backups, but not file system backups, to volumes that use a content-managed expiration policy. A volume expires when all backup pieces on the volume have been marked as deleted. Note that 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 through the Web tool or the `chmf` command in `obtool`.

As shown in Figure 2–12, 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 Basics* to learn about crosschecking backups
- *Oracle Database Backup and Recovery Basics* to learn about deleting RMAN 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. Upon reaching this point in time, Oracle Secure Backup automatically considers each volume in the volume set eligible to be overwritten.

As shown in Figure 2–12, 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 in which volumes in a media family are not eligible to be overwritten. All volumes in a volume set share the same retention period.

  The retention period begins when the write window closes for the volume set. This 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, you set the write window for a media family to 7 days. You set the retention period to 14 days, which means that the data on all volumes in the volume set is retained for 14 days from the close of the write window. 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 RMAN backups to time-managed volumes. Thus, volumes with a time-managed expiration policy can 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 the backup pieces as available. In this case, you must use the `CROSSCHECK` command in RMAN to resolve the discrepancy.

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. Normally, the volume sequence file is located in the `admin/state/general` subdirectory of the Oracle Secure Backup home.

Upon defining 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_data00001. 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_data00002 and so on.

- Administrative domain default volume sequence file

  This file, vol-sequence, is created during installation and 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.

- User-specified volume sequence file

  When you specify a volume sequence file, Oracle Secure Backup uses the named 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 or DAT to identify volumes created by different devices

  – The prefix INCR or FULL to identify volumes used for full or incremental backups

  – An operator's initials to identify the user 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.

Daemons and Services

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.

Types of Daemons

An Oracle Secure Backup administrative domain uses a variety of daemons to perform backup, restore, and configuration tasks. As explained in "Host Access Modes" on page 1-7, these daemons run only in hosts using primary access mode; NDMP-accessed hosts do not have Oracle Secure Backup installed.

The daemon programs are located in the `etc` subdirectory of the Oracle Secure Backup home on Linux/UNIX, and in the `bin` subfolder in Windows.

This section describes the Oracle Secure Backup daemons and indicates the hosts on the domain on which they run.

- Service Daemon
- Schedule Daemon
- Index Daemon
- Apache Web Server Daemon
- NDMP Daemon
- Robot Daemon
- Proxy Daemon

Service Daemon

The `observiced` daemon provides a wide variety of services. The service daemon 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 domain. `observiced` also serves as the Certification Authority (CA), accepting certificate signing requests from hosts within the 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 domain, allows for remote administration of the host, handles certificate operations, and initiates Oracle database backup and restore operations. The requesting host's identity certificate is used to verify that it is permitted to invoke the operation.

On all hosts, the service daemon is normally 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 scheduled backups, retains a list of available devices in the administrative domain, and assigns backups to devices as they become available. The daemon receives job creation requests from `obtool` users and from the SBT interface in response to RMAN commands.

The scheduler policies (see "Defaults and Policies" on page 2-30) control how the scheduler dispatches backups.

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 service daemon, which itself is normally started as part of system startup.

NDMP Daemon

The obndmpd daemon implements the NDMP tape service and provides media services to remote clients. The NDMP daemon runs intermittently on a media server.

This daemon is launched by the service daemon in response to client requests to open a channel to a tape drive that is not locally connected to the client. For example, if obtar is performing a backup operation on client C and writing to a tape drive on media server M, then obtar on C directs its I/O requests to an instance of obndmpd running on M.

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 needs to interact with a 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 library, and so on. Each invocation of obrobotd manages a single library. obrobotd exits when all users of a library have closed their connections.

Proxy Daemon

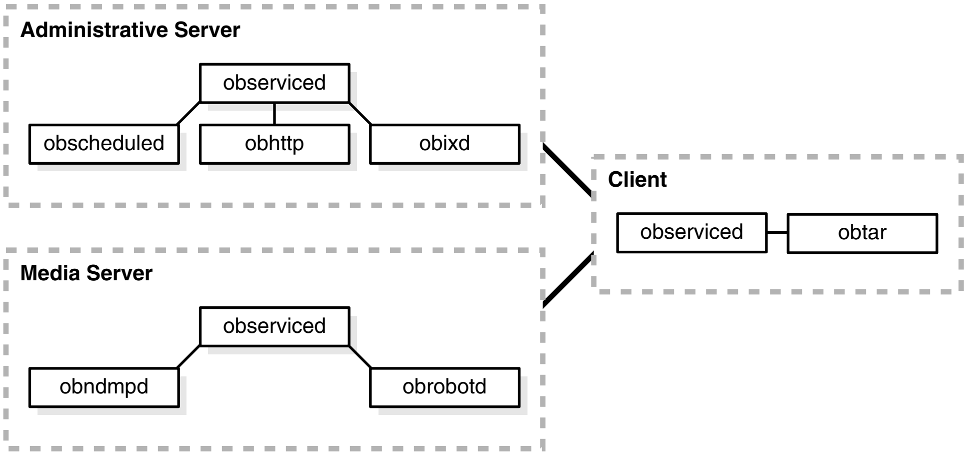
The obproxyd daemon verifies user access for SBT backup and restore operations. The proxy daemon runs on the host that contains the SBT library accessed during the operations. The invocation of the proxy daemon is platform-specific.

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, and if the associated Oracle Secure Backup user is permitted to perform RMAN backups, then the login to Oracle Secure Backup is permitted.

Daemon Interaction in a File System Backup

Figure 2–13 provides a simplified graphical illustration of the relationships among the daemons on an administrative server, media server, and client.

Figure 2–13 Daemons in an Administrative Domain



The client host in Figure 2–13 shows an instance obtar, which is not itself a daemon but the application that serves as the Data Management Application (DMA). obtar is the underlying Oracle Secure Backup engine that manipulates the data and tape services during a backup or restore operation. Typically, you issue commands in obtool or the Web tool, which Oracle Secure Backup then translates internally to obtar commands.

Assume a scenario in which observiced is running on all hosts, observiced on the administrative server has invoked obscheduled and obhttpd, and a client 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 volumes required for the backup job.
3. observiced on the administrative server sends a request to observiced on the client to invoke obtar.
4. obtar on the client communicates with obndmpd on the media server until the file system data is written to tape. The client obtar is the data service, while the media server obndmpd is the NDMP tape service.
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 are configuration data that control how Oracle Secure Backup operates within an administrative domain. The data is 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 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.

- Device policies

  These policies control how devices are automatically detected during device discovery as well as when device write warnings are generated.

- 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.

- Naming policy

  This policy specifies a WINS server for the administrative domain.

- NDMP policies

  These policies specify NDMP Data Management Agent (DMA) defaults. For example, you can specify a password used to authenticate Oracle Secure Backup to each NDMP server.

- 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.

- Security policies

  These policies control aspects of domain security. For example, you can specify the key size to be used when creating the public/private key pair used in identity certificates in the administrative domain.

Network Backup Security

An Oracle Secure Backup administrative domain is a network of hosts. Any such network has a level of vulnerability to malicious attacks. The task of the security administrator is to learn the types of possible attacks and how to guard against them.

An adequately secured backup system must meet the following requirements:

- Software components must not expose the hosts they run on to attack. For example, a daemon should be prevented from listening on a well-known port and performing arbitrary privileged operations.

- Data managed by the backup software must not be viewable, erasable, or modifiable by unauthorized users. Conversely, the backup software must permit authorized users to perform these tasks.

You can use Oracle Secure Backup to meet the preceding requirements. By default, all hosts that run Oracle Secure Backup must have their identity verified before they can join the administrative domain. Hosts within the domain use X.509 certificates for host authentication. After a Secure Sockets Layer (SSL) connection is established between hosts, control and data messages are encrypted when transmitted over the network. SSL protects the administrative domain from eavesdropping, message tampering or forgery, and replay attacks.

Network backup software such as Oracle Secure Backup is only one component of a secure backup network. Oracle Secure Backup can supplement, but not take the place of, the physical and network security provided by administrators.

This section contains the following topics:

- Host Authentication and Communication
- Data Encryption
- Default Security Configuration

Host Authentication and Communication

By default, Oracle Secure Backup uses the SSL protocol to establish a secure communication channel between hosts in an administrative domain. Each host has an X.509 certificate known as an identity certificate. This certificate is signed by the Certification Authority (CA) and uniquely identifies this host within the administrative domain. The identity certificate is required for authenticated SSL connections.

Note: Currently, the NDMP protocol does not support an SSL connection to filers.

Identity Certificates and Public Key Cryptography

An identity certificate has both a body and a digital signature. The contents of a certificate include the following:

- A public key
- The identity of the host
- The attributes of the host, that is, what the host is authorized to do

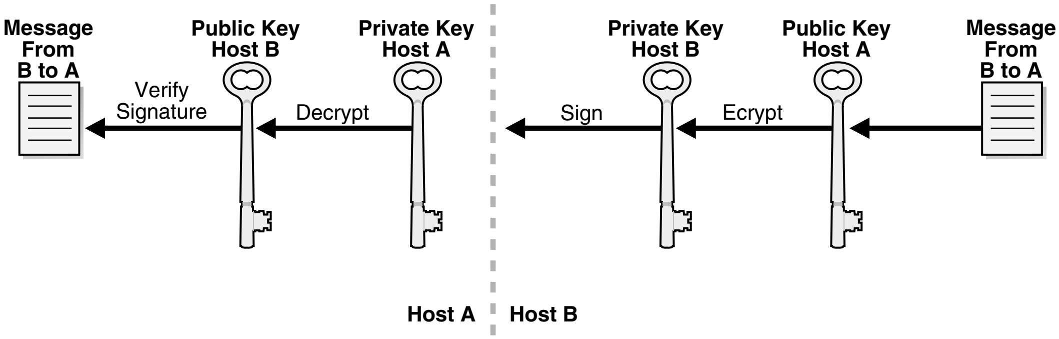
Every host in the domain, including the administrative server, has a private key known only to that host that is stored with the host's identity certificate. This private key corresponds to a public key that is made available to other hosts in the administrative domain.

Any host in the domain can use a public key to send an encrypted message to another host, but only the host with the corresponding private key can decrypt the message. A host can use its private key to attach a digital signature to the message. The host creates a digital signature by submitting the message as input to a cryptographic hash function and then encrypting the output hash with a private key.

The receiving host authenticates the digital signature by decrypting it with the sending host's public key. Afterwards, the receiving host decrypts the encrypted message with its private key, inputs the decrypted message to the same hash function used to create the signature, and then compares the output hash to the decrypted signature. If the two hashes match, then the message has not been tampered with.

Figure 2–14 illustrates how host B can encrypt and sign a message to host A, which can in turn decrypt the message and verify the signature.

Figure 2–14 Using Public and Private Keys to Encrypt and Sign Messages



Authenticated SSL Connections

For hosts to securely exchange control messages and backup data within the domain, they must first authenticate themselves to one another. Host connections are always two-way authenticated with the exception of the initial host invitation to join a domain and communication with NDMP servers.

In two-way authentication, the hosts participate in a handshake process whereby they mutually decide on a cipher suite to use, exchange identity certificates, and validate that each other's certificate has been issued by a trusted CA. At the end of this process, a secure and trusted communication channel is established for the exchange of data.

The use of identity certificates and SSL prevents outside attackers from impersonating a client in the administrative domain and accessing backup data. For example, an outside attacker could not run an application on a non-domain host that sends messages to domain hosts that claim origin from a host within the domain.

Certification Authority

The service daemon (`observiced`) on the administrative server is the root CA of the administrative domain. The primary task of the CA is to issue and sign identity certificates for the hosts in the administrative domain. The CA's signing certificate, which it issues to itself and then signs, gives the CA the authority to sign identity certificates for hosts in the domain. The relationship of trust requires that all hosts in the administrative domain can trust certificates issued by the CA.

Each host stores its own identity certificate as well as a trusted certificate (or set of certificates) that establishes a chain of trust to the CA. Like other hosts in the domain, the CA stores its identity certificate. The CA also maintains a signing certificate that authorizes the CA to sign the identity certificates for the other hosts in the domain.

Automated and Manual Certificate Provisioning Mode Oracle Secure Backup provides the following methods of initializing the security credentials for a client host that wants to join the domain:

- An automated mode that is easy to use, but has potential (if unlikely) security vulnerabilities
- A manual mode that is harder to use but less vulnerable to tampering

In automated certificate provisioning mode, which is the default, adding a host to the domain is transparent. The new host generates a public/private key pair and then sends the certificate request—which includes the public key—to the CA. The CA issues the host an identity certificate, which it sends to the new host along with any certificates required to establish a chain of trust to the CA.

The communication between the two hosts is over a secure but non-authenticated SSL connection. It would be conceivable, although extremely difficult, for a rogue host to insert itself into the network between the CA and the new host, thereby masquerading as the legitimate host and illegally entering the domain.

In manual certificate provisioning mode, the CA does not automatically transmit certificate responses to the new host. You must transfer the certificate as follows:

1. Use the `obcm` utility to export a signed certificate from the CA.
2. Use a secure mechanism such as a floppy disk or USB keychain drive to transfer a copy of the signed identity certificate from the CA to the new host.
3. Use `obcm` on the new host to import the transferred certificate into host's wallet. The `obcm` utility verifies that the certificate request in the wallet matches the signed identity certificate.

You must balance security and usability to determine which certificate provisioning mode is best for your administrative domain.

See Also: "Managing Certificates with obcm" on page 11-12

Oracle Wallet

Oracle Secure Backup stores certificates in an Oracle wallet. The wallet is represented on the operating system as a password-protected, encrypted file. Each host in the administrative domain has its own wallet in which it stores its identity certificate, private key, and set of trusted certificates. Oracle Secure Backup does not share its wallets with other Oracle products.

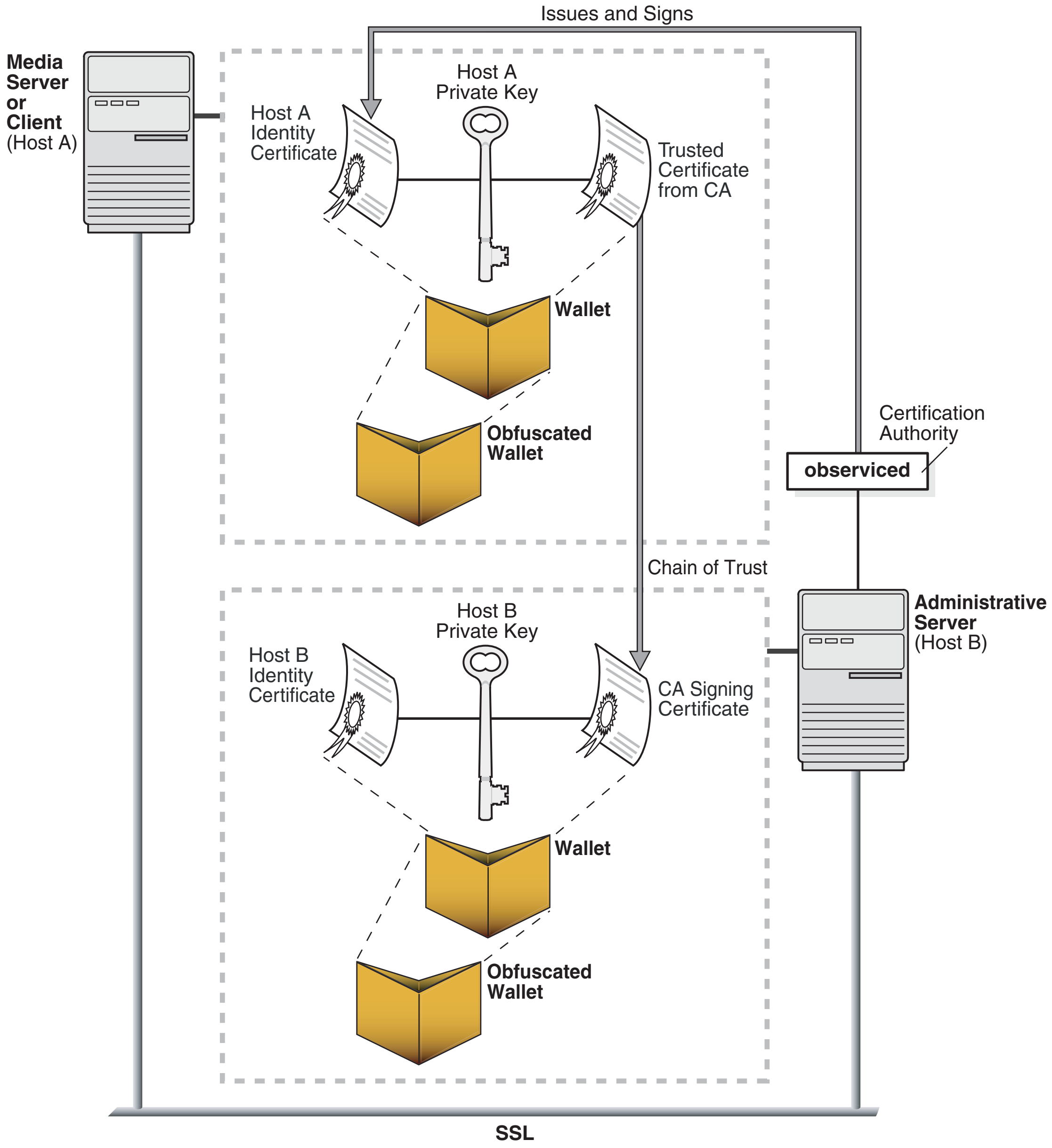
Besides maintaining its password-protected wallet, each host in the domain maintains an obfuscated wallet. This version of the wallet does not require a password. The obfuscated wallet, which is scrambled but not encrypted, enables the Oracle Secure Backup software to run without requiring a password during system startup.

Note: To reduce risk of unauthorized access to obfuscated wallets, Oracle Secure Backup does not back them up. The obfuscated version of a wallet is named `cwallet.sso`. By default, the wallet is located in `/usr/etc/ob/wallet` on Linux and UNIX and `C:\Program Files\Oracle\Backup\db\wallet` on Windows

The password for the password-protected wallet is generated by Oracle Secure Backup and not made available to the user. The password-protected wallet is not normally used after the security credentials for the host have been established because the Oracle Secure Backup daemons use the obfuscated wallet.

Figure 2–15 illustrates the relationship between the CA and other hosts in the domain.

Figure 2–15 Oracle Wallets

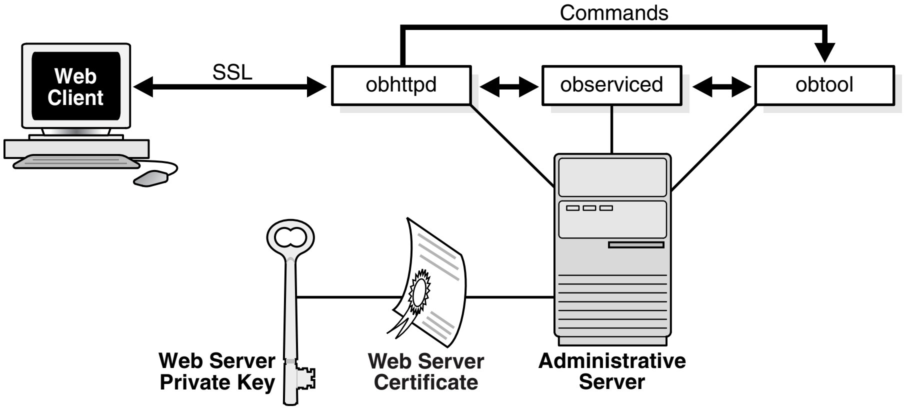


Web Server Authentication

As explained in "Oracle Secure Backup Interfaces" on page 1-3, you can manage Oracle Secure Backup through the Web tool. The Apache Web server for the administrative domain runs on the administrative server as the `obhttpd` daemon. When you issue commands through the Web tool, `obhttpd` repackages them as `obtool` commands and passes them to an instance of `obtool` running on the administrative server.

The Web server requires a signed X.509 certificate and associated public and private keys to establish an SSL connection with a client Web browser. The X.509 certificate for the Web server is self-signed by the `installob` program when you install Oracle Secure Backup on the administrative server. Figure 2–16 shows the interaction between Web server and client.

Figure 2–16 Web Server Authentication



The Web server X.509 certificate and keys are not stored in the wallet used for host authentication in the Oracle Secure Backup administrative domain, but are stored in files in the `/apache/conf` subdirectory of the Oracle Secure Backup home. A single password protects the certificates and keys. This password is stored in encrypted form in the `/admin/config/default/daemons` file. When the Web server starts, it obtains the password by using a mechanism specified in the Web server configuration file. This password is never transmitted over the network.

Data Encryption

Figure 1–2, "Administrative Domain with Five Hosts" illustrates the control flow and data flow within an administrative domain. Control messages exchanged by hosts in the administrative domain are encrypted by SSL.

Data flow in the domain includes both file system and database backup data. To understand how backup encryption affects data, it is helpful to distinguish between data at rest, which is backup data that resides on media such as disk or tape, and data in transit, which is backup data transferred over the network.

File system backups on tape (data at rest) are not encrypted by Oracle Secure Backup. RMAN-encrypted backups made through the Oracle Secure Backup SBT interface are supported, but the encryption is provided by RMAN before the backup is provided to the SBT interface. The Oracle Secure Backup SBT is the only supported interface for making encrypted RMAN backups directly to tape.

By default, the backup data in transit within an administrative domain, both file system and database data, is encrypted through SSL. To improve performance, you can disable encryption for data in transit within the administrative domain with the `encryptdataintransit` security policy (see "Defaults and Policies" on page 2-30).

Note: If database backup data is first encrypted by RMAN, then the data is not further encrypted in transit.

Table 2–4 explains how Oracle Secure Backup handles data encryption. The table assumes that you have chosen not to disable SSL encryption for backup data in transit within the domain.

Table 2–4 Data Encryption

Type of Backup Data	Encrypted at Rest	Encrypted in Transit
File system	No	Yes
Database backup not encrypted by RMAN	No	Yes
Database backup encrypted by RMAN	Yes	Yes, but only because it is already encrypted: RMAN-encrypted data is not encrypted again by SSL

For example, suppose RMAN makes an encrypted backup of a database on client host C to a tape drive attached to media server S. RMAN encrypts the backup before it is provided to the SBT interface on client C. Oracle Secure Backup transfers the RMAN-encrypted data over the network to server S. Oracle Secure Backup does not apply additional encryption to the data as it passes over the network. After Oracle Secure Backup writes the data to tape, the data resides on tape in encrypted form.

Assume a different case in which you use Oracle Secure Backup to back up the file system on host C to the tape drive attached to server S. Oracle Secure Backup sends the unencrypted backup data over the network to server S. Oracle Secure Backup applies encryption to the data as it passes over the network. After Oracle Secure Backup writes the data to tape, the file system data resides in unencrypted form.

> **See Also:** *Oracle Database Backup and Recovery Advanced User's Guide* to learn about encryption of RMAN backups

Default Security Configuration

When you install Oracle Secure Backup on the administrative server, the installation program configures the administrative server as the CA automatically. By default, security for an administrative domain is configured as follows:

- SSL is used for host authentication and message integrity.
- The CA signs and issues the identity certificate for each domain host in automated certificate provisioning mode.
- The size of the public and private key for every host in the domain is 1024 bits.
- Host communications within the domain are encrypted by SSL.

When you add hosts to the administrative domain, Oracle Secure Backup creates the wallet, keys, and certificates for each host when you create the hosts in `obtool` or the Web tool. No additional intervention or configuration is required.

Refer to Chapter 11, "Configuring Security: Advanced Topics" if you plan change the default configuration in any of the following ways:

- Disable SSL for inter-host authentication and communication by setting the `securecomms` security policy
- Transmit identity certificates in manual certificate provisioning mode
- Set the key size for a host to a value greater or less than the default of 1024 bits
- Disable encryption for backup data in transit by setting the `encryptdataintransit` security policy

Besides explaining how to perform the preceding tasks, the advanced security chapter provides instructions for planning security in an administrative domain. The chapter also explains how Oracle Secure Backup manages certificates, keys, and wallets.

Part II

Configuring the Administrative Domain

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

This part contains the following chapters:

- Chapter 3, "Getting Started"
- Chapter 4, "Setting Up the Administrative Domain"
- Chapter 5, "Configuring Backup and Media Settings"

3

Getting Started

This chapter provides a brief tour of the interfaces that you can use with Oracle Secure Backup. You will need to use one or more of the interfaces when you configure and manage your administrative domain. This chapter contains the following topics:

- Before You Begin
- Using the Web Tool
- Using obtool
- Using Oracle Enterprise Manager

See Also:

- *Oracle Secure Backup Reference* for a description of `obtool` commands
- Chapter 12, "Using obtar" to learn how to use the `obtar` command-line interface, which is intended for advanced users only

Before You Begin

Before you begin using Oracle Secure Backup, ensure that:

- Oracle Secure Backup is installed on each UNIX and Windows computer in your administrative domain. The *Oracle Backup Installation Guide* describes how to perform installation.
- On UNIX systems, the Oracle Secure Backup service daemon `observiced` is running. On Windows systems, the Oracle Secure Backup `service` is running.
- On your administrative server, the Apache Web server is running. The Web server, which is started behind the scenes during Oracle Secure Backup installation, enables you to use the Oracle Secure Backup Web tool.

Using the Web Tool

The Web tool is the browser-based interface to Oracle Secure Backup. You can use the Web tool to configure the administrative domain, perform file system backup and restore operations, browse and manage backup data, and monitor operations.

Oracle Secure Backup invokes the Apache Web server, which runs behind the scenes when Oracle Secure Backup is started on the administrative server, to launch the Web tool. As explained in "Web Server Authentication" on page 2-35, you can access the Web tool from any supported browser that can connect to the server through SSL (see *Oracle Secure Backup Readme* for a list of supported Web browsers).

This section contains the following topics:

- Starting the Web Tool
- Exploring the Web Tool

Starting the Web Tool

This section explains how to log in to the Oracle Secure Backup administrative domain through a Web browser.

Follow these steps:

1. Launch your Web browser and supply the URL of the host running Oracle Secure Backup. Use the following syntax, where *hostname* can be a fully qualified domain name:

   ```
   https://hostname
   ```

   For example, you might invoke the following URL:

   ```
   https://patti.oracle.com
   ```

   The **Security Alert** box warns that the certificate is not trusted, but it is not necessary to view the certificate and make any configuration changes.

   Oracle Secure Backup installs a self-signed certificate for the Apache Web server. The Web server requires a signed certificate for data encryption purposes. The **Security Alert** box is displayed because the signer of the certificate is not trusted, that is, the browser does not recognize the signer as a registered Certificate Authority (CA). This alert does not mean that your data is not encrypted, only that the CA is not recognized.

2. Click **Yes** to continue.

The Oracle Secure Backup Login page appears.

3. Enter an Oracle Secure Backup username in the **User Name** box and a password in the **Password** box.

   Log in as the `admin` user if you are logging into Oracle Secure Backup for the first time. You can create additional users after you log in.

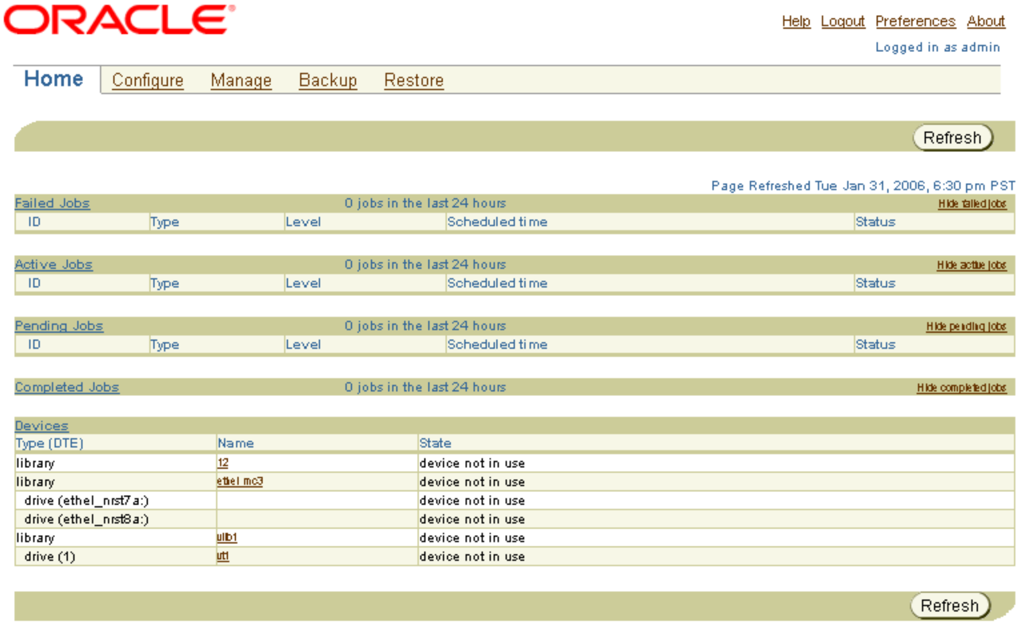
4. Click the **Login** button. The Oracle Secure Backup Home page appears.

   The **Home**, **Configure**, **Manage**, **Backup**, and **Restore** tabs are explained in detail in the following sections.

Exploring the Web Tool

After you log in to the Oracle Secure Backup Web tool interface, the Oracle Secure Backup Home page appears. Figure 3–1 shows an example of the Home page.

Figure 3–1 Home Page



Page Refreshed Tue Jan 31, 2006, 6:30 pm PST

Failed Jobs 0 jobs in the last 24 hours Hide failed jobs

ID	Type	Level	Scheduled time	Status

Active Jobs 0 jobs in the last 24 hours Hide active jobs

ID	Type	Level	Scheduled time	Status

Pending Jobs 0 jobs in the last 24 hours Hide pending jobs

ID	Type	Level	Scheduled time	Status

Completed Jobs 0 jobs in the last 24 hours Hide completed jobs

Devices

Type (DTE)	Name	State
library	12	device not in use
library	ethel mc3	device not in use
drive (ethel_nrst7a:)		device not in use
drive (ethel_nrst8a:)		device not in use
library	ulib1	device not in use
drive (1)	utl	device not in use

The purpose of this page is to provide a snapshot of the current status of Oracle Secure Backup jobs and devices. As such, the page presents important summary information to administrators and users.

The main page includes the schedule times and status of recent jobs as well as job IDs, job type, and job level. Oracle Secure Backup provides a link for failed jobs, alerting users and administrators to potential trouble spots.

The **Devices** link lists the devices associated with each job along with information concerning device type, device name, and status. This page provides you with an overall picture of the various backup or restore processes that are going on.

Note: A status of "device not in use" means that the device is present but is not currently being utilized for backup or restore operations.

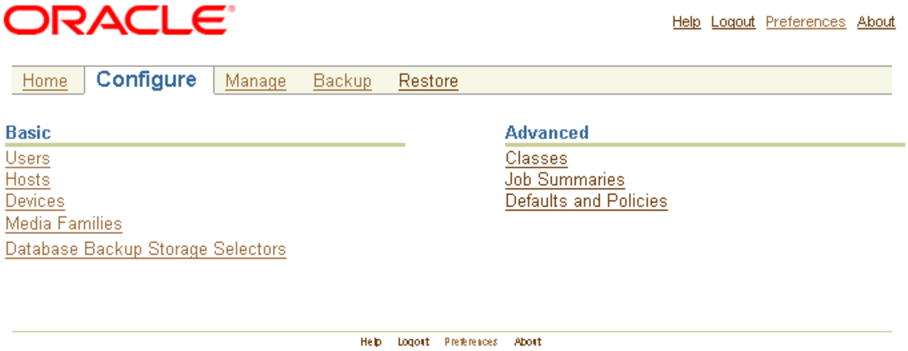
A menu bar at the top of the Oracle Secure Backup Home page enables you to select among the **Configure**, **Manage**, **Backup**, and **Restore** tabs.

> **Note:** When using the Web tool, make sure that your browser is configured to reload the page every time it is viewed. Otherwise, the browser may display stale information. For example, changes made in `obtool` may not be visible in the browser.

Configure Tab

Click the **Configure** tab from the menu bar to display configuration options. Figure 3–2 shows an example of the Configure page.

Figure 3–2 Configure Tab



The Configure page is divided into two main sections:

- Basic
- Advanced

Basic This section provides the following links:

- **Users**

  Click this link to configure one or more user accounts for logging into and employing Oracle Secure Backup.

- **Hosts**

  Click this link to configure one or more hosts. A host is a machine that participates in the Oracle Secure Backup administrative domain

- **Devices**

  Click this link to configure devices for use with Oracle Secure Backup. A device is a tape drive or library identified by a user-defined name.

- **Media Families**

  Click this link to configure media families. A media family is a named classification of backup volumes. A volume is a single unit of media, such as an 8mm tape.

- **Database Backup Storage Selectors**

  Click this link to configure one or more devices and media families for use during Oracle database backup and restore operations.

Advanced This section provides the following links:

- **Classes**

  Click this link to configure classes. A class defines a set of rights that are granted to a user. A class can apply to multiple users; however, each user is assigned to exactly one class.

- **Job Summaries**

  Click this link to create a job summary schedule for generation of job summaries for email distribution. A job summary is a generated text file report that tells you whether a backup operation was successful. Oracle Secure Backup can generate and email job summaries detailing the status of scheduled backups.

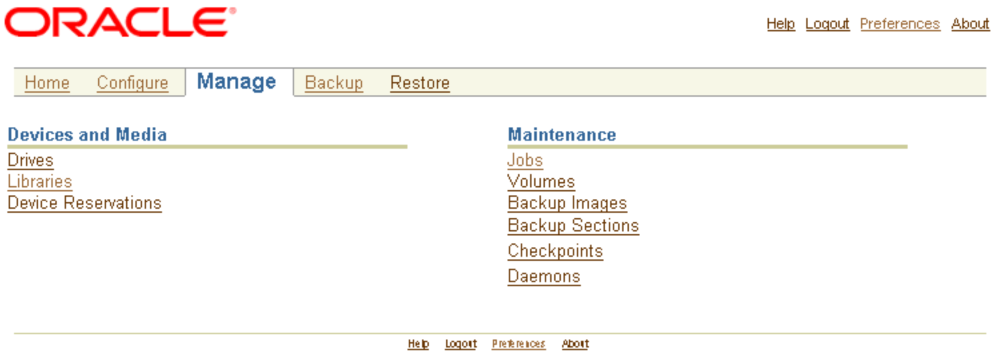
- **Defaults and Policies**

  Click this link to edit defaults and policies. Defaults and policies are a set of configuration data that control how Oracle Secure Backup runs throughout an administrative domain.

Manage Tab

Click the **Manage** tab to display management options. Figure 3–3 shows an example of the Manage page.

Figure 3–3 Manage Tab



The Manage page is divided into two main sections:

- Devices and Media
- Maintenance

Devices and Media This section includes the following links:

- **Drives**

  Click this link to determine the status of a volume or device or mount or unmount a volume.

- **Libraries**

  Click this link to view and control libraries.

- **Device Reservations**

  Click this link to reserve and unreserve devices for private use.

Maintenance This section includes the following links:

- **Jobs**

  Click this link to manage jobs in an administrative domain. You can view the status of backup and restore jobs.

- **Volumes**

  Click this link to filter and then view all volumes in the catalog. You can filter the results to scale down your search. A volume is a single unit of media, such as 8mm tape. A volume can contain one or more backup images.

- **Backup Images**

  Click this link to manage backup images. A backup image is the work product of a single backup operation.

- **Backup Sections**

  Click this link to view and remove backup sections. A backup section is that part of a backup image that occupies one physical volume.

- **Checkpoints**

  Click this link to list and delete checkpoints describing certain in-progress, failed, and completed NDMP backups.

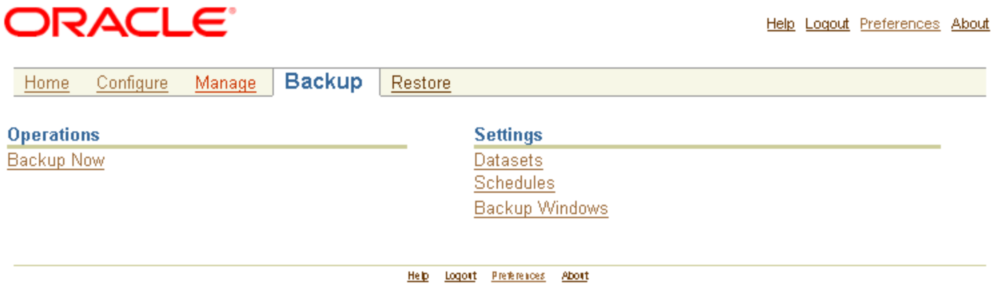
- **Daemons**

  Click this link to manage daemons and control and view daemon properties.

Backup Tab

Click the **Backup** tab to display backup image options. Figure 3–2 shows a sample page.

Figure 3–4 Backup Tab


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Operations
Backup Now
Settings
Datasets
Schedules
Backup Windows
Help Logout Preferences About

The Backup page is divided into two main sections:

- Operations
- Settings

Operations This section includes the **Backup Now** link. Click this link to perform one-time backups of data described by existing dataset files.

Settings This section includes the following links:

- **Datasets**

  Click this link to configure dataset files. A dataset file describes the data that you want to back up.

- **Schedules**

Click this link to configure a backup schedule. The backup schedule describes the frequency with which a backup runs.

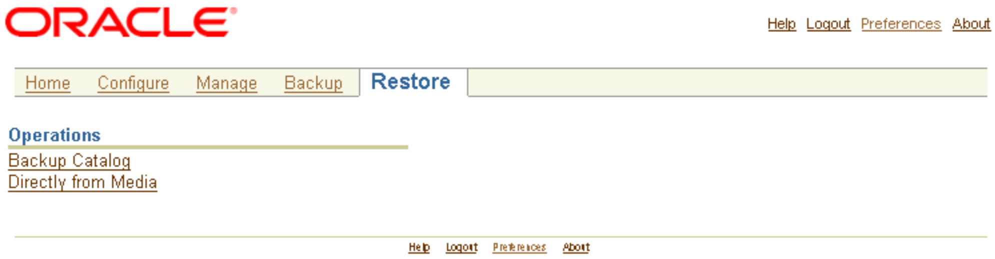
- **Backup Windows**

  Click this link to configure backup windows. A backup window is a time range for the execution of scheduled backups.

Restore Tab

Click the **Restore** tab to display restore options. Figure 3–5 shows a sample page.

Figure 3–5 Restore Tab


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Operations
Backup Catalog
Directly from Media
Help Logout Preferences About

The Operations section includes the following links:

- **Backup Catalog**

  Click this link to browse data associated with backup and restore operations.

- **Directly from Media**

  Click this link to perform *raw* restores, which require prior knowledge of the names of the file system objects you want to restore. You must also know the volume IDs and the file numbers on which the volumes are stored.

Persistent Page Links

The top and bottom panels of the Home page, and every page of the Web tool interface, have the following persistent links:

- Help
- Logout
- Preferences
- About

Help Click **Help** to display this manual in PDF form.

Logout Click **Logout** to log out of Oracle Secure Backup and return to the Oracle Secure Backup Login page. Oracle Secure Backup clears your user name and password cookies from the Web browser that you are using.

Preferences Click **Preferences** to go to the Preference page. In this page you can select settings for the following options:

- **Extended command output**

  Click this button to specify that Oracle Secure Backup should display a section with the commands that enable the Web tool to build its pages.

The Web tool makes calls into `obtool`, the underlying Oracle Secure Backup command line engine. If you select **On**, then directory paths and command line entries for `obtool` executables are displayed at the bottom of each page. Select **Off** to hide the display of command output.

- **Background timeout**

  Enter a value in this box to set the maximum idle time for `obtool` background processes.

  Operations such as catalog browsing, data restore operations, and on-demand backups require Oracle Secure Backup to create a background `obtool` process to retain state information too complex to represent in a browser cookie. The background timeout value identifies the maximum idle time of these background process. When a background process exceeds this idle time limit, it exits gracefully and the associated user's browser state is lost. The default is **24 hours**.

- **Select table size**

  Enter a value in this box to set the size (in number of rows) of the display window of the Web tool interface. The default is **8** rows.

- **Inactivity logout**

  Enter a time period. If the user does not use the Web tool within this time frame, then the browser will automatically refresh the user to the login page. The default is 30 minutes.

About The bottom panel of every page of the Web tool has a link to information about the Oracle Secure Backup product, including release date, system information, administrative server, and IP address.

Using obtool

This section explains how to use `obtool`, which is the primary command-line interface to Oracle Secure Backup. The `obtool` executable is located in the `bin` subdirectory of the Oracle Secure Backup home. You can start `obtool` on any host in the administrative domain, log in to the domain as an Oracle Secure Backup user, and issue commands.

This section contains the following topics:

- Displaying obtool Invocation Help
- Starting obtool in Interactive Mode
- Executing obtool Commands in Interactive Mode
- Executing obtool Commands in Noninteractive Mode
- Configuring an Administration Domain with obtool

Displaying obtool Invocation Help

Assuming that the `bin` subdirectory of the Oracle Secure Backup home is in your system path, you can obtain online help about `obtool` invocation options by running the following command at the operating system prompt:

```
% obtool help invocation
```

The `obtool` utility displays the following output:

```
obtool invocation:
```

```
Usage: To enter interactive mode:
       obtool [<cl-option>]...
Usage: To execute one command and exit:
       obtool [<cl-option>]... <command> [<option>]... [<argument>]...
Usage: To display program version number and exit:
       obtool --version/-V
Usage: To create a new administrative domain with this machine acting as the
       administrative server:
       obtool --initnewdomain [--adminpassword/-A passwd] [--force]
       [--nullpassword/-N] [--verbose/-v]
```

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

Starting obtool in Interactive Mode

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

```
% obtool
```

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

```
ob>
```

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

```
% obtool
Oracle Secure Backup 10.1
login:
```

The Oracle Secure Backup installation script creates the `admin` user automatically and requires you to create a password. You can enter the `admin` credentials when you log in to Oracle Secure Backup for the first time.

Executing obtool Commands in Interactive Mode

You can enter the commands described in *Oracle Secure Backup Reference* at the `obtool` prompt. For example, you can enter the `lshost` command to display the hosts in your administrative domain (sample output included):

```
ob> lshost
brhost2          client                           (via OB)   in service
brhost3          mediaserver,client               (via OB)   in service
br_filer         client                           (via NDMP) in service
stadv07          admin,mediaserver,client         (via OB)   in service
```

In general, this manual describes how to use the Web tool rather than `obtool` to perform administrative tasks. You can click **Preferences** at the top of any Web tool page and enable **Extended command output**. Whenever you perform a task in the Web tool, the Extended Command Output section at the bottom of the page shows the underlying `obtool` commands used to perform the task.

Redirecting Input in Interactive Mode

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

```
ob> < pathname
```

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

```
lshost --long
lsdev --long
```

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

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

Executing obtool Commands in Noninteractive Mode

To execute commands in `obtool` noninteractively, use the following syntax:

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

The following example executes the `obtool lshost` command and then returns to the operating system prompt:

```
% obtool lshost
brhost2          client                            (via OB)   in service
brhost3          mediaserver,client                (via OB)   in service
br_filer         client                            (via NDMP) in service
stadv07          admin,mediaserver,client          (via OB)   in service
%
```

Redirecting Input in Noninteractive Mode

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

```
lshost --long
lsdev --long
```

You can redirect the `obtool` input to this script as follows at the system prompt:

```
% obtool < /home/hosts.txt
```

Configuring an Administration Domain with obtool

When you run `installob` and specify a host as the administrative server, Oracle Secure Backup implicitly initializes the administrative domain. Initializing the domain assigns the host the role of administrative server within the administrative domain.

In some circumstances, you may need to initialize a new domain or reinitialize an old domain. You can use the following syntax to establish the local host as the administrative server for a new Oracle Secure Backup administrative domain:

```
obtool --initnewdomain [--adminpassword/-A passwd] [--force]
       [--nullpassword/-N] [--verbose/-v]
```

If the local host is already established as an administrative server, then specifying `--force` causes the host to reinitialize itself. The `--force` option is useful when you have forgotten your password.

Using Oracle Enterprise Manager

You can use Oracle Enterprise Manager 10*g* (10.2) to use the Oracle Secure Backup SBT interface for database backup and restore operations. You cannot use Enterprise Manager to perform file system backup and restore operations, although Enterprise Manager includes a link to the Web tool. In general, you should use Enterprise Manager only for database-related tasks.

This section contains the following topics:

- Registering an Administrative Server in Enterprise Manager
- Accessing the Oracle Secure Backup Web Tool in Enterprise Manager

Registering an Administrative Server in Enterprise Manager

You can make RMAN backups to the Oracle Secure Backup SBT interface by using Enterprise Manager Database Control or Grid Control. As explained in "Interfaces for Managing Database Backup and Recovery" on page 6-2, the Database Control console must run on the administrative server and can only back up an Oracle database running on the administrative server. You can run the Grid Control console on any database host in the administrative domain and use it to back up any database in the domain. This section describes how to get started with the Database Control console.

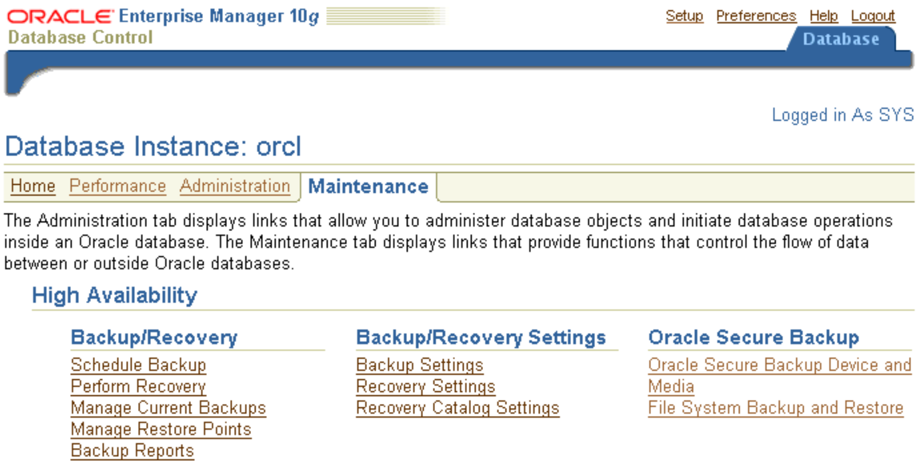
To use Enterprise Manager to manage your backups, you need to make Enterprise Manager aware of your administrative server. As explained in "Administrative Domains" on page 1-5, the administrative server stores the configuration data and catalog for the administrative domain.

> **Note:** This section assumes that you are familiar with Oracle Enterprise Manager Database Control and use it to manage backup and recovery. If you need an introduction to using Oracle Enterprise Manager with RMAN, refer to the chapter on backup and recovery in *Oracle Database 2 Day DBA*.

To register the administrative server in Oracle Enterprise Manager Database Control:

1. Log in to the Oracle Enterprise Manager Database Control console as a user with database administrator rights.
2. Navigate to the Oracle Secure Backup section of the Maintenance page. Figure 3–6 shows the relevant section of the Maintenance page.

Figure 3–6 Maintenance Page



The Administration tab displays links that allow you to administer database objects and initiate database operations inside an Oracle database. The Maintenance tab displays links that provide functions that control the flow of data between or outside Oracle databases.

If you are using releases 10.2.0.1 or 10.2.0.2 of Enterprise Manager Grid Control or release 10.2.0.2 of Enterprise Manager Database Control, then the Maintenance page does not include the Oracle Secure Backup section by default. In this case, proceed to the next step to make the links active; otherwise, skip the following step and proceed directly to Step 4.

3. If (and only if) the Oracle Secure Backup section does not appear in the Maintenance page, then perform the following steps:

   a. Navigate to the *ORACLE_HOME*/*hostname_SID*/sysman/config directory and open the emoms.properties file in a text editor.

   b. Set osb_enabled=true and save the file.

   c. Stop the Oracle Enterprise Manager Database Control console as follows:

      ```
      emctl stop dbconsole
      ```

   d. Restart the Oracle Enterprise Manager Database Control console as follows:

      ```
      emctl start dbconsole
      ```

   e. Navigate to the Maintenance page and confirm that the Oracle Secure Backup section is shown.

4. Click **Oracle Secure Backup Device and Media**.

   The Add Administrative Server page appears.

5. Log in to your Oracle Secure Backup administrative domain as follows:

   - In the **Oracle Secure Backup Home** box, enter the Oracle Secure Backup home directory, which is directory in which you installed Oracle Secure Backup. Typically, this directory is /usr/local/oracle/backup on UNIX and Linux and C:\Program Files\Oracle\Backup on Windows.

   - In the **Username** box, enter the name of an Oracle Secure Backup administrative user. For example, enter admin.

   - In the **Password** box, enter the password for the Oracle Secure Backup administrator.

   The Host Credentials page appears.

6. Enter the username and password of the operating system user on the administrative server. This user needs `root` privileges.

   The Oracle Secure Backup Device and Media: Administrative Server: *hostname* page appears. You can use this page to load tapes.

After you have registered the administrative server, you are ready to use Enterprise Manager with Oracle Secure Backup. Refer to Chapter 6, "Using Recovery Manager with Oracle Secure Backup" for further instructions.

Accessing the Oracle Secure Backup Web Tool in Enterprise Manager

Enterprise Manager provides the interface for database backup and recovery. To access information relating to file system backups, you must use either `obtool` or the Web tool. The Enterprise Manager console provides a link to the Web tool.

To access the Web tool through Enterprise Manager Database Control:

1. Log in to the Enterprise Manager Database Control as a user with database administrator rights.
2. Navigate to the Oracle Secure Backup section of the Maintenance page.

   > **Note:** If the Oracle Secure Backup section is not displayed in the Maintenance page, then follow the instructions in Step 3 of the previous section to make the links active.

3. Click **File System Backup and Restore**.

   Enterprise Manager starts the Web tool interface, which is described in "Starting the Web Tool" on page 3-2.

4

Setting Up the Administrative Domain

This chapter explains the basic steps involved in setting up an administrative domain. It is assumed that you have read the conceptual overview in "Administrative Domains" on page 1-5. This chapter covers the following topics:

- Overview of Administrative Domain Configuration
- Configuring Defaults and Policies
- Configuring Hosts
- Configuring Tape Devices
- Configuring Classes
- Configuring Users

Note: Before you set up an administrative domain, ensure you have logged into Oracle Secure Backup as explained in "Starting the Web Tool" on page 3-2.

Overview of Administrative Domain Configuration

This section describes the steps involved in configuring an Oracle Secure Backup administrative domain. In many cases, the domain defaults are sufficient, so no additional configuration is required. Steps that are optional are noted.

This section makes the following assumptions:

- Reliaty Backup is not currently installed on the hosts in your domain. If you are migrating Reliaty Backup to Oracle Secure Backup, then refer to *Oracle Secure Backup Migration Guide*.
- You have already installed Oracle Secure Backup on a host and configured it as the administrative server. If you have not yet performed this task, refer to *Oracle Secure Backup Installation Guide*.
- You have installed Oracle Secure Backup on the media servers and clients (except hosts that use NDMP access mode) and configured drivers and device special files so that the tape devices are usable by Oracle Secure Backup. If you have not yet performed this task, refer to *Oracle Secure Backup Installation Guide*.
- You have not yet used the Web tool or `obtool` to configure your clients, media servers, and tape devices. It is assumed that the only member of your domain is the administrative server.

  If you already configured the hosts and devices in your domain, which is a step that you can optionally perform during post-installation as described in *Oracle Secure Backup Installation Guide*, then skip Steps 3 and 4 in the following procedure.
- You are using the Oracle Secure Backup Web tool to configure the domain. "Using the Web Tool" on page 3-2 provides an introduction to the Web tool.

> **Note:** If you plan to use Oracle Secure Backup with RMAN, then see Chapter 6, "Using Recovery Manager with Oracle Secure Backup". The RMAN chapter explains how to use Enterprise Manager to configure Oracle Secure Backup and perform database backup and recovery.

- You accept the default mode of security described in "Default Security Configuration" on page 2-37. In this case no additional security configuration is required. You need only ensure that the hosts with the administrative server and media server roles have sufficient physical and network security.

You can configure your administrative domain in the following steps:

1. Use the Web tool to log in to the administrative domain as `admin`. You created this user and set the password when you installed Oracle Secure Backup on the administrative server.
2. If necessary, configure defaults and policies for the administrative domain. For example, you could configure default media retention values or NDMP authentication information.

   This task is described in "Configuring Defaults and Policies" on page 4-3.
3. Configure the media servers and clients. Optionally, you can configure a subset of the hosts now and add the remaining hosts later.

   This task is described in "Configuring Hosts" on page 4-6.
4. Configure tape devices.

   This task is described in "Configuring Tape Devices" on page 4-14.

5. If necessary, configure classes and users. For example, you may want to create an Oracle Secure Backup user that can make backups but does not have full administrator rights.

   These tasks are described in "Configuring Classes" on page 4-24 and "Configuring Users" on page 4-26.

   > **Note:** In this step you can specify user accounts for unprivileged backup and restore operations. Unprivileged operations run under the specified operating system accounts rather than as `root` (UNIX/Linux) or a member of the Administrator group (Windows). See "About User Configuration" on page 4-27 for more information.

6. If necessary, configure backup and media settings in preparation for setting up backup schedules. This stage of configuration is described in Chapter 5, "Configuring Backup and Media Settings" and includes the following tasks:

   a. Configure media families.

      This task is described in "Configuring Media Families" on page 5-2.

   b. Configure database backup storage selectors.

      This task is described in "Configuring Database Backup Storage Selectors" on page 5-5.

   c. Configure job summary schedules.

      This task is described in "Configuring Job Summary Schedules" on page 5-8.

   After you have configured the administrative domain, you are ready to set up your backup schedules and perform on-demand backups. These tasks are explained in Chapter 7, "Backing Up File System Data".

Configuring Defaults and Policies

As explained in "Defaults and Policies" on page 2-30, defaults and policies are configuration data that control how Oracle Secure Backup operates within an administrative domain. Policies are divided into classes.

This section contains the following topics:

- About Defaults and Policies Configuration
- Displaying the Defaults and Policies Page
- Setting a Policy
- Resetting a Policy

About Defaults and Policies Configuration

In most cases, the policy defaults are sufficient for your administrative domain, so this step is optional. Nevertheless, you can review the defaults and make changes where necessary. Which changes are necessary depends on the specifics of your network environment.

Table 4–1 lists classes of policies that you may want to review or change.

Table 4–1 Policy Classes

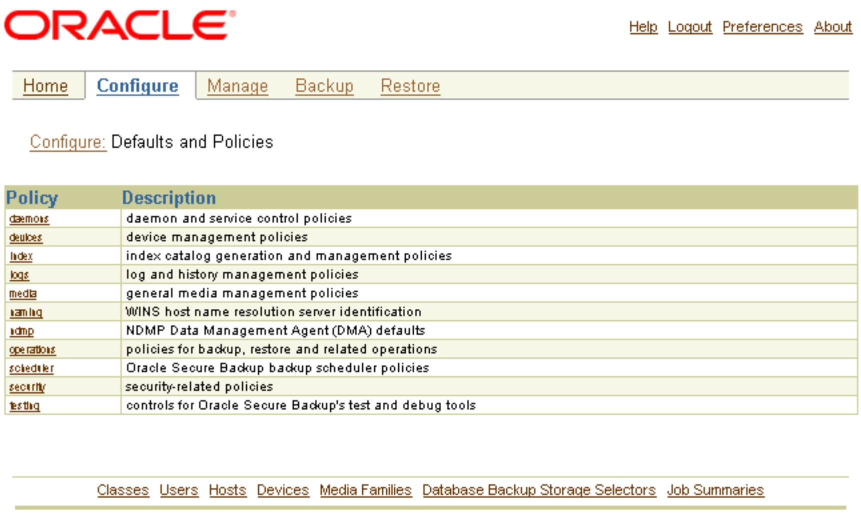
Policy Class	Description
Media	Controls media management for the administrative domain. For example, you can choose whether tapes are required to have barcodes and set the retention period and write window for volumes in the default media family.
NDMP	Controls settings applicable to hosts that use NDMP access mode. For example, you can configure backup environment variables or specify a user name for authentication.
Operations	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	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	Controls aspects of administrative domain security. For example, you can enable SSL encryption for backup data in transit or set the key size for host identity certificates. "Configuring Security for the Administrative Domain" on page 11-7 explains how to change the default security policies.

Refer to the "Defaults and Policies" appendix in *Oracle Secure Backup Reference* for descriptions of the policies and valid settings for the classes listed in Table 4–1. Keep this information handy as you review the current policy settings for your domain.

Displaying the Defaults and Policies Page

In the Advanced section of the Configure page, click **Defaults and Policies** to display the page shown in Figure 4–1. This page lists the policy classes.

Figure 4–1 Defaults and Policies Page



Policy	Description
daemons	daemon and service control policies
devices	device management policies
index	index catalog generation and management policies
logs	log and history management policies
media	general media management policies
naming	WINS host name resolution server identification
ndmp	NDMP Data Management Agent (DMA) defaults
operations	policies for backup, restore and related operations
scheduler	Oracle Secure Backup backup scheduler policies
security	security-related policies
testing	controls for Oracle Secure Backup's test and debug tools

See Also: *Oracle Secure Backup Reference* to learn about the policy commands in the `obtool` command-line interface and the descriptions of the classes and policies

Setting a Policy

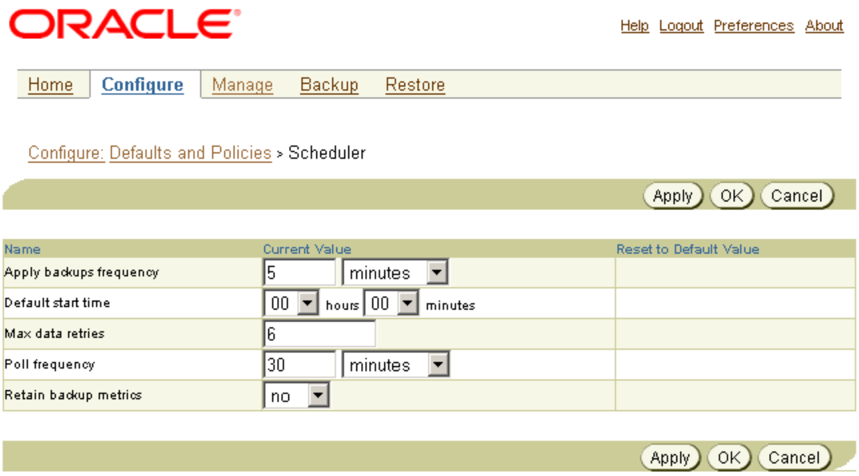
Before changing a policy setting, refer to the "Defaults and Policies" appendix in *Oracle Secure Backup Reference*. This appendix contains extensive descriptions of the policies and describes valid settings. Typically, should not need to change the default settings.

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 4–2 shows the Scheduler page.

Figure 4–2 Scheduler Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Defaults and Policies > Scheduler
Apply OK Cancel

Name	Current Value	Reset to Default Value
Apply backups frequency	5 minutes	
Default start time	00 hours 00 minutes	
Max data retries	6	
Poll frequency	30 minutes	
Retain backup metrics	no	

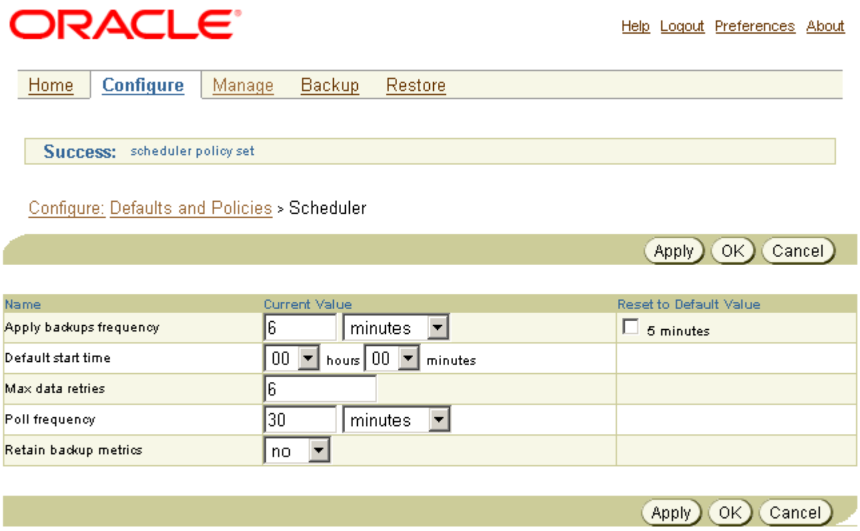
2. Change the settings of one or more policies. Refer to the "Defaults and Policies" appendix in *Oracle Secure Backup Reference* for explanations of the policies.

3. Choose 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 Web tool displays the default value for the policy in the Reset to Default Value column. Figure 4–2 shows the Scheduler page after the backup frequency has been changed to 6 minutes from the default of 5 minutes.

Figure 4–3 Scheduler Page



Success: scheduler policy set

Configure: Defaults and Policies > Scheduler

Name	Current Value	Reset to Default Value
Apply backups frequency	6 minutes	□ 5 minutes
Default start time	00 hours 00 minutes	
Max data retries	6	
Poll frequency	30 minutes	
Retain backup metrics	no	

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. Check box in the Reset to Default Value column for the policy that you are resetting.
3. Click **Apply** or **OK**.

Configuring Hosts

This section explains how to define, change, and remove hosts. This section contains the following topics:

- About Host Configuration
- Displaying the Hosts Page
- Adding a Host
- Pinging a Host
- Displaying or Editing Host Properties
- Adding Backup and Restore Environment Variables to an NDMP Host
- Configuring Preferred Network Interfaces (PNI)
- Removing a Host
- Renaming a Host
- Updating a Host

About Host Configuration

Although it is assumed that you have installed Oracle Secure Backup on the network hosts (except filers and other hosts that use NDMP access mode), you have not yet made the administrative server aware of the other hosts in your domain. This section explains how to configure the identity and membership of the hosts in your domain.

For hosts on which Oracle Secure Backup is installed, you can configure attributes such as the following:

- Host name
- IP address
- Role
- Host accessibility (whether the host is in service or not in service)

For hosts that use NDMP access mode, you can configure the same host attributes in the preceding list, but also configure the following attributes:

- NDMP authorization type
- NDMP password
- TCP port number for use with NDMP

Refer to the `mkhost` description in *Oracle Secure Backup Reference* for a complete account of host attributes.

It is recommended that you configure your hosts as follows:

1. Configure the media servers.

   This task is described in "Adding a Host" on page 4-8.

2. Configure the clients.

   In some cases, your media servers and administrative server are the only clients, so you can skip this step. This task is described in "Adding a Host" on page 4-8.

3. Ping all hosts in the domain to make sure that they are accessible.

   You can use the ping operation to determine whether a host is responsive to requests from Oracle Secure Backup. This task is described in "Pinging a Host" on page 4-11.

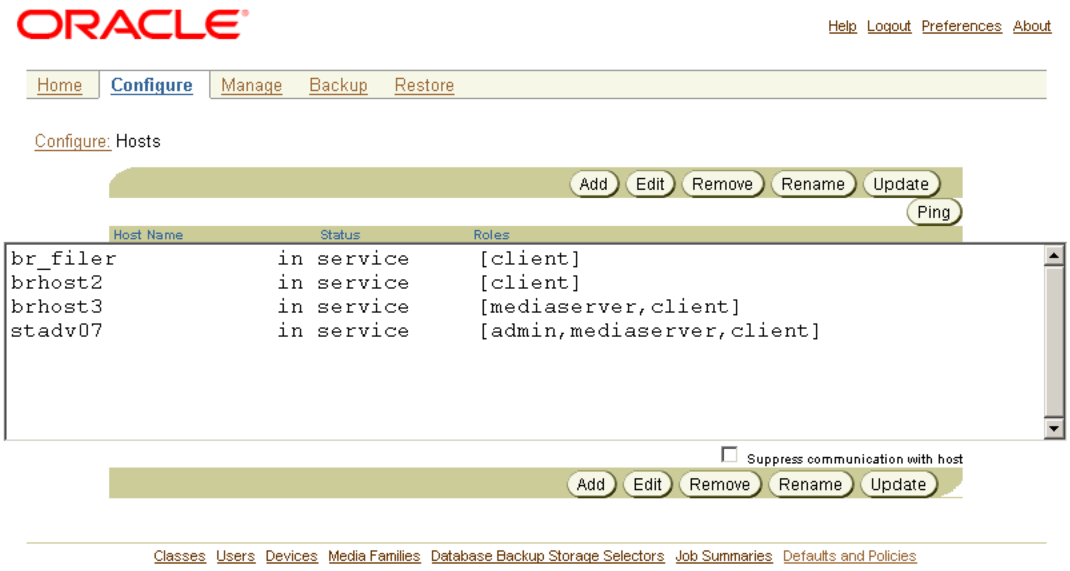
4. If necessary, modify, rename, or remove media servers and clients.

   These tasks are described in "Displaying or Editing Host Properties" on page 4-11, "Renaming a Host" on page 4-13, and "Removing a Host" on page 4-12.

Displaying the Hosts Page

Click **Hosts** in the Configure page to display the Hosts page, which is shown in Figure 4–4. The Hosts page lists the host name, status, and roles attributed to the host. You can perform all host configuration tasks in this page or in pages to which it is linked.

Figure 4–4 Hosts Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Hosts
Add Edit Remove Rename Update
Ping
Host Name
Status
Roles
□ Suppress communication with host
Add Edit Remove Rename Update
Classes Users Devices Media Families Database Backup Storage Selectors Job Summaries Defaults and Policies

```
br_filer            in service     [client]
brhost2             in service     [client]
brhost3             in service     [mediaserver,client]
stadv07             in service     [admin,mediaserver,client]
```

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

Adding a Host

To add a new host to an administrative domain:

1. From the Home page, click the **Configure** tab.
2. Click **Hosts** in the Basic section to display the Hosts page.
3. Click **Add** to add a host.

   The Web tool displays a form for entering a host name.
4. In the **Host** box, enter the name of the host.

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

   The host name must be unique among all Oracle Secure Backup host names.

   If you do not configure explicit IP interface names for this host (see the following step), then Oracle Secure Backup considers this host name to be the IP interface name for the host. As such, it must be resolvable through your site's host name resolution system (usually DNS or NIS) to the IP address of a network interface on the host.
5. In the **IP Interface name(s)** box, optionally enter one or more IP interface names. Separate multiple entries with a comma.

   If you define one or more IP names, then you can specify either resolvable host names or IP addresses. For example, you can use `myhost.oracle.com` for a host name or 141.146.8.66 for an IP address.

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

If this box is not empty, then Oracle Secure Backup never uses the user-assigned host name to get the host's IP address; instead, it considers each name in this IP address field until it finds one that resolves to a working IP address. If preferred network interfaces (PNI) are used, then Oracle Secure Backup considers the PNI address first.

If you leave this box blank, then Oracle Secure Backup uses the name you assigned to the host in the previous step as the resolvable IP name for the host.

6. In the **Status** list, select one of the following:

   - **in service**

     Select this option to indicate that the machine is logically available to perform backup and restore operations.

   - **not in service**

     Select this option to indicate that the machine is logically unavailable to perform backup and restore operations.

7. In the **Roles** list, select one or more administrative domain roles for the host. You can select multiple roles. Your choices are the following:

   - **admin**
   - **client**
   - **mediaserver**

   Note: See "Administrative Domains" on page 1-5 to learn about these roles.

8. In the **Access method** box, select an access method for the host (if applicable). Your choices are the following:

   - **ob**

     Select this option if the host has Oracle Secure Backup installed.

   - **NDMP**

     Select this option if the host does not have Oracle Secure Backup installed—for example, a Network-Attached Storage (NAS) device—and uses the Network Data management Protocol (NDMP) to perform all backup and restore operations.

   Note: NDMP is an open standard that defines a common architecture for the way heterogeneous file servers on a network are backed up. This protocol permits the creation of a common agent used by the central backup application to back up servers running different operating systems.

If you select **ob**, then perform Step 9 and then jump to Step 16. If you select **NDMP**, then skip to Step 10 and perform all subsequent steps.

9. In **Public and private key sizes**, select a size for the public/private key associated with the identity certificate for this host.
10. In the **NDMP authorization type** list, select an authorization type. The authorization type defines the way in which Oracle Secure Backup authenticates itself to the NDMP server. Typically, you should use the default setting.

    Your choices are the following:

    - **default**

      Select this option to use the value of the Authentication type for the NDMP policy.

    - **none**

      Select this option to attempt to use the NDMP server from Oracle Secure Backup and provide no authentication data. This technique is usually unsuccessful.

    - **negotiated**

      Select this option to negotiate with the NDMP server to determine the best authentication mode to use.

    - **text**

      Select this option to use plain (unencrypted) text to authenticate.

    - **md5**

      Select this option to use the MD5 digest algorithm to authenticate.

    See Also: "Configuring Defaults and Policies" on page 4-3 to learn about NDMP-related policies

11. In the **Username** box, enter the name used to authenticate Oracle Secure Backup to this NDMP server. If left blank, then the Oracle Secure Backup uses the name in the NDMP policy.
12. In the **Password** list, select one of the following options:

    - **Use default password**

      Select this option to use the default NDMP password.

    - **Use text password**

      Select this option to enter a password.

    - **Set to NULL**

      Check this box to use a NULL password.

    The password is used to authenticate Oracle Secure Backup to this NDMP server.

13. In the **Backup type** box, enter an NDMP backup type. A backup type is the name of a backup method supported by the NDMP Data Service running on a host. Backup types are defined by each Data Service provider.
14. In the **Protocol Version** list, select **2**, **3**, **4**, or **as proposed by server**.

    The NDMP protocol has three public versions, called 2, 3, and 4. Typically, it is acceptable to let Oracle Secure Backup choose the protocol version that the server proposes when the connection is established. If necessary (for example, for testing) you can change the NDMP protocol version with which Oracle Secure Backup communicates to this server.

15. In the **Port** box, enter a port number. Typically, the TCP port (10000) in the NDMP policy is used. You can specify another port if this server uses a port other than the default.

> **Note:** You can add backup and restore environment variables only *after* you create the host. Refer to "Adding Backup and Restore Environment Variables to an NDMP Host" on page 4-12.

16. Check the **Suppress communication with host** checkbox if you want to add a host to the administrative domain that is currently not accessible on the network.
17. Click **Apply**, **OK**, or **Cancel**.

Pinging a Host

You can use the ping operation to determine whether a host is responsive to requests from Oracle Secure Backup.

Ping attempts to establish a TCP connection to the host on each of the IP addresses you have configured for it. For hosts that use primary access mode, connection occurs through TCP port 400; for hosts that use the NDMP access mode, connections occur through the configured NDMP TCP port, usually 10000.

Oracle Secure Backup reports the status of each connection attempt and immediately closes each connection that has been established successfully.

This operation is useful for ensuring that a host is responsive on all of its configured IP addresses.

To ping a host:

1. From the Hosts page, select a host to ping.
2. Click **Ping**.

   A status line appears on the page with the results of the operation.

Displaying or Editing Host Properties

To display or edit host properties:

1. From the Hosts page, select the name of the host whose properties require editing.

   Click the **Suppress communication with host** checkbox to edit a host that is not accessible through the network.
2. Click **Edit**.

   The Web tool displays a page with details for the host you selected.
3. Make any required changes to the host properties. If you only want to view the properties, then do not make changes.
4. Click **Apply**, **OK**, or **Cancel**.
5. See "Configuring Preferred Network Interfaces (PNI)" in the following section to specify, on a client-by-client basis, which of the server's network interfaces should be used to transmit data to be backed up or restored.

Adding Backup and Restore Environment Variables to an NDMP Host

After you configure and create an NDMP host, you can edit the host to add backup and restore environment variables.

To add backup and restore variables:

1. In the box that displays next to the **Backup environment vars** or **Restore environment vars** box, enter a name-value pair.
2. Click **Add** to add the name-value pair as an environment variable.

   For example, enter **A=B** or **"Name A"="Value B"** (if the name or value includes spaces). Select an existing environment variable pair and click **Remove** to remove the pair.

Configuring Preferred Network Interfaces (PNI)

Multiple physical data paths can exist between a client, which contains primary storage to be backed up or restored, and a server, which controls secondary storage devices that write and read the backup media or serves as the administrative server. The PNI (Preferred Network Interface) specifies the network interface that should be used to transmit data to be backed up or restored.

To configure a preferred network interface:

1. Follow Steps 1 and 2 in "Displaying or Editing Host Properties" on page 4-11 to select a host.
2. Click **Preferred Network Interfaces**.
3. In the **IP Address** list, select an IP address or name. The IP address or name identifies the network interface that the clients you select will use when communicating with the server.
4. Select one or more clients to use this IP address or DNS name from the **Host list** box.
5. Click **Add**.

   The Web tool displays the PNI in the **IP Address:Host List** box.

Removing a PNI

To remove a PNI:

1. In the **IP Address:Host List** box, select the name of the PNI that you want to remove.
2. Click **Remove**.

Removing a Host

This section explains how to remove a host from an Oracle Secure Backup administrative domain.

When you remove a host, Oracle Secure Backup destroys all information pertinent to that host, including:

- Configuration data
- Incremental backup state information
- Metadata in the backup catalog for this host

- Device attachments
- Preferred network interface references

Moreover, when you remove a UNIX or Windows host, Oracle Secure Backup contacts that host and directs it to delete the administrative domain membership information it maintains locally. You can suppress this communication if the host is no longer accessible.

To remove a host:

1. From the Hosts page, select the name of the host that you want to remove.

   Check **Suppress communication with host** to remove a machine that is not connected to the network.

2. Click **Remove**.

   Oracle Secure Backup prompts you to confirm the removal of the host.

3. Click **Yes** to remove the host or **No** to leave the host undisturbed.

   If you selected **Yes**, then Oracle Secure Backup removes the host and returns you to the **Host** page.

Renaming a Host

To rename a host:

1. In the Hosts page, select the name of the host to rename.

   Check **Suppress communication with host** to rename a machine that is not connected to the network.

2. Click **Rename**.

   The Web tool displays a message box in which you can enter the new name.

3. Enter the new name for the host in the text box.
4. Click **Yes** to rename the host or **No** to leave the host name unchanged.

   If you select **Yes**, then Oracle Secure Backup renames the host and returns you to the Host page.

Updating a Host

This section explains how and when to update a host. When you add or modify a host in an Oracle Secure Backup administrative domain, Oracle Secure Backup exchanges messages with that host to inform it of its new state. If no communication is possible (such as when you have checked the **Suppress communication with host checkbox**) during an add or edit operation, then the host contains out-of-date configuration information. Use Update Host to send fresh state information to the host.

Updating is useful only for hosts that use the primary access method. NDMP-accessed hosts do not maintain any Oracle Secure Backup state data and are therefore not eligible for this function.

To update a host:

1. From the Host page, select the name of the host to be updated.
2. Click **Update**.

Configuring Tape Devices

This section explains how to configure secondary storage devices for use with Oracle Secure Backup. This section contains the following topics:

- About Tape Device Configuration
- Displaying the Devices Page
- Adding a Device
- Configuring a Tape Library
- Configuring a Tape Drive
- Editing Device Properties
- Removing a Device
- Renaming a Device
- Configuring a Device Attachment
- Displaying Device Properties
- Pinging a Device
- Discovering NDMP-Based Tape Devices Automatically

About Tape Device Configuration

This section explains how to configure tape libraries and tape drives for use with Oracle Secure Backup. For both tape drives and tape libraries, you can configure attributes such as the following:

- The name of the device
- The attachment, which is the description of a physical or logical connection of a device to a host
- Whether the device is in service, that is, logically accessible to Oracle Secure Backup

For tape drives, you can configure additional attributes such as the following:

- The library in which the tape drive is housed, if the drive is not standalone
- A range of library storage elements that can be used by the device, if the drive is in a tape library

For tape libraries, you can additionally set attributes such as the following:

- Whether automatic cleaning is enabled
- Whether a barcode reader is present
- The duration of a cleaning interval

Refer to the `mkdev` description in *Oracle Secure Backup Reference* for a complete account of tape device attributes.

It is recommended that you configure your tape devices as follows:

1. Disable any system software that scans and opens arbitrary SCSI targets before configuring Oracle Secure Backup tape devices. If Oracle Secure Backup has to contend with other system software (such as monitoring software) for access to tape libraries and drives, then unexpected behavior can result.

2. Configure tape libraries or tape drives locally attached to your media servers.

   > **Note:** Oracle Secure Backup automatically assigns the media server role to an administrative server when you configure an attached tape device.

   This tasks are described in "Configuring a Tape Library" on page 4-17 and "Configuring a Tape Drive" on page 4-19.

3. Configure tape devices that are network-accessible but are not locally attached to hosts. In this case, you must you must choose which media servers should control the devices.

   This tasks are described in "Configuring a Tape Library" on page 4-17 and "Configuring a Tape Drive" on page 4-19.

4. Discover tape devices attached to hosts that use NDMP access mode.

   Oracle Secure Backup can automatically detect NDMP-attached devices and configure them for the administrative domain. This task is described in "Discovering NDMP-Based Tape Devices Automatically" on page 4-23.

5. Ping each tape device to make sure that it is accessible by Oracle Secure Backup.

   This task is described in "Pinging a Device" on page 4-23.

6. Inventory each library and then list its volumes.

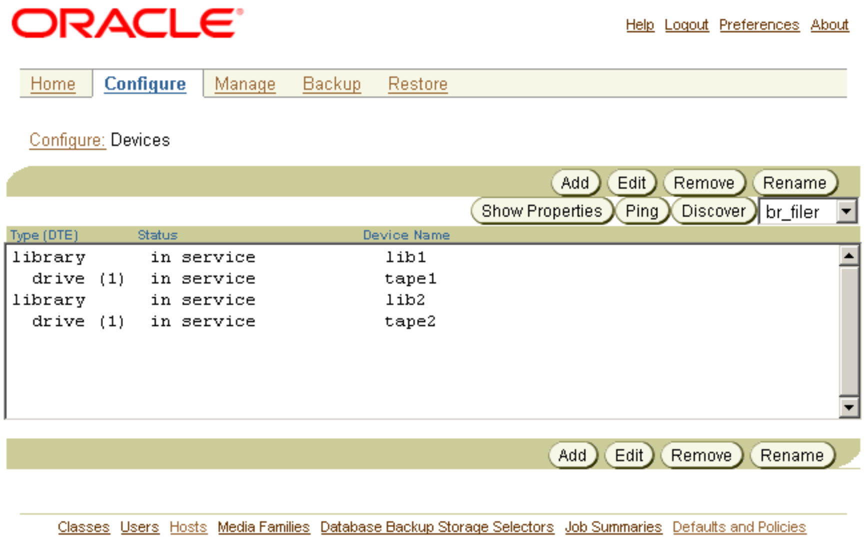
   Volumes in a library should show either a barcode or the status `unlabeled`. If a library shows a slot as `occupied`, then this slot is in an invalid state.

   This task is described in "Updating an Inventory" on page 9-6 and "Browsing Volumes" on page 10-7.

Displaying the Devices Page

The Devices page, which is shown in Figure 4–5, lists the tape libraries and tape drives that are currently in the administrative domain. The page lists the type, status, and name of every device.

Figure 4–5 Devices Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Devices
Add Edit Remove Rename
Show Properties Ping Discover br_filer
Add Edit Remove Rename
Classes Users Hosts Media Families Database Backup Storage Selectors Job Summaries Defaults and Policies

```
Type (DTE)          Status                  Device Name
library             in service              lib1
  drive  (1)        in service              tape1
library             in service              lib2
  drive  (1)        in service              tape2
```

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

Adding a Device

To add a tape device to an administrative domain:

1. From the Home page, click the **Configure** tab.
2. Click **Devices** in the Basic section to display the Devices page.

   You can add new devices in one of two ways:

   - By automatically discovering them. Oracle Secure Backup can automatically discover and configure secondary storage devices connected to certain types of NDMP servers, such as Network Appliance filers. See "Editing Device Properties" on page 4-20 to use automatic device discovery.
   - By adding them manually. See the next step to define devices that cannot be automatically discovered.

   Note: Discovery is a way to learn out about new devices or otherwise unconfigured devices that exist on the host. This technique works only for NDMP devices.

3. Click **Add** to add a device.
4. In the **Device** box, enter a name for the device.

   The name must start with an alphanumeric character. It can only contain letters, numerals, dashes, underscores, or periods. It may contain at most 127 characters.

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

5. In the **Type** list, select one of the following:

   - **library**

If you select this option, then see "Configuring a Tape Library" on page 4-17 to continue.

- **tape**

  If you select this option, then see "Configuring a Tape Drive" on page 4-19 to continue.

> **Note:** If you a configuring a tape device housed within a tape library, then configure the library first. See "Configuring a Tape Library" on page 4-17 for more information.

Configuring a Tape Library

This section explains how to configure a library for use with Oracle Secure Backup. A library is a medium changer that accepts SCSI commands to move media between storage locations and drives.

Before configuring your library, ensure that you followed the instructions in "Configuring Tape Devices" on page 4-14.

To configure a tape library:

1. In the **Status** list, select one of the following options:

   - **in service**

     Select this option to indicate that the device is logically available to perform Oracle Secure Backup backup and restore operations.

   - **not in service**

     Select this option to indicate that the device is logically unavailable to perform backup or restore operations.

   - **auto not in service**

     This option indicates that the device is logically unavailable to perform backup or restore operation and is set automatically as a result of a failed operation.

2. In the **Debug mode** list, select **yes** or **no**. The default is **yes**.

3. In the **World Wide Name** box, enter a world-wide name if one exists for the device.

   Oracle Secure Backup supports devices whose operating system-assigned logical names (for example, `nrst0a`) can vary at each operating system restart. This situation applies to Fibre Channel-attached tape drives and libraries connected to Network Appliance filers. You can refer to these raw devices with their world-wide names (for example, `nr.WWN[2:000:0090a5:0003f7]L1.a`), rather than their logical names.

   This option is most useful for tape drives and libraries attached to Network Appliance filers. Unlike the logical name, the world-wide name does not change across reboots.

   Any substring of the attachment's raw device name that is the string `$WWN` is replaced with the value of the WWN each time the device is opened. For example a usable raw device name for a SAN-attached Network Appliance filer is `nr.$WWN.a`, specifying a no-rewind, best-compression device having the World Wide Name found in the device object.

The WWN is usually auto-discovered by the device discovery function in Oracle Secure Backup; however, you can enter it manually if necessary.

4. In the **Barcode reader** list, select one of the following options to indicate whether a barcode reader is present. A barcode is a symbol code that is physically applied to volumes for identification purposes; some libraries have an automated means to read barcodes, which Oracle Secure Backup supports.

    - **yes**

      Select this option to indicate that the library has a barcode reader.

    - **no**

      Select this option to indicate that the library does not have a barcode reader.

    - **default**

      Select this option to indicate that Oracle Secure Backup should automatically determine the barcode reader using information reported by either the library, the external device file, or both.

5. In the **Barcode required** list, select **yes** or **no**. If you specify **yes**, and if a tape in the library does not have a readable barcode, then Oracle Secure Backup refuses to use the tape. This option is configurable for each library.

   Typically, Oracle Secure Backup does not discriminate between tapes with readable barcodes and those without. This policy ensures that Oracle Secure Backup can always solicit a tape needed for restore by using both the barcode and the volume ID.

6. See "Configuring Automatic Tape Cleaning for a Library" on page 4-18 for instruction on using the **Auto clean**, **Clean interval (duration)**, and **Clean using emptiest** options.

7. In the **Unload required** list, select **yes**, **no** or **default** to specify whether or not an unload operation is required before moving a tape from a drive to a storage element.

   Typically, you should leave this set to default **yes**, which means the value comes from the external device table `ob_drives`. If you encounter difficulties, however, particularly timeouts waiting for offline while unloading a drive, then select **no**.

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

9. After the device has been created, you can select **Attachments** to configure device attachments. See "Configuring a Device Attachment" on page 4-21 for more information.

Configuring Automatic Tape Cleaning for a Library

Oracle Secure Backup can automatically clean tape drives in a library. A cleaning cycle is initiated either when a drive reports that it needs cleaning or when a specified usage time has elapsed.

Oracle Secure Backup checks for cleaning requirements when a cartridge is either loaded into or unloaded from a drive. If at that time a cleaning is required, Oracle Secure Backup loads a cleaning cartridge, waits for the cleaning cycle to complete, replaces the cleaning cartridge in its original storage element, and continues with the requested load or unload.

To configure automatic cleaning for a library:

1. In the **Auto clean** list, select **yes** to enable automatic drive cleaning or **no** to disable it. You can also manually request that a cleaning be performed whenever a drive is not in use.

   > **Note:** Not all drives can report that cleaning is required. For those drives, you must define a cleaning interval.

   In the **Clean interval (duration)** box, enter a value and then select the cleaning frequency from the adjacent list. This interval is the amount of time a drive is used before a cleaning cycle is initiated. If automatic drive cleaning is enabled, then this duration indicates the interval between cleaning cycles.

2. In the **Clean using emptiest** box, select one of the following options:

   - **yes**

     Select this option to specify the emptiest cleaning tape, which causes cleaning tapes to "round robin" as cleanings are required.

   - **no**

     Select this option use the fullest cleaning tape, which causes each cleaning tape to be used until it fills, then the next cleaning tape fills, and so on.

   If there are multiple cleaning tapes in a library, then Oracle Secure Backup needs to decide which to use. If you do not otherwise specify, Oracle Secure Backup chooses the cleaning tape with the fewest number of cleaning cycles remaining.

3. Click **Apply**, **OK**, **Cancel**, or **Attachments** (see "Configuring a Device Attachment" on page 4-21).

Configuring a Tape Drive

Before configuring a tape drive, ensure that you followed the instructions in "Configuring Tape Devices" on page 4-14.

To configure tape drives for use with Oracle Secure Backup:

1. Select the **Status**, **Debug mode**, and **World Wide Name**. Refer to Steps 1 through 3 in "Configuring a Tape Library" on page 4-17 for an explanation of these options.

2. In the **Library** list, select a library name if the drive is located in a library.

3. In the **DTE** box, enter the Data Transfer Element (DTE). DTE is the SCSI-2 name for a tape drive in a library. DTEs are numbered 1 through *n* and are used to identify drives in a library.

   > **Note:** This option is not available for standalone tape drives.

4. In the **Automount** box, select **yes** (default) or **no** to specify whether automount mode is on or off. Enable the automount mode if you want Oracle Secure Backup to mount tapes for backup and restore operations without operator intervention.

5. In the **Error rate** box, enter an error rate percentage or leave this box blank to accept the default setting. The default is **8**.

   The error rate is the ratio of restored write errors that occur during a backup job divided by the total number of blocks written, multiplied by 100. If the error rate for any backup is higher than this setting, then Oracle Secure Backup displays a warning message in the backup transcript.

Oracle Secure Backup also issues a warning if it encounters a SCSI error when trying to read or reset the drive's error counters. Some drives do not support the SCSI commands necessary to perform these operations. To avoid these warnings, error rate checking can be disabled by checking **None**.

6. In the **Blocking factor** box, enter the blocking factor or leave this box blank to accept the default setting. The default is 128 bytes.

   A blocking factor specifies how many 512-byte records to include in each block of data written to tape. By default, Oracle Secure Backup writes 64K blocks to tape (blocking factor 128).

7. In the **Max Blocking factor** box, enter the maximum blocking factor.

   The largest value permitted for the maximum blocking factor is 4096. This represents a maximum tape block size of 2MB. This maximum is subject to device and operating system limitations that can reduce this maximum block size.

8. In the **Drive usage** box, enter the amount of time a drive has been in use since it was last cleaned and then select the time unity from the adjacent list.

9. Leave the **Current tape** box empty during initial configuration. This box will automatically be filled in after an inventory has been taken.

10. In the **Use list** group, select one of the following options to configure the use list:

    - **Storage element range or list**

      Click this button to select a numerical range of storage element addresses. Enter a range in the box, for example, **1-20**.

    - **All**

      Click this button to specify all storage elements. For libraries with single drives, you can select this option to use all tapes.

    - **None**

      Select this button to indicate that no storage elements have yet been specified. This is the default setting. If you select **All** or **Storage element range or list**, then this option is no longer visible.

    Oracle Secure Backup allows all tapes to be accessed by all drives. The use list enables you to divide the use of the tapes for libraries containing multiple drives in which you are using more than one drive to perform backups. For example, you might want the tapes in the first half of the storage elements to be available to the first drive, and those in the second half to be available to the second drive.

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

Editing Device Properties

To edit the properties for an existing device:

1. From the Devices page, select the name of the device.

2. Click **Edit**.

   The Web tool displays a page with details for the device you selected.

3. Make any required changes.

4. Click **Apply**, **OK**, **Cancel**, or **Attachments** (see "Configuring a Device Attachment" on page 4-21 to configure attachments to the device).

Removing a Device

To remove a device:

1. From the Devices page, select the name of the device.
2. Click **Remove**.

   Oracle Secure Backup prompts you to confirm the removal.
3. Click **Yes** to remove the device.

   Oracle Secure Backup informs you that the device was successfully removed and returns you to the **Device** page.

Renaming a Device

To rename a device:

1. From the Devices page, select the name of the device.
2. Enter the new name for the device in the text box.
3. Click **Rename**.

   Oracle Secure Backup prompts you to confirm the removal.
4. Click **Yes** to accept the new name.

   The Web tool informs you that the device was successfully renamed and returns you to the **Device** page.

Configuring a Device Attachment

As explained in "Device Names and Attachments" on page 2-17, Oracle Secure Backup maintains a distinction between a device and the means by which the device is connected to a host. Each configurable device can have one or more attachments, where each attachment describes a data path between a host and the device. Typically, an attachment includes the identity of a host plus a UNIX device special file name, a Windows device name, or NAS device name. In rare cases, Oracle Secure Backup requires additional information to complete the attachment definition.

Before proceeding to configure the device attachment, refer to the description of the `mkdev` command in *Oracle Secure Backup Reference*. The description of the *aspec* placeholder describes the syntax and naming conventions for device attachments.

To configure a device attachment:

1. After adding or editing a device, click the **Attachments** button.
2. In the **Host** list, select a host.
3. In the **Raw device** box, enter the raw device name. This is the operating system's name for the device, such as a UNIX device special file. For example, a library name might be `/dev/obl0` on Linux and `//./obl0` on Windows.

> **Note:** Steps 4 through 8 need to be performed only for certain hosts running certain NDMP version 2 and 3 servers, such as Network Appliance Data ONTAP 5.1 or 5.2.

4. In the **ST device** box, enter a device name.
5. In the **ST target** box, enter a target number.
6. In the **SCSI device** box, enter a SCSI device.
7. In the **ST controlle**r box, enter a bus target number.
8. In the **ST lun** box, enter a SCSI logical unit number for the device.
9. Click **Add** to add the attachment.

Editing a Device Attachment

To change an existing device attachment on the Attachments page:

1. In the **host:raw device** box, select the device attachment you want to change.
2. Click **Edit**.

   The Web tool displays a page with details for the device attachment you selected.
3. Make the required changes.
4. Click **Add** to change the device attachment.

Removing a Device Attachment

To remove a device attachment from a tape drive or library on the Attachments page:

1. In the **host:raw device** box, select the name of the device attachment.
2. Click **Remove**.

Displaying Device Attachment Properties

You can display device attachment properties from the Devices page.

To display attachment properties:

1. Select the name of the device for which you want to view attachment properties.
2. Click the **Show Properties** button.

   The Web tool displays a page that displays various properties, including device attachments, for the device you selected.
3. Click **Close** to exit the page.

Pinging a Device Attachment

Oracle Secure Backup enables you to determine whether a device is accessible to Oracle Secure Backup using a specific attachment.

When you ping a device, Oracle Secure Backup performs the following steps:

1. Establishes a logical connection to the device
2. Inquires about the device's identity data with the SCSI INQUIRY command
3. Closes the connection

If the attachment is remote from the host running the Web tool (or `obtool`), then Oracle Secure Backup establishes an NDMP session with the remote media server to effect this function.

To ping an attachment from the Attachments page:

1. In the **host:raw device** box, select the attachment to ping.

2. Click the **Ping** button.

   The Web tool opens a new window that describes the status of the attachment.

3. Click **Close** to exit the page.

Displaying Device Properties

The Web tool a device is in service, which host or hosts the device is connected to, the device type, and various other details relating to devices.

> **Note:** If a device is in service, it means the device can be used by Oracle Secure Backup; if it is not in service, then it cannot be used by Oracle Secure Backup. When a device is taken out of service, no more backups are dispatched to it.

To display device properties:

1. In the Device page, select the name of the device for which you want to display properties.

2. Click the **Show Properties** button.

   The Web tool displays a page with the properties for the device you selected.

Pinging a Device

Oracle Secure Backup enables you to determine whether a tape device is accessible to Oracle Secure Backup using any available attachment.

Pinging a library causes all of its in service member tape drives to be pinged as well.

To ping a device:

1. In the Devices page, select a device to ping.

2. Click the **Ping** button.

   The Web tool displays the status of the operation.

Discovering NDMP-Based Tape Devices Automatically

Oracle Secure Backup can detect changes in device configuration for some types of NDMP-accessed hosts and, based on this information, automatically update the administrative domain's device configuration.

Oracle Secure Backup detects and acts on these kinds of changes:

- Devices that were not previously configured but have appeared. For each such device, Oracle Secure Backup creates a new device with an internally-assigned name and configures a device attachment for it.
- Devices that were previously configured for which a new attachment has appeared. For each, Oracle Secure Backup adds an attachment to the existing device.
- Devices that were previously configured for which an attachment has disappeared. For each, Oracle Secure Backup removes the attachment from the device.

Oracle Secure Backup detects multiple hosts connected to the same device by comparing the serial numbers reported by the operating system. Oracle Secure Backup also determines whether any discovered device is accessible by its serial number; if so, it configures each device attachment to reference the serial number instead of any logical name assigned by the operating system.

To discover a device:

1. In the list of hosts, select the name of an NDMP host.
2. Click **Discover**.

   The Web tool displays a message in the status area, which can also be a message stating that no changes to device configuration are discovered.
3. Click **OK** to return to the Devices page.

Configuring Classes

As explained in "Oracle Secure Backup Classes and Rights" on page 1-9, a class defines a set of rights that are granted to a user. A class can include multiple users, but each user is a member of one and only one class.

In most cases, the default classes are sufficient. Refer to *Oracle Secure Backup Reference* for a complete account of the rights that belong to each class.

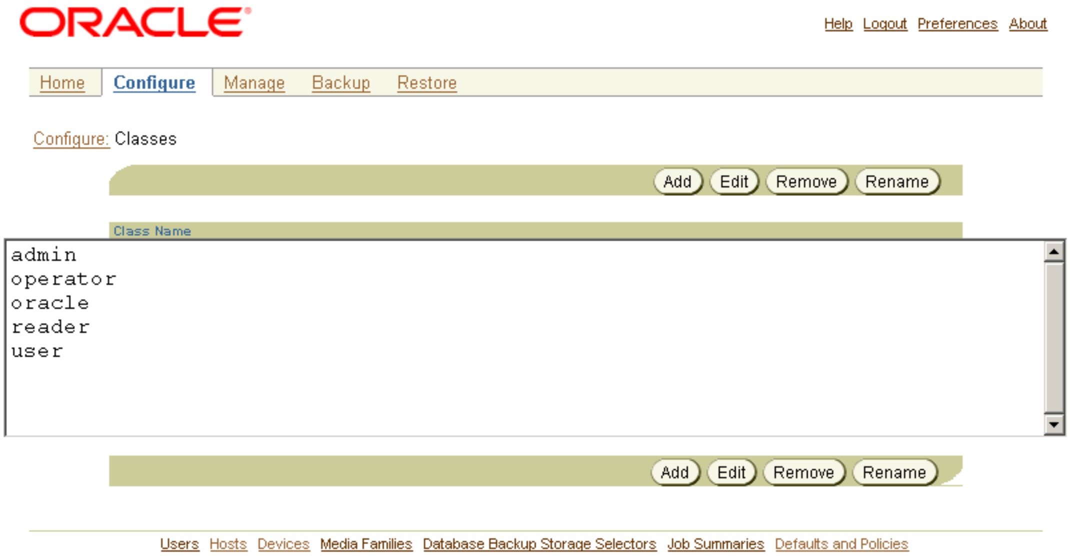
This section contains the following topics:

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

Displaying the Classes Page

In the Advanced section of the Configure page, click **Classes** to display the page shown in Figure 4–6. You can use this page to manage existing classes or configure new classes.

Figure 4–6 Classes Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Classes
Add Edit Remove Rename
Class Name

admin
operator
oracle
reader
user

Add Edit Remove Rename
Users Hosts Devices Media Families Database Backup Storage Selectors Job Summaries Defaults and Policies

> **See Also:** *Oracle Secure Backup Reference* to learn about the class commands in `obtool`

Adding a Class

As explained in "Users and Classes" on page 1-8, 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. Click **Add** to add a new class.

   The New Classes page appears. This page describes class rights options.

2. In the **Class** box, enter a name for the class. 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 is of your choosing. It 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.

3. Select the rights to grant to this class. Refer to the "Classes and Rights" in *Oracle Secure Backup Reference* for a detailed explanation of these rights.

4. Click **Apply** or **OK**.

Editing a Class

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

To edit a class:

1. In the **Class Name** box, select the name of the class that you want to edit.

2. Click **Edit**.

The Web tool displays a page with details for the class name you selected.

3. Make any required changes.
4. Click **Apply** or **OK**.

Removing a Class

You cannot remove a class to which any users currently belong. Instead, you need to reassign or delete all existing members of a class before the class can be removed.

To remove a class:

1. In the **Class Name** box, select the name of the class to be removed.
2. Click **Remove**.

   A message prompts you to confirm the removal of the class.
3. Click **Yes** to remove the class name or **No** to leave the class undisturbed.

   A message appears in Status box telling you whether the class was successfully removed.

Renaming a Class

To rename a class:

1. In the **Class name** box, select the name of the class that you want to rename.
2. Click **Rename**.

   A message prompts you to confirm the renaming of the class.
3. In the text box, enter the new name for the class.
4. Click **Yes** to rename the class name or **No** to leave the class undisturbed.

   A message appears in Status box telling you the result of the operation.

Displaying Class Properties

To display the properties for a class:

1. In the **Class Name** box, select the name of the class whose properties you want to display.
2. Click **Edit**.

   The Web tool displays a page with details for the class name you selected.
3. Click **Cancel** to return to the Classes page.

Configuring Users

As explained in "Oracle Secure Backup Users and Passwords" on page 1-8, an Oracle Secure Backup user exists in a separate namespace from an operating system user. This section explains how to define, change, and remove Oracle Secure Backup users. It contains the following topics:

- About User Configuration
- Displaying the Users Page
- Adding a User

- Editing User Properties
- Changing a User Password
- Assigning Windows Account Information
- Assigning Preauthorized Access
- Renaming a User
- Removing a User

About User Configuration

When you run `installob` on the administrative server, Oracle Secure Backup creates the `admin` user by default. Unless you configured your `obparameters` file to create the `oracle` user, no other users exist in the administrative domain.

At this stage, you can optionally create new users or modify the attributes of the current users. The following user attributes are particularly important:

- Preauthorizations

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

  A preauthorization for an operating system user is associated with a specific Oracle Secure Backup user. For example, you can enable the Linux user `muthu` to log in to `obtool` as the Oracle Secure Backup user named `backup_admin`. Additionally, you could preauthorize `muthu` 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` (UNIX/Linux) or a member of the Administrators group (Windows). You must specify which operating system accounts are used for unprivileged backups.

It is recommended that you follow these steps:

1. If necessary, add new users.

   This task is described in "Adding a User" on page 4-28.

2. If necessary, change the `admin` password. 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 4-29.

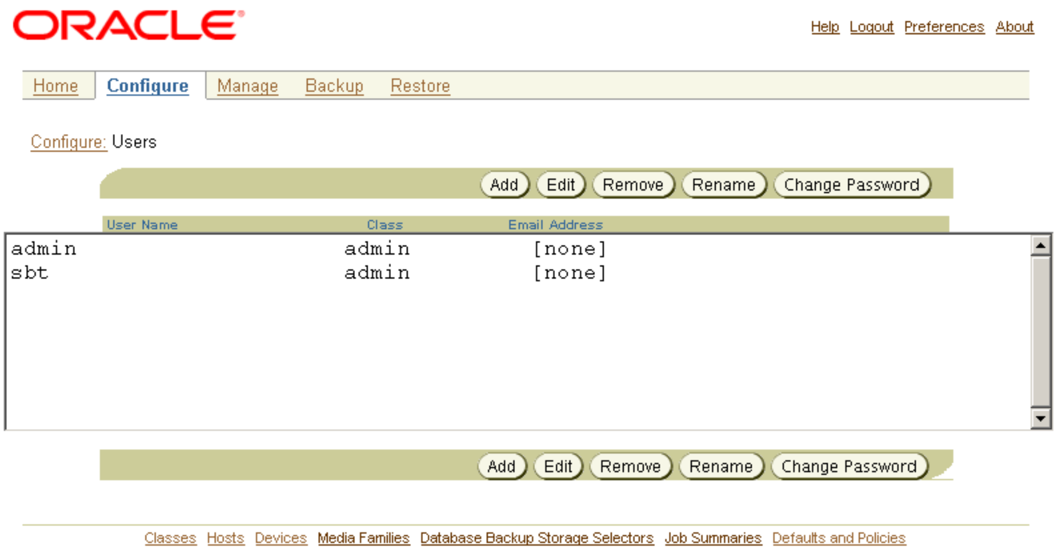
3. Review the attributes of every user and, if necessary, configure preauthorizations and account settings for unprivileged backups.

   These tasks are described in "Editing User Properties" on page 4-29, "Assigning Windows Account Information" on page 4-30, and "Assigning Preauthorized Access" on page 4-30.

Displaying the Users Page

In the Configure page, click **Users** to display the Users page, which is shown in Figure 4–7. This page lists all users authorized by Oracle Secure Backup along with their class names and email addresses. You can perform all user configuration tasks in this page or in pages to which it provides links.

Figure 4–7 Users Page



User Name	Class	Email Address
admin	admin	[none]
sbt	admin	[none]

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

Adding a User

To add one or more users:

1. In the Users page, click **Add** to add a new user.

   The Web tool displays the New Users form for entering a user name.

2. In the **User** box, enter a user name.

   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 Windows or UNIX user names.

3. In the **Password** box, enter a password. This password is used to log in to Oracle Secure Backup. The maximum character length that you can enter is 16 characters.

4. In the **User class** list, select a class. A class defines a set of rights.

   > **See Also:** "Oracle Secure Backup Classes and Rights" on page 1-9 for more detail on the default Oracle Secure Backup classes

5. In the **Given name** box, optionally enter a name for the user. This name is for information purposes only.

6. In the **UNIX name** box, enter a UNIX name for this account.

   This name forms the identity of any non-privileged jobs run by the user on UNIX systems. If this Oracle Secure Backup user will not—or is not permitted to—run Oracle Secure Backup jobs on UNIX systems, then the user can leave this field blank.

7. In the **UNIX group** box, enter a UNIX group name for this account.

   This name forms the identity of any non-privileged jobs run by the user on UNIX systems. If this Oracle Secure Backup user will not —or is not permitted to—run Oracle Secure Backup jobs on UNIX systems, then the user can leave this field blank.

8. In the **NDMP server user** box, select **yes** to request that Oracle Secure Backup's NDMP server accept a login from this 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**.
9. In the **Email address** box, enter the email address for the user. When Oracle Secure Backup wants to communicate with this user, such as to deliver a job summary or notify the user of a pending input request, it sends email to this address.
10. Click **Apply**, **OK**, or **Cancel**.
11. If the user you configured needs to initiate backup and restore operations on Windows clients, see "Assigning Windows Account Information" on page 4-30.

Editing User Properties

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

> **Note:** To modify users, you need to be a member of a class that has this right enabled. See "Oracle Secure Backup Classes and Rights" on page 1-9 for details.

To edit user properties:

1. From the **Users** page, select the name of the user from the **User name** box.
2. Click **Edit**.

   The Web tool displays a page with details for the user you selected.

3. Make any required changes.
4. Click **Apply**, **OK**, or **Cancel**.
5. If the user you configured needs to initiate backup and restore operations on Windows clients, see "Assigning Windows Account Information" in the following section.

Changing a User Password

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

> **Note:** To modify users, you need to be a member of a class that has this right enabled. See "Oracle Secure Backup Classes and Rights" on page 1-9 for details.

To edit user properties:

1. From the **Users** page, select the name of the user from the **User name** box.
2. Click **Change Password**.

   The Web tool displays a page with details for the user you selected.

3. Enter a new password and confirm it.
4. Click **OK** or **Cancel**.

Assigning Windows Account Information

This section explains how to configure Windows account information for Oracle Secure Backup users who need to 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 Steps 1 and 2 in "Editing User Properties" on page 4-29.
2. Click **Windows Domains**.
3. In the **Domain name** box, enter a Windows domain name. Enter an asterisk (`*`) in this box for all Windows domains.
4. In the **Username** and **Password** boxes, enter the account information for a Windows user.
5. Click **Add** to add the Windows account information. The account information appears in the **Domain:Username** box.

Removing a Windows Account

To remove a Windows account:

1. From the Windows Domain page, select the name of the Windows account from the **Domain: Username** box.
2. Click **Remove**.

   The Web tool displays a message in the Status box informing you that the Windows account was successfully removed.

Assigning Preauthorized Access

This section explains how to grant access to Oracle Secure Backup services and data to the 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 the specified operating system user on the specified host. For each host within an Oracle Secure Backup administrative domain, the administrator may declare one or more one-to-one mappings between operating system and Oracle Secure Backup user identities.

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

To assign preauthorized access:

1. From the Users page, select the name of the user from the **User name** box.
2. Click **Edit**.

   The Web tool displays a page with details for the user you selected.
3. Click **Preauthorized Access**.

4. In the **Hosts** lists, select either **all hosts** or the name of the host to which the operating system user is granted preauthorized access.
5. In the **OS username** box, 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 users.
6. In the **Windows domain name** box, 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** box, then you must enter an asterisk, leave the box blank, or enter a specific domain.
7. In the **Attributes** box, select **cmdline** or **rman**.

   The **cmdline** attribute preauthorizes login through the user-invoked Oracle Secure Backup command-line utilities such as `obtool`. The **rman** attribute preauthorizes Oracle Database SBT backups through RMAN.
8. Click **Add**.

   The Web tool displays the preauthorization information in the Preauthorized Access page.

> **See Also:** "Creating a Preauthorized Oracle Secure Backup Account" on page 6-8 for more details about RMAN preauthorizations

Removing Preauthorized Access

To remove preauthorized access:

1. From the Preauthorized Access page, select the preauthorized access entry in the main text box.
2. Click **Remove**.

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

Renaming a User

To rename a user:

1. From the **Users** page, select the name of the user from the **User Name** box.
2. Click **Rename**.

   Oracle Secure Backup prompts you to enter the new name of the user.
3. Enter the new name for the user in the text box.
4. Click **Yes** to rename the user.

   You are returned to the Users page.

Removing a User

To remove an Oracle Secure Backup user:

1. From the **Users** page, select the name of the user from the **User Name** box.
2. Click **Remove**.

   Oracle Secure Backup prompts you to confirm the removal of the user.

3. Click **Yes** to remove the user.

   You are returned to the **Users** page. A message appears in the **Success** box telling you the user was successfully removed.

5 Configuring Backup and Media Settings

This chapter explains how to configure backup and media settings for an administrative domain. This chapter contains the following topics:

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

Configuring Media Families

This section explains how to configure media families. This section contains the following topics:

- About Media Family Configuration
- Displaying the Media Families Page
- Adding a Media Family
- Editing or Displaying Media Family Attributes
- Removing a Media Family
- Renaming a Media Family

About Media Family Configuration

As explained in "Media Families" on page 2-23, 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 policies: content-managed (default) or time-managed. Content-managed volumes expire only when all backup pieces recorded on a volume have 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 attributes (see "Editing or Displaying Media Family Attributes" on page 5-4).

If you do not specify a media family for file system backups, 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
- Offsite backups

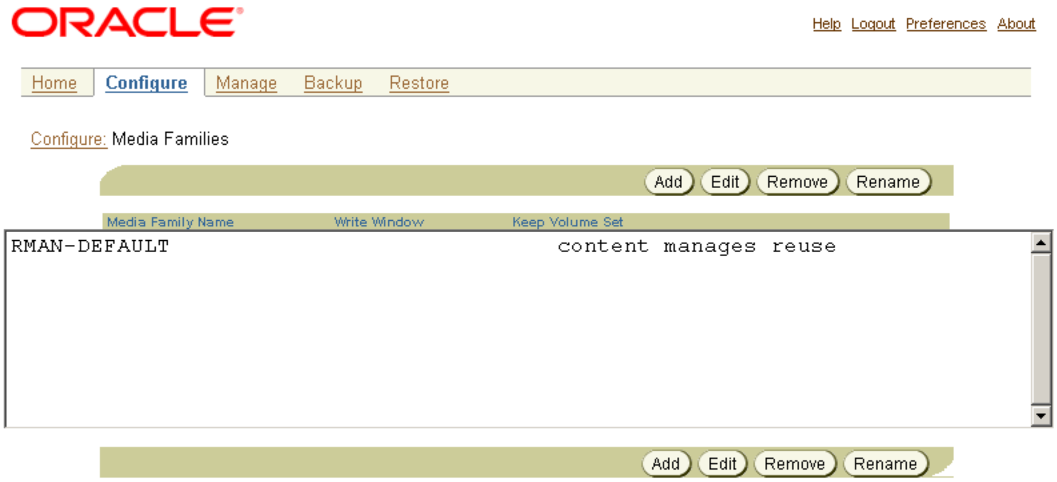
  This media family contains volumes with no expiration time. These volumes, which are stored offsite, are intended for disaster recovery or long-term storage.
- Scratch backups

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

Displaying the Media Families Page

Click **Media Families** in the Configure page to display the Media Families page, which is shown in Figure 5–1. You can perform all media management configuration tasks in this page or in pages to which it provides links.

Figure 5–1 Configure Media Families Page



ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Media Families
Add Edit Remove Rename
Media Family Name Write Window Keep Volume Set
Add Edit Remove Rename

Media Family Name	Write Window	Keep Volume Set
RMAN-DEFAULT		content manages reuse

See Also: *Oracle Secure Backup Reference* to learn about the media family commands in `obtool`

Adding a Media Family

To add a media family:

1. In the Media Families page, click the **Add** button to add a new media family.

   Oracle Secure Backup displays the New Media Families page.

2. In the **Media Family** box, enter a name for the media family. Normally, this name forms the prefix in each volume ID that uses this media family. Media family names are case-sensitive and must start with an alphanumeric character. They can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 31 characters.

3. In the **Volume ID used** group, select a means for volume identification. Your choices are:

   - **System default**

     Select this option to use the same volume ID sequencing as would be used if no media family were assigned. The default volume ID begins at `VOL000001` and increments after each time it is assigned.

   - **Unique to this media family**

     Select this option to use the volume ID `*media-family-name*-000001`, where `*media-family-name*` is the **Media Family** box, and increment it each time it is assigned.

   - **Same as for media family**

     Select this option to use the same volume ID sequencing as the media family that you select from the adjacent list.

   - **From file**

     Select this option to specify a volume sequence file that will be used to name volumes. You must specify the path of the volume sequence file.

     If you select this option, then you must manually create a text-based volume sequence file. The default path for the file within the Oracle Secure Backup home is as follows, where *familyname* is the name of the media family that you are creating:

```
admin/state/family/familyname/vol-seq-familyname
```

For example, if you are creating the media family called `incrbak`, then you would create the file as follows:

```
admin/state/family/incrbak/vol-seq-incrbak
```

After creating this file, use a text editor to insert the first volume ID to be assigned to the media family as a single line of text, for example, `MYVOLUME-00001`. Volumes in this media family will be named `MYVOLUME-00001`, `MYVOLUME-00002`, and so on.

4. In the **Write window** box, enter a write-allowed time period.

   You can set the write window to a specific duration, such as 14 days or 3 weeks. All volume sets that are members of the media family remain open for updates for this period.

   > **Note:** If you do not specify a write window for a volume set, then Oracle Secure Backup considers the volume set eligible to be updated indefinitely.

5. In the **Keep volume set** group, select **Retain time** or **Content managed volume**, depending on the type of expiration policy that you want. Expiration policies are explained in "Volume Expiration Policies" on page 2-24. If you select **Retain time**, then enter a time and select a unit of time from the adjacent list.
6. In the **Comment** box, you can optionally enter any information that want to store with the media family.
7. Click **Apply**, **OK**, or **Cancel**.

Editing or Displaying Media Family Attributes

You can edit any attributes of user-defined media families 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 the following:

- **Write window**
- **Keep volume set**

To display or edit attributes for an existing media family:

1. From the Media Families page, select the name of the media family.
2. Click **Edit**.

   The Web tool displays a page with details of the media family.
3. Make any required changes. If you merely want to display attributes, then do not make changes.
4. Click **Apply**, **OK**, or **Cancel**.

Removing a Media Family

To remove a media family:

1. From the Media Families page, select the name of the media family.

   Oracle Secure Backup prompts you to confirm the removal of the media family.

2. Click **Yes** to remove the media family.

   The media family is removed and you are returned to the Media Families page.

> **Note:** Removing a media family has no effect on existing volumes that use the media family.

Renaming a Media Family

To rename a media family:

1. From the Media Families page, select the name of the media family.

2. Click **Rename**.

   Oracle Secure Backup prompts you for the new name.

3. Enter the new name for the media family in the text box. 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 may contain at most 31 characters.

4. Click **Yes** to accept the new name.

   The media family is renamed and you are returned to the Media Families page.

> **Note:** Renaming a media family has no effect on previous volumes in the family.

Configuring Database Backup Storage Selectors

This section explains how to configure a database backup storage selector. This section contains the following topics:

- About Database Backup Storage Selector Configuration
- Displaying the Database Backup Storage Selectors Page
- Adding a Database Backup Storage Selector
- Editing a Database Backup Storage Selector
- Removing a Database Backup Storage Selector
- Renaming a Database Backup Storage Selector

About Database Backup Storage Selector Configuration

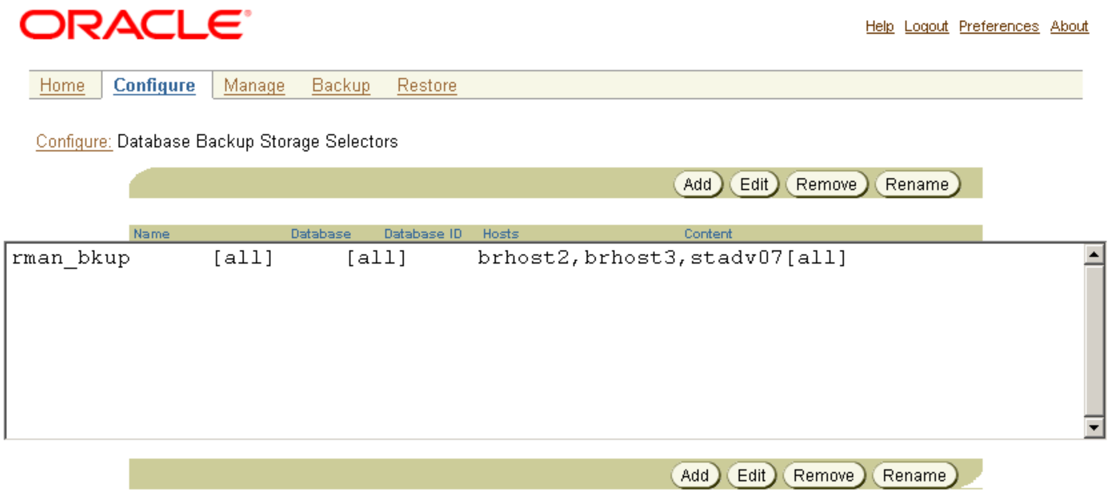
A database backup storage selector associates an RMAN backup with Oracle Secure Backup storage media. For example, you can specify that RMAN backups of archived redo logs from the `orcl` database should use the `orcl_log` media family.

You can use either the Web tool or Enterprise Manager to configure database backup storage selectors. This chapter explains how to use the Web tool, whereas "Creating a Database Backup Storage Selector" on page 6-12 explains how to use Enterprise Manager. In most cases, it is easier to use Enterprise Manager to perform RMAN-related configuration.

Displaying the Database Backup Storage Selectors Page

In the Configure page, click **Database Backup Storage Selectors** to display the page shown in Figure 5–2. You can perform all storage selector configuration tasks in this page or in pages to which it provides links.

Figure 5–2 Database Backup Storage Selectors Page



```
Name              Database     Database ID  Hosts                          Content
rman_bkup       [all]      [all]      brhost2,brhost3,stadv07[all]
```

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

Adding a Database Backup Storage Selector

To configure a database backup storage selector:

1. Click the **Add** button to display the New Database Backup Storage Selectors page.
2. In the **Name** box, enter a name for the database backup storage selector.

   You can create multiple storage selectors for any given database depending on what you enter in the **Content** box. For example, you can create one storage selector called `DB1-full` and another storage selector called `DB1-incr`. These storage selectors define different backup operations.
3. In the **Content** box, select one of the following options:
   - **all**

     Select this option to specify that this storage selector is applicable to any of the content types: **full**, **incr**, **archive log**, and **auto backups**.
   - **full**

     Select this option to restrict this storage selector to full database backups.
   - **incr**

     Select this option to restrict this storage selector to incremental database backups.
   - **archive log**

     Select this option to restrict this storage selector to archived redo log backups.
   - **auto backups**

Select this option to restrict this storage selector to control file autobackups.

4. In the **Database(s)** box, enter a name for the physical database. Enter an asterisk (*) for all database names.
5. In the **Database ID(s)** box, enter a name for the database ID. Enter an asterisk (*) for all database IDs.
6. In the **Host** list, select the host on which the database resides.
7. In the **Media family** list, select the name of a media family. For more information about Media Families see "Configuring Media Families" on page 5-2.
8. In the **Restrictions** box, optionally enter the names of devices to which backups controlled by this storage selector are restricted. Restrictions are used to specify a definite device, host, or device/host pair that users want Oracle Secure Backup to utilize. If this option is left blank, then Oracle Secure Backup uses device polling to find any available device for use in backup operations.

   Restrictions come in the following formats:

   - *device*
   - *@hostname*
   - *device@hostname*
9. From the **Copy number** list, select the copy number to which this storage selector applies. The copy number must be an integer in the range of 1 to 4. Specify an asterisk (*) to indicate that the storage selector applies to any copy number.
10. In the **Resource wait time** box, enter a time interval to wait for the availability of resources required by backups under the control of this storage selector. Select a time unit from the adjacent list. Note that you can select **forever** to specify that the wait time is unlimited.
11. Click **Apply**, **OK**, or **Cancel**.

Editing a Database Backup Storage Selector

To edit parameters for an existing database backup storage selector:

1. In the Database Backup Storage Selectors page, select the name of the storage selector.
2. Click the **Edit** button.

   The Web tool displays a page with details of the storage selector.
3. Make any required changes.
4. Click **Apply**, **OK**, or **Cancel**.

Removing a Database Backup Storage Selector

To remove a database backup storage selector:

1. In the Database Backup Storage Selectors page, select the name of the storage selector to remove.

   Oracle Secure Backup prompts you to confirm the removal of the object.
2. Click **Yes** to remove the storage selector.

   The storage selector is removed and you are returned to the Database Backup Storage Selectors page.

Renaming a Database Backup Storage Selector

To rename a database backup storage selector:

1. In the Database Backup Storage Selector page, select the name of the storage selector to rename.
2. Click the **Rename** button.

   Oracle Secure Backup prompts you for the new name.
3. Enter the new name for the storage selector in the text box.
4. Click **Yes** to accept the new name. The storage selector is renamed and you are returned to the Database Backup Storage Selectors page.

Configuring Job Summary Schedules

This section contains the following topics:

- Displaying the Job Summaries Page
- Creating a Job Summary Schedule
- Editing a Job Summary Schedule
- Removing a Job Summary Schedule
- Renaming a Job Summary Schedule

About Job Summary Schedule Configuration

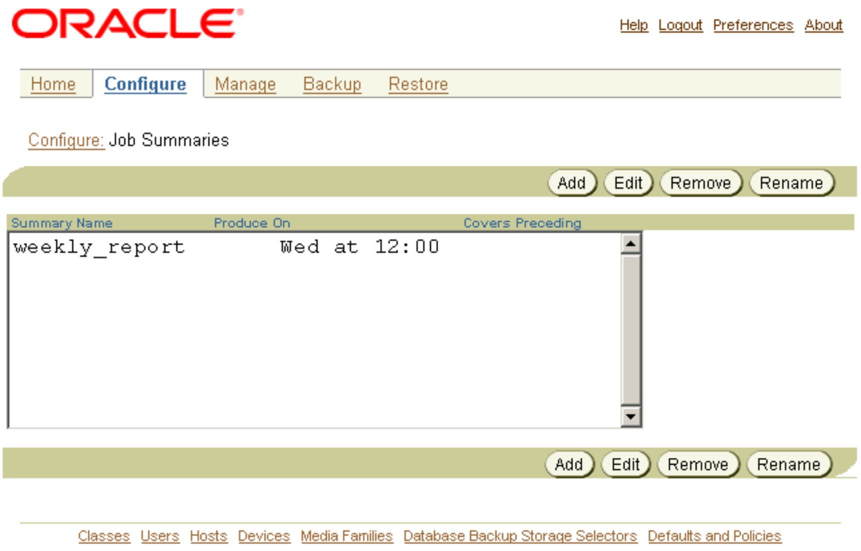
As explained in "Job Summaries" on page 2-14, a job summary is a report produced by Oracle Secure Backup. This report describes the status of selected file system backup and restore jobs. You can configure a job summary schedule that indicates when the reports should be generated and who should receive them.

It is recommended that you create at least one job summary schedule so that you receive an automated email describing your backup jobs.

Displaying the Job Summaries Page

In the Advanced section of the Configure page, click **Job Summaries** to display the page shown in Figure 5–3. This page lists the job summary schedules for the administrative domain.

Figure 5–3 Job Summaries Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Configure: Job Summaries
Add Edit Remove Rename
Add Edit Remove Rename
Classes Users Hosts Devices Media Families Database Backup Storage Selectors Defaults and Policies

Summary Name	Produce On	Covers Preceding
weekly_report	Wed at 12:00	

> **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:

1. Click **Add** to create a new job summary schedule.

   The New Job Summaries page appears.

2. In the **Summary** box, enter a name for the job summary schedule, for example, `weekly_backup_jobs`. Names are case-sensitive and must start with an alphanumeric character. Names can contain only letters, numerals, dashes, underscores, and periods (no spaces). They may contain at most 127 characters.

3. In the **Produce on** group, select the days on which to generate the report. You can check one of the following boxes:

   - **Select daily**

     Check this box to generate reports on all 7 days of the week.

   - **Select weekdays**

     Check this box to generate a reports on Monday through Friday only.

   - **Select weekend**

     Check this box to generate reports on Saturday and Sunday only.

4. In the time lists, select the local time (hour and minutes) of the day in which to generate the report. The time is expressed in 24-hour format.

5. In the **Mail to** box, enter one or more email addresses. This option enables you to identify the recipients of email notification reports. An email system such as `sendmail` must be operational on the administrative server for this feature to operate. Separate multiple entries with a comma.

6. In the **Schedule** group, indicate the earliest time at which Oracle Secure Backup should gather information for the report. You can select one of the following options:

- **Cover preceding**

  Select this option to specify a start time (in seconds, minutes, hours, days, weeks, months, years, or forever) for gathering report data. For example, you can include activity for the last week.

- **Since**

  Select this option to specify a start day and time (expressed in 24-hour format) for gathering report data. For example, you can include activity between Monday at 8:30 a.m. until now.

7. In the **Report options** group, enable (or disable) any of the following report content options:

   - **Backup jobs**

     Select this option to include all backup jobs.

   - **Restore jobs**

     Select this option to include all restore jobs.

   - **Scheduled jobs**

     Select this option to include all jobs that were created as a result of scheduled backups.

   - **User jobs**

     Select this option to include all jobs that were created as a result of explicit user requests.

   - **Subordinate jobs**

     Select this option to include subordinate jobs. As explained in "Job Creation" on page 2-12, Oracle Secure Backup breaks down dataset backup jobs into one or more subordinate jobs, where each subordinate job pertains to one host included in the dataset.

   - **Superseded jobs**

     Select this option to report jobs that were superseded by other jobs. When Oracle Secure Backup detects identical pending backup jobs, it automatically marks the older or less comprehensive one as having been superseded.

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

Editing a Job Summary Schedule

To edit a job summary schedule:

1. In the main box of the Job Summaries page, select the name of the job summary schedule to edit.
2. Click **Edit**.

   The Web tool displays a page with details of the job summary schedule.

3. Make needed changes and click **OK** to save your changes.

   The Status box displays the result of the operation.

Removing a Job Summary Schedule

To remove a job summary schedule:

1. In the main box of the Job Summaries page, select the name of the job summary schedule to edit.
2. Click **Remove**.

   A message prompts you to confirm the operation.
3. Click **Yes** to remove the job summary schedule.

   The Status box displays the result of the operation.

Renaming a Job Summary Schedule

To rename a job summary schedule:

1. In the main box of the Job Summaries page, select the name of the summary to rename.
2. Click **Rename**.

   A message prompts you for the new name.
3. In the text box, enter the new name for the job summary schedule.
4. Click **Yes** to accept the new name.

   The Status box displays the result of the operation.

Part III

Performing Backup and Restore Operations

This part provides an architectural and conceptual overview of Oracle Secure Backup. This part contains the following chapters:

6

Using Recovery Manager with Oracle Secure Backup

This chapter explains how to use RMAN with Oracle Secure Backup. This chapter contains the following topics:

- Overview of Recovery Manager and Oracle Secure Backup
- Configuring RMAN and Oracle Secure Backup
- Performing Backups with RMAN and Oracle Secure Backup
- Performing Recovery with RMAN and Oracle Secure Backup
- Managing RMAN Metadata in Oracle Secure Backup
- Using RMAN and Oracle Secure Backup in a Real Application Clusters Environment

Overview of Recovery Manager and Oracle Secure Backup

Oracle Secure Backup serves as a media management layer for Recovery Manager (RMAN) through the SBT interface. In this capacity, Oracle Secure Backup provides the same services for RMAN as other third-party SBT interfaces. Oracle Secure Backup provides the following additional features:

- Its SBT library is the only interface that supports RMAN-encrypted backups directly to tape.
- It is better integrated with Oracle Enterprise Manager than other media managers.

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

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

This section contains the following topics:

- RMAN Environment
- Interfaces for Managing Database Backup and Recovery
- RMAN and the Oracle Secure Backup Administrative Domain
- How RMAN Accesses Oracle Secure Backup

RMAN Environment

This chapter assumes that you are familiar with Recovery Manager. The RMAN environment includes the following basic components:

- RMAN client

  The RMAN client program, which is installed automatically with an Oracle database, initiates database backup and recovery. The RMAN client can back up and recover any Oracle database accessible locally or through Oracle Net so long as it meets compatibility requirements.

- RMAN target database

  The target is the database that 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.

- RMAN recovery catalog

  The 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.

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

  The `rman` executable is located in the `$ORACLE_HOME/bin` directory of a database installation. Note the following considerations when using the RMAN command-line client with Oracle Secure Backup:

  - The RMAN client can run from any Oracle home, regardless of whether the computer containing this home is a member of the Oracle Secure Backup administrative domain.
  - The target database host must be a member of the Oracle Secure Backup administrative domain.
  - The target database uses the Oracle Secure Backup SBT interface on the target host to communicate with the Oracle Secure Backup administrative domain.

- Oracle Enterprise Manager 10*g* Database Control

  You can manage single-instance database operations, including backup and recovery, through the Database Control console. Note the following considerations when using Enterprise Manager Database Control with Oracle Secure Backup:

  - The Database Control console must run on the same host as the target database.
  - The Database Control console must run on the administrative server of the Oracle Secure Backup domain.

- Oracle Enterprise Manager 10*g* Grid Control

  You can use the Grid Control console to manage multiple databases. Note the following considerations when using Enterprise Manager Grid Control with Oracle Secure Backup:

  - The Grid Control console can run on any database host in the administrative domain. Unlike Database Control, Grid Control does not need to run on the administrative server of the Oracle Secure Backup 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, 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.

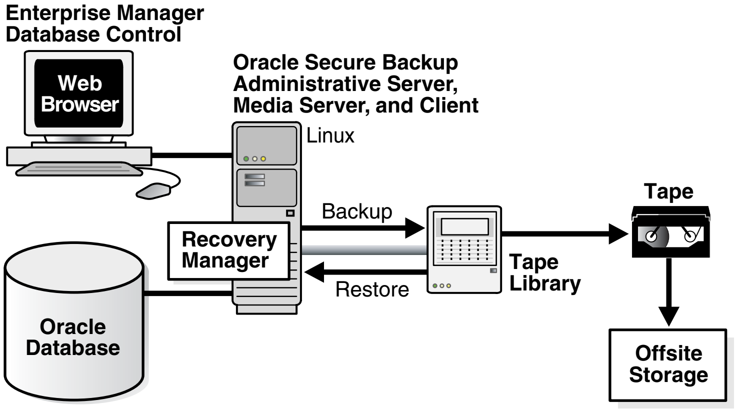
RMAN and the Oracle Secure Backup Administrative Domain

How you use RMAN in conjunction with Oracle Secure Backup depends on the configuration of your administrative domain. This section describes two typical scenarios.

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 6–1 illustrates a typical single-host scenario.

Figure 6–1 Single-Host Administrative Domain


Enterprise Manager Database Control
Web Browser
Oracle Secure Backup Administrative Server, Media Server, and Client
Linux
Backup
Recovery Manager
Restore
Tape
Tape Library
Oracle Database
Offsite Storage

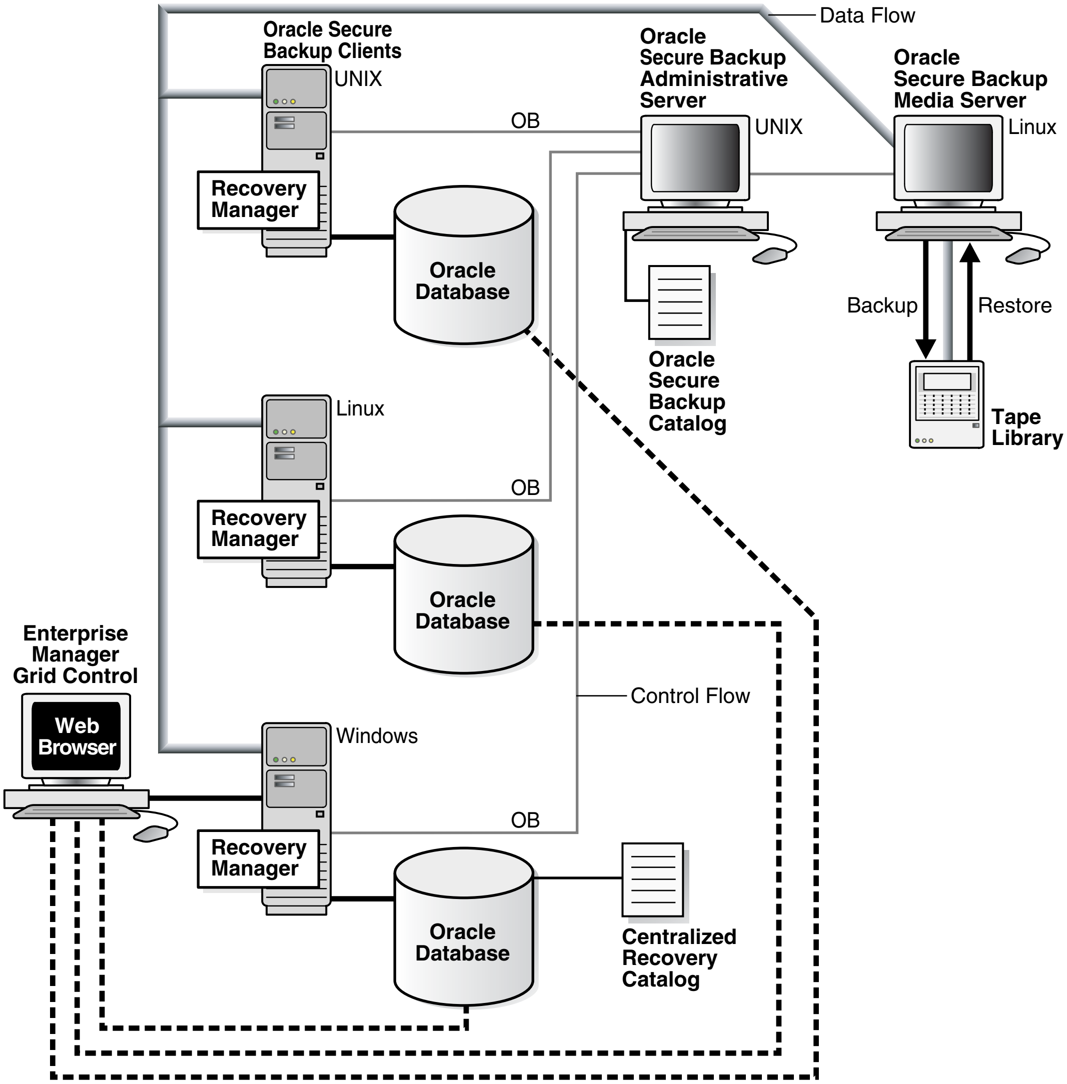
Because the database is installed on the administrative server, you can use Enterprise Manager Database Control console to perform database backup and restore operations involving Oracle Secure Backup. This chapter is written from the perspective of the administrator of a single-host domain that is configured like the one in Figure 6–1.

Multiple-Host Administrative Domain

In a typical multiple-host administrative domain, the administrative server, media server, and clients are on separate hosts. A single administrative domain can include only one administrative server but may include multiple media servers and clients.

Figure 6–2 illustrates a typical multiple-host domain in which each client host runs an Oracle database. In this example, the administrative server and media server do not run databases. The Windows database includes a centralized recovery catalog to store RMAN metadata for backups of all databases in the domain.

Figure 6–2 Multiple-Host Administrative Domain


Data Flow
Oracle Secure Backup Clients
UNIX
OB
Oracle Secure Backup Administrative Server
UNIX
Oracle Secure Backup Media Server
Linux
Recovery Manager
Oracle Database
Oracle Secure Backup Catalog
Backup
Restore
Tape Library
Linux
OB
Recovery Manager
Oracle Database
Enterprise Manager Grid Control
Web Browser
Control Flow
Windows
OB
Recovery Manager
Oracle Database
Centralized Recovery Catalog

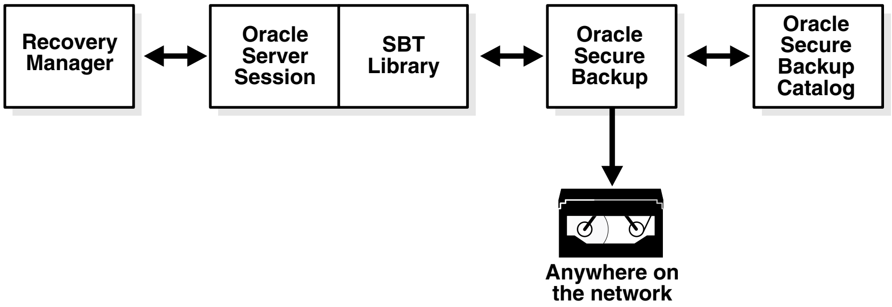
Because the target databases do not reside on the administrative server, you cannot use Enterprise Manager Database Control to back them up through the Oracle Secure Backup SBT interface. You can use Grid Control on one of the clients, however, to initiate SBT operations involving all databases in the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

How RMAN Accesses Oracle Secure Backup

Regardless of the 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 6–3 displays the basic components of RMAN backup and restore operations that use the Oracle Secure Backup SBT interface.

Figure 6–3 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. The user starts the RMAN client (either through the command line or the Enterprise Manager console), allocates an SBT channel, and executes a `BACKUP` or `RESTORE` command.

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

2. The server session on the database host makes the backup or restore job request through the Oracle Secure Backup SBT library.

3. Oracle Secure Backup creates the backup or restore job and assigns it a unique identifier such as `sbt/15`. Refer to *Oracle Secure Backup Reference* for a description of job identifiers.

4. For backups, Oracle Secure Backup immediately tries to reserve and start the appropriate resources, for example, reserve the tape drive and load a tape. If the resource is unavailable, then Oracle Secure Backup queues the job while it waits for the resource to become available.

   Note: You can control how long a job waits in the queue through the `rmanresourcewaittime` operations policy (set to `forever` by default), the `--waittime` option in a backup storage selector, or the RMAN parameter `OB_RESOURCE_WAIT_TIME` (see "Setting Media Management Parameters in RMAN" on page 6-14).

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

   Note: SBT backup jobs do not honor the existing Oracle Secure Backup backup windows, but execute immediately whenever they enter the system.

5. Oracle Secure Backup creates or restores the backup pieces.

6. 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 and reports metadata about the contents of each backup piece.

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

Configuring RMAN and Oracle Secure Backup

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

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

   This step is explained in "Configuring RMAN Access to the Oracle Secure Backup SBT Library" on page 6-7.

2. Create a preauthorized Oracle Secure Backup account for use by RMAN.

   This step is explained in "Creating a Preauthorized Oracle Secure Backup Account" on page 6-8.

3. Optionally, create media families for datafiles and archived redo logs. By default RMAN uses the `RMAN-DEFAULT` media family.

   This step is explained in "Creating Media Families for RMAN Backups" on page 6-11.

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

   These steps are explained in "Creating a Database Backup Storage Selector" on page 6-12 and "Setting Media Management Parameters in RMAN" on page 6-14.

You can perform the preceding tasks in Enterprise Manager or the Oracle Secure Backup Web tool or command-line interfaces. Where possible, this section explains how to perform these tasks through the Enterprise Manager Database Control console.

Configuring RMAN Access to the Oracle Secure Backup SBT Library

If you use Enterprise Manager Database Control, then configure RMAN access to Oracle Secure Backup. This preliminary task is described in "Registering an Administrative Server in Enterprise Manager" on page 3-11. You need only specify the Oracle Secure Backup home directory. RMAN locates the SBT library automatically.

By default, RMAN looks in a platform-specific default location for the SBT library. On UNIX/Linux, 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 performs the following tasks:

- Copies the SBT library to the `lib` subdirectory of the Oracle Secure Backup home
- 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 Account

RMAN backup and restore operations that make use of Oracle Secure Backup involve interaction between the following users:

- The Oracle Secure Backup user who processes the backup or restore request

  Note that this user must have the following rights:

  - `access Oracle backups` (set to `owner`, `class`, or `all`)
  - `perform Oracle backups and restores`

- The operating system user under which the database server session is running

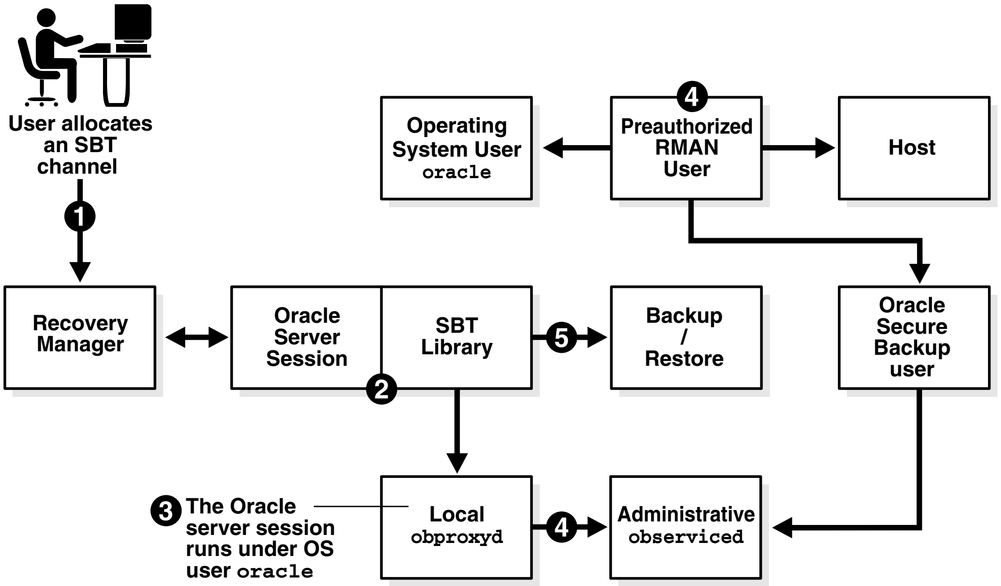
  Typically, the server session runs under the `oracle` operating system account. Oracle Secure Backup honors SBT requests only if the requesting operating system user accesses Oracle Secure Backup as a user with the correct rights.

As explained in "Assigning Preauthorized Access" on page 4-30, you can preauthorize an operating system user to access an Oracle Secure Backup account as a specified user. In the case of RMAN SBT backups, Oracle Secure Backup preauthorizes an operating system user to perform backup and restore operations as an Oracle Secure Backup user with the appropriate rights.

How Oracle Secure Backup Preauthorizes SBT Backups

Figure 6–4 illustrates the basic process in which a preauthorized operating system user submits a backup or restore request to Oracle Secure Backup.

Figure 6–4 Preauthorization for Database Backup and Restore Operations


User allocates an SBT channel
1
Recovery Manager
Oracle Server Session
SBT Library
2
5
Backup / Restore
Operating System User oracle
4
Preauthorized RMAN User
Host
Oracle Secure Backup user
3 The Oracle server session runs under OS user oracle
Local obproxyd
4
Administrative observiced

The preauthorization of the operating system user 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.
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 6–4, the backup and restore operations run under the oracle operating system account on brhost2.

Configuring an RMAN Preauthorization

This section explains how to configure an RMAN preauthorization. You can preauthorize the operating system user during or after installation. The instructions vary according to platform.

Configuring an RMAN Preauthorization on Linux or UNIX During Installation To create the Oracle Secure Backup user during installation of the Oracle Secure Backup software on Linux or UNIX, modify the obparameters file when prompted by the installob script. The script prompts you as follows:

```
Have you already reviewed and customized install/obparameters for your
Oracle Secure Backup installation [yes]?
```

You can enter no and then modify the obparameters file, which is located in the install subdirectory of the Oracle Secure Backup home. Change the value of the following parameter to yes:

```
create pre-authorized oracle user: no
```

In the obparameters file, you can specify the default operating system user and group or accept the defaults. For example, on Linux and UNIX the default user is oracle and default group is dba:

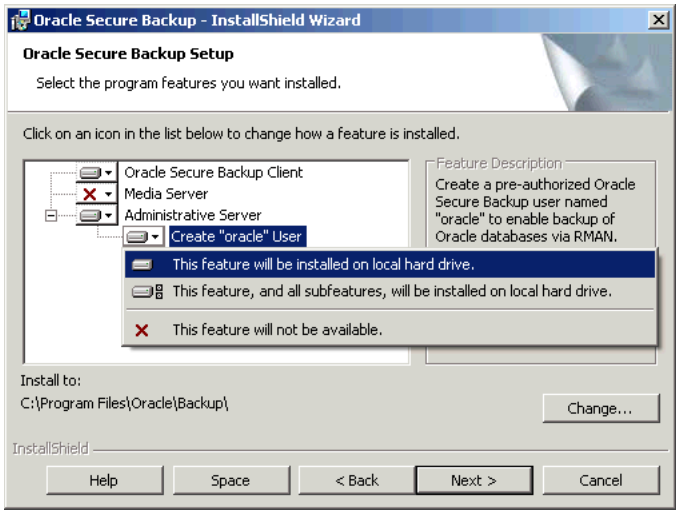
```
default UNIX user:  oracle
default UNIX group: dba
```

If you accept the default user and group names, then the installation program automatically creates an Oracle Secure Backup user named oracle. The Linux or UNIX user named oracle in the dba group is granted preauthorized access to this Oracle Secure Backup account.

> **See Also:** *Oracle Secure Backup Installation Guide* to learn how to install Oracle Secure Backup on Linux and UNIX

Configuring an RMAN Preauthorization on Windows During Installation To create the Oracle Secure Backup user on Windows, run the InstallShield wizard as described in *Oracle Secure Backup Installation Guide*. When you are prompted to choose a role for the host, you can select **Create "oracle" user** and remove the red X as shown in Figure 6–5.

Figure 6–5 Creating the oracle User During a Windows Installation



Oracle Secure Backup - InstallShield Wizard

Oracle Secure Backup Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Oracle Secure Backup Client
- ✗ Media Server
- Administrative Server
  - Create "oracle" User

Feature Description

Create a pre-authorized Oracle Secure Backup user named "oracle" to enable backup of Oracle databases via RMAN.

- This feature will be installed on local hard drive.
- This feature, and all subfeatures, will be installed on local hard drive.
- ✗ This feature will not be available.

Install to:
C:\Program Files\Oracle\Backup\

The installer automatically creates an Oracle Secure Backup user named `oracle` and assigns it to the `oracle` class. Example 6–1 shows sample `lsuser` output for the `oracle` user after an installation on Windows.

Example 6–1 Default oracle User

```
ob> lsuser --long oracle
oracle:
    Password:                (not set)
    User class:              oracle
    Given name:              [none]
    UNIX name:               oracle
    UNIX group:              dba
    Windows domain/acct:     [all] Administrator
    NDMP server user:        no
    Email address:           [none]
    UUID:                    e95891fa-5a80-4500-8865-3706a7db74da
    Preauthorized access:
        Hostname:            [all]
        Username:            [all]
        Windows domain:      [all]
        RMAN enabled:        yes
        Cmdline enabled:     no
```

By default, all Windows users on all Windows domains are preauthorized to make RMAN backups to the Oracle Secure Backup SBT interface.

The Oracle Secure Backup user named `oracle` does not have the right to perform backups as a privileged user. To enable `oracle` to make unprivileged backups, ensure that the Windows domain, user name, and password information is correct. By default the password is not set for the user listed in the `Windows domain/acct` (see output in Example 6–1). You can run the `chuser` command in `obtool` to modify the Windows domain setting for the `oracle` user, either specifying a new password for the currently specified Windows account or entering completely new information.

Example 6–2 specifies the password for the `Administrator` user listed in the `Windows domain/acct` shown in Example 6–1. Because no password is specified in `--adddomain`, `obtool` prompts for it.

Example 6–2 Setting the Windows Domain Password for the oracle User

```
ob> chuser oracle --adddomain *,Administrator
Password:
Password (again):
ob>
```

See Also:

- *Oracle Secure Backup Installation Guide* to learn how to install Oracle Secure Backup on Windows
- *Oracle Secure Backup Reference* to learn about the `chuser` command

Configuring an RMAN Preauthorization Post-Installation To create the Oracle Secure Backup user after installation, use the Web tool as described in "Assigning Preauthorized Access" on page 4-30. If you are using Enterprise Manager, then you can navigate to the Oracle Secure Backup Web tool by clicking **File System Backup and Restore** in the Maintenance page.

Alternatively, you can run the `mkuser` command in `obtool` to create the user. Example 6–3 uses `mkuser` to create an Oracle Secure Backup user named `oracle` and assign this user to the `oracle` class. Example 6–3 uses the `--preauth` option to grant RMAN SBT access to the Linux/UNIX user `oracle` on host `brhost2`.

Example 6–3 Preauthorizing an Operating System User to Make RMAN SBT Backups

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

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

Creating Media Families for RMAN Backups

A media family is a named classification of volumes that share common attributes. As explained in "Content-Managed Expiration Policies" on page 2-25, the default media family for use by RMAN is named `RMAN-DEFAULT`. Thus, creating media families for use in RMAN backups is optional.

Note: You cannot delete or rename the `RMAN-DEFAULT` media family, although you can modify certain attributes through the Web tool or `obtool` (see "Editing or Displaying Media Family Attributes" on page 5-4).

You may find it useful to create different media families depending on the type of backup set: archived redo logs or datafiles. You can create media families in Enterprise Manager. Alternatively, you can use the Oracle Secure Web tool, as described in "Adding a Media Family" on page 5-3, or use the `mkmf` command in `obtool`.

When you create a media family, you specify a volume expiration policy that determines when volumes in a media family are expired, that is, eligible to be overwritten and recycled. Volumes in a media family use either a content-managed expiration policy or time-managed expiration policy.

Media families that are content-managed (for example, `RMAN-DEFAULT`) are for RMAN backups only. You can make also RMAN backups to time-managed volumes, which means that it is possible for these volumes to 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 the backup pieces as available. In this case, you must use the `CROSSCHECK` command in RMAN to resolve the discrepancy.

To create a content-managed media family in Enterprise Manager Database Control:

1. Log in to the Enterprise Manager Database Control as a user with database administrator rights.
2. Navigate to the Oracle Secure Backup section of the Maintenance page. Figure 3–6 shows the relevant section of the Maintenance page.
3. Click **Oracle Secure Backup Device and Media**.

   The Administrative Server: *hostname* page appears.
4. In **Media Families**, click the adjacent number.

   The Media Families page appears. The table should include a row for the system-supplied `RMAN-DEFAULT` media family.
5. Click **Add** to create a new media family.
6. Configure your media family as follows:
   - In the **Media Family Name** box, enter the name for the media family. For example, enter `datafile_mf` for a media family that applies to datafiles.
   - In the **Write Window** box, enter the amount of time during which a volume set can be appended. For example, enter `7 days`.
   - In the **Retention Policy** section, select **Content Manages Reuse**.
   - In the **Comment** box, you can optionally enter a description of the media family. For example, you can indicate that it is intended for backups of datafiles only.
7. Click **OK**.

   You are returned to the Media Families page. The table should now contain the media family that you just created.

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

Creating a Database Backup Storage Selector

As explained in "Database Backup Storage Selectors" on page 2-11, Oracle Secure Backup uses storage selectors to represent backup attributes that describe an Oracle database. You can use storage selectors to specify which resources should be used by Oracle Secure Backup SBT backups. The selectors act as a layer between RMAN, which accesses the database, and the Oracle Secure Backup software, which manages the backup media.

About Database Backup Storage Selectors

The following settings are required in database backup storage selectors:

- The database name or ID
- The name of the database host
- The name of the media family to use for the RMAN backups

Optional settings of backup storage selectors include the following:

- The content of the backup, for example, full or incremental backup
- The copy number of duplexed backups

You can create multiple database backup storage selectors. For example, you could create one database storage selector for datafile backups of all databases in the domain, and another selector for archived log backups of all databases in the domain. You could specify one library destination for the datafile backups and a different library destination for the archived log backups.

You cannot create multiple storage selectors if the database name, database ID, host name, content type, and copy numbers all match. 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 (`*`).

> **Note:** "Setting Media Management Parameters in RMAN" on page 6-14 explains how media management parameters specified on RMAN channels can override settings in a backup storage selector.

Configuring a Database Backup Storage Selector

You can use Enterprise Manager to create database backup storage selectors. Note that Enterprise Manager gives the selector a system-defined name. Alternatively, you can use the Web tool as described in "Configuring Database Backup Storage Selectors" on page 5-5 or use the `mkssel` command in `obtool`, in which case you can give the storage selector a user-defined name.

To create a database backup storage selector in Enterprise Manager Database Control:

1. Log in to the Enterprise Manager Database Control as a user with database administrator rights.
2. Navigate to the Backup/Recovery Settings section of the Maintenance page. This page is shown in Figure 3–6 on page 3-12.
3. Click **Backup Settings**.

The Backup Settings page appears.

4. In the Device property page, scroll down to the Oracle Secure Backup section and click **Configure**.

   The Administrative Server Login page appears.

5. In the **Administrative Server** list, select the administrative server. In this example, you are using the Database Console so the database host and administrative server are the same.

   In the **Username** and **Password** boxes, enter operating system credentials for the administrative server. Optionally, check **Save as Preferred Credential**. Click **OK**.

   The Backup Storage Selectors page appears.

6. Click **Add**.

   The Add Backup Storage Selector page appears.

7. Optionally, make the following selections:

   a. In the For These Types of Backups section, check the types of backups that should use this storage selector. You can also select the copy number; the default is an asterisk (`*`), which means all copies.

   b. In the Use Media Family section, select a media family for the selector. The media family defaults to `RMAN-DEFAULT`.

   c. In the Use Resource Wait Time section, specify 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. The default wait time is `forever`, which means there is no limit.

8. In the Use Device section, click **Add** to restrict the backup to the specified devices.

   The Use Devices page appears.

9. In the Search Results table, select the device to which to restrict the backup and click **Select**. Note that you can filter the devices that are displayed by first entering a search string in the **Device Name** box and clicking **Go**.

   The Add Backup Storage Selector page is displayed.

10. In Use Devices, check the added device and then click **OK**.

    The Backup Storage Selectors page appears. The table displays the backup storage selector that you created. Note that the selector has a system-generated name. You can edit the storage selector by selecting it and clicking **Edit**.

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

Setting Media Management Parameters in RMAN

This section assumes that you are familiar with setting Recovery Manager media management parameters. For a general explanation of how to specify media management parameters in RMAN, refer to *Oracle Database Backup and Recovery Advanced User's Guide*.

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, the preceding media management parameters override the settings of matching database backup storage selectors. Refer to *Oracle Secure Backup Reference* for an exhaustive chart that shows the relationship between RMAN media management parameters and database backup storage selectors.

To set media management parameters in an RMAN database backup:

1. Follow Step 1 through Step 6 in the section "Performing Backups with RMAN and Oracle Secure Backup" on page 6-15.

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.

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

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 Basics*. This section describes how to use Enterprise Manager to back up the whole database through the Oracle Secure Backup SBT.

To back up the database:

1. Log in to the Enterprise Manager Database Control as a user with database administrator rights.
2. In the Backup/Recovery section of the Maintenance page, click **Schedule Backup**. Figure 3–6 shows the relevant section of the Maintenance page.
3. In the Customized Backup section, select **Whole Database** and then click **Schedule Customized Backup**.

   The Schedule Customized Backup: Options page appears.
4. Perform the following actions and then click **Next**:
   - In the Backup Type section, select **Full Backup**.
   - In the Backup Mode section, select **Online Backup**.
   - In the Advanced section, check **Also back up all archived logs on disk**.

   The Schedule Customized Backup: Settings page appears.
5. Click **Tape** and click **Next**.

   The Schedule Customized Backup: Schedule page appears.
6. Click **Next** and review your backup characteristics.
7. Click **Submit Job**.

   The Status page appears.
8. Click **View Job** to monitor the progress of the backup.

   The Execution: *database_name* page appears. Refresh the page until the **Backup** link appears.
9. 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 restore database files is the same as described in *Oracle Database Backup and Recovery Basics*. This section describes how to use Enterprise Manager to restore a tablespace from tape and perform media recovery.

To restore and recover a tablespace:

1. Log in to the Enterprise Manager Database Control as a user with database administrator rights.
2. In the Storage section of the Administration page, click **Tablespaces**.

   The Tablespaces page appears.
3. In the table describing the tablespaces, click **EXAMPLE**.

   The View Tablespace: EXAMPLE page appears.
4. In the **Actions** list, select **Take Offline** and then click **Go**.

   The Take Tablespace Offline page appears.
5. Select **Immediate** and click **OK**.

The View Tablespace: EXAMPLE page appears. The status bar should indicate that the tablespace is offline.

6. Use an operating system utility to delete the datafile for the `example` tablespace from the operating system.

7. In Enterprise Manager, navigate to the Backup/Recovery section of the Maintenance page and select **Perform Recovery**.

   The Information bar indicates that a tablespace and datafile are offline.

8. In the Object Level Recovery section, make the following selections and then click **Perform Object Level Recovery**:

   - In the **Object Type** list, select **Tablespaces**.
   - In the Operation Type section, select **Recover to current time or a previous point-in-time**.

   The Perform Object Level Recovery: Point-in-time page appears.

9. Select EXAMPLE and click **Next**.

   The Perform Object Level Recovery: Rename page appears.

10. Accept the default location and click **Next**.

    The Perform Object Level Recovery: Review appears.

11. Review the recovery request and click **Submit**.

    The Processing: Perform Object Level Recovery page appears. When RMAN completes the recovery, the Perform Recovery: Result page appears with the transcript of the job.

Managing RMAN Metadata in Oracle Secure Backup

This section explains how to use Oracle Secure Backup to access and manage information about RMAN backups. This section contains the following topics:

- About RMAN and Oracle Secure Backup Metadata
- Displaying RMAN Job Information in Oracle Secure Backup
- Displaying Backup Piece Information
- Adding Information About RMAN Backups to the Oracle Secure Backup Catalog

About RMAN and Oracle Secure Backup Metadata

Oracle Database Backup and Recovery Basics explains how to access metadata in the RMAN repository through RMAN commands, dynamic performance (`V$`) views on the target database, and recovery catalog views. Although this metadata includes information about RMAN backups made to the Oracle Secure Backup SBT interface, the metadata is managed by RMAN.

Oracle Secure Backup maintains its own catalog of backup metadata; this backup catalog is located on the administrative server and is not managed by RMAN. You can use the Oracle Secure Backup Web tool to display catalog metadata about RMAN jobs and backup pieces. Alternatively, you can use the `lsjob`, `catxcr`, and `lspiece` commands in `obtool`.

Expiration of RMAN Backups

You can make RMAN backups on volumes that use a content-managed expiration policy or time-managed expiration policy (see "Volume Expiration Policies" on page 2-24). In general, you should use the DELETE command in RMAN to mark backup pieces on tape as deleted. 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.

If you use the rmpiece command in Oracle Secure Backup to delete backup pieces from tape, then the RMAN metadata will fail to reflect the tape contents. This discrepancy can also occur when RMAN backup pieces exist on volumes that are expired by time-managed policy, or when you forcibly overwrite a volume containing RMAN backup pieces. Use the CROSSCHECK command in RMAN to resolve discrepancies between tape backups and the RMAN repository.

See Also:

- *Oracle Database Backup and Recovery Basics* to learn about crosschecking backups
- *Oracle Database Backup and Recovery Basics* to learn about 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. "Managing Backup and Restore Jobs" on page 10-2 explains how to manage file system and database backup and restore jobs.

When you use RMAN to backup or restore a database, the job contains the name of the database. Example 6–4 shows sample output for backup and restore jobs relating to a database named orcl.

Example 6–4 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
```

Note: If multiple RMAN sessions are running concurrently on a database, then the sessions are grouped in the same Oracle Secure Backup job.

Displaying Job Transcripts

Job transcripts contain detailed information, low-level about RMAN jobs. "Displaying Job Transcripts" on page 10-4 explains how to use the Web tool to display transcripts. Alternatively, you can use the catxcr command in obtool.

Example 6–5 shows part of the transcript for an archived log backup. This backup uses the `RMAN-DEFAULT` media family.

Example 6–5 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* to learn about the job commands

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 Advanced User's Guide* to learn how troubleshoot RMAN backup and restore operations

Displaying Backup Piece Information

Typically, you use RMAN to access metadata about RMAN backup sets. You can also view RMAN backup piece information in Oracle Secure Backup.

As explained in "Backup Sets and Backup Images" on page 2-10, an RMAN backup piece is represented in Oracle Secure Backup as a backup image. "Managing Backup Images" on page 10-9 explains how to use the Web tool to display information about backup pieces recorded in the Oracle Secure Backup catalog. Alternatively, you can use `lspiece` command. Example 6–6 shows sample output for `lspiece`.

Example 6–6 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: *Oracle Secure Backup Reference* to learn about the `lspiece` command

Adding Information About RMAN Backups to the Oracle Secure Backup Catalog

In some circumstances, a tape may contain information about RMAN backups when this information is not in the Oracle Secure Backup catalog. The situation could occur if a disk fails and you must restore files on the administrative server as described in "Restoring Critical Data on the Administrative Server" on page 8-10.

To add metadata about RMAN backups to the Oracle Secure Backup catalog, you must use the `obtar` command-line utility rather than the Web tool or `obtool`. "Cataloging the Contents of a Backup Image" on page 12-12 explains how to use the `-tG` options in `obtar` to recatalog the files.

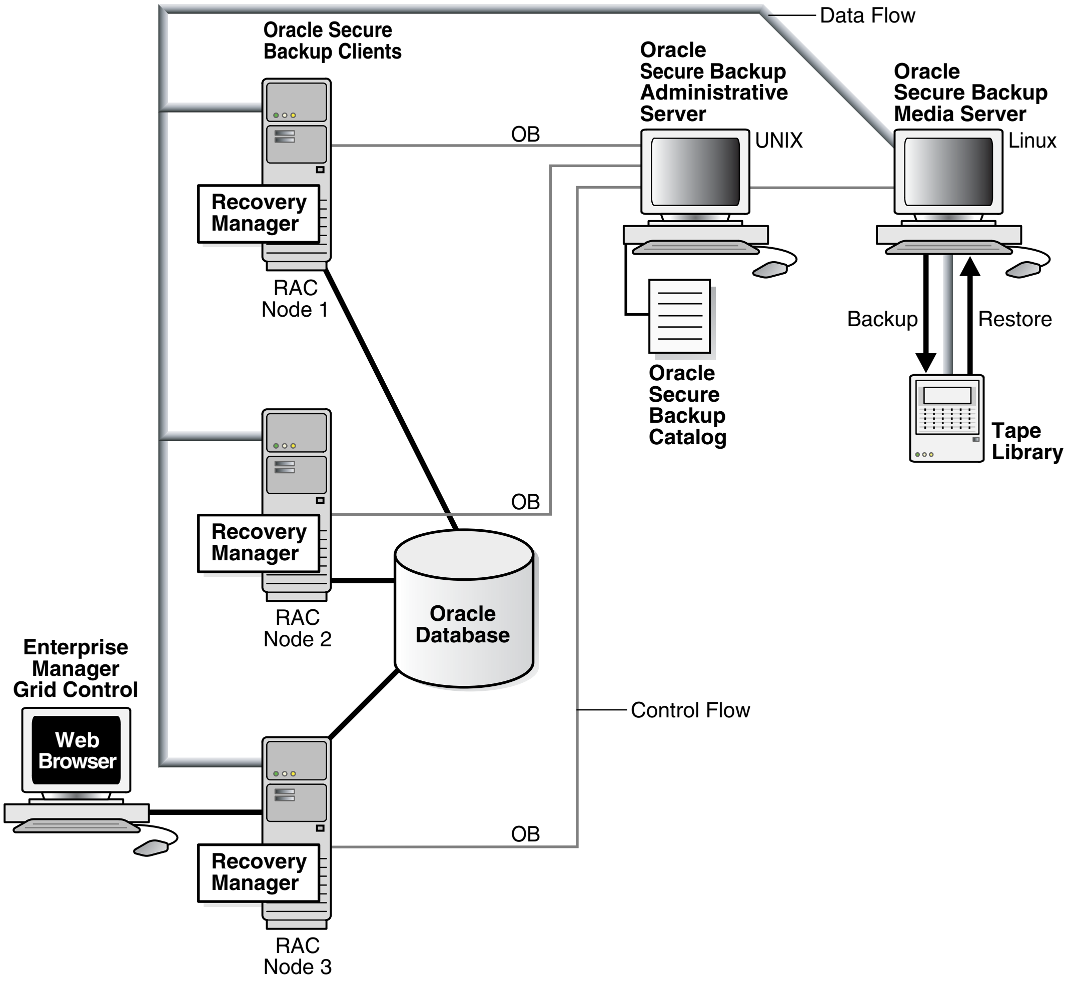
Using RMAN and Oracle Secure Backup in a Real Application Clusters Environment

You can use the Oracle Secure Backup SBT library in conjunction with RMAN to back up the database in an Oracle Real Application Clusters (RAC) system. If the Oracle Secure Backup software is installed on a cluster node, then RMAN can connect to the database instance on this node and then back up or restore data by means of the SBT library on this node.

It is recommended that you install Oracle Secure Backup on each node in the cluster. This practice enables RMAN to connect to any instance and initiate SBT operations. 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.

The best practice is to configure each RAC node as a client host within the administrative domain. You can use Oracle Secure Backup to back up node-specific configuration data on the file system of each node. Note that Oracle Secure Backup handles file system backups of a RAC client no differently from any other client host. Figure 6–6 shows a sample administrative domain that includes a three-node RAC system, with each node configured as an Oracle Secure Backup client.

Figure 6–6 Using RMAN and Oracle Secure Backup in a Real Application Clusters Environment



7

Backing Up File System Data

This chapter explains how to make backups of the file system with Oracle Secure Backup. This chapter contains the following topics:

- Overview of File System Backups
- Creating Dataset Files
- Configuring Backup Windows
- Configuring Backup Schedules
- Configuring Triggers
- Performing On-Demand File System Backups
- Backing Up Critical Data on the Administrative Server

Overview of File System Backups

This section provides an overview of how to schedule and perform file system backups. Unlike Recovery Manager (RMAN) database backups made through the SBT interface, file system backups are initiated by Oracle Secure Backup and can include any file on the file system.

You can set up backup schedules so that file system backups occur automatically at user-defined intervals. You can also perform on-demand backups, which are one-time-only backups. You can create scheduled and on-demand file system backups with either the Web tool or `obtool` (but not Enterprise Manager). This chapter assumes that you are using the Web tool.

Before proceeding to set up your backups, make sure that you have performed all necessary configuration steps as described in "Overview of Administrative Domain Configuration" on page 4-2.

> **See Also:** Chapter 6, "Using Recovery Manager with Oracle Secure Backup" to learn how to perform RMAN backups

Overview of Scheduled Backups

Scheduled backups are the basis of your backup strategy. Your first task after setting up the administrative domain choosing and configuring a backup schedule that makes sense for your environment.

This section contains the following topics:

- Choosing a Backup Strategy
- Choosing a Backup Schedule
- Configuring a Backup Schedule

Choosing a Backup Strategy

Because there is not a 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 need to consider several factors when determining the best method of performing backups at your site:

- How much data do you need to back up?

  If you need to back up a large amount of data, then you will probably want to consider some combination of full and incremental backups. 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 your dataset files include only the path names that you need to include in the backup.

- How will you protect the critical data on the administrative server?

  The administrative server manages all of the administrative data for your network and so must be protected. "Backing Up Critical Data on the Administrative Server" on page 7-24 explains how to perform this task.

Caution: You should regularly back up the Oracle Secure Backup home directory on the administrative server. The administrative server manages the backup and configuration data for the entire administrative domain.

- How frequently will you be expected to make backups, both full and incremental?

  Your management or users may expect full backups to be performed at a certain frequency.

- How frequently do you need to restore data?

  You may need to perform restore operations many times a day or only rarely. If you need to restore data frequently, then you may also want to perform full backups frequently to decrease the amount of time needed to restore. If you perform restore operations infrequently, however, then you may 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?

  As explained in "Administrative Data" on page 1-7, 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 may want to use more than one administrative domain.

Choosing a Backup Schedule

As explained in "Full and Incremental File System Backups" on page 2-2, 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.

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 would only need to restore the contents of the most recent backup image to fully restore a given tree. If you use incremental backups, however, then you may need 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 may need 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.

Cumulative Incremental Backup Strategy: Example 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 two backups:

- The full backup made on Sunday
- The most recent incremental backup

Restoring `/data` on Saturday or Sunday would require the volumes from three backups:

- The full backup made on Sunday
- The incremental backup made on Thursday
- The incremental backup made on Friday

Configuring a Backup Schedule

The basic steps for configuring a backup schedule are as follows:

1. Log in to the administrative domain as `admin` or a user with the `modify administrative domain's configuration` right.
2. Create datasets.

   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 domain and specify which paths should be included in the backup of each host. "Creating Dataset Files" on page 7-5 explains how to create dataset files.
3. Create backup windows.

   Backup windows are time ranges within which Oracle Secure Backup can run scheduled backup jobs. 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. "Configuring Backup Windows" on page 7-10 explains how to configure backup windows.
4. Create backup schedules.

Backup schedules specify the dataset, media family, backup priority, and so on. "Configuring Backup Schedules" on page 7-12 explains how to configure schedules.

5. Create triggers.

   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, no backups will occur. "Configuring Triggers" on page 7-15 explains how to configure triggers.

Overview of On-Demand Backups

Although scheduled backups are the basis of your backup strategy, you may also need to make one-time-only backups. On-demand backups are useful for supplementing your scheduled backups as well as testing whether the administrative domain is correctly configured.

The basic steps for creating on-demand backups are as follows:

1. Create datasets (if they are not already created).

   "Creating Dataset Files" on page 7-5 explains how to create dataset files. Note that to create dataset files you must have the `modify administrative domain's configuration` right.

2. Log in to the administrative domain as an Oracle Secure Backup user with the rights to perform the backup and the UNIX/Linux or Windows account needed to access the data to be backed up.

   You need the `perform backups as self` right to perform unprivileged backups and `perform backups as privileged user` to perform privileged backups.

3. Create one or more backup requests.

   As explained in "Jobs and Requests" on page 2-11, Oracle Secure Backup saves each backup request locally in your Web tool or `obtool` session until you send it to the scheduler. In this state, the backup is not eligible to run.

   "Creating an On-Demand Backup Request" on page 7-22 explains how to create backup requests.

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

   "Displaying the Backup Now Page" on page 7-21 shows the page in which you can display backup requests. "Removing a Backup Request" on page 7-23 explains how to delete backup requests.

5. Send all queued backup requests to the Oracle Secure Backup scheduler.

   "Sending Backup Requests to the Scheduler" on page 7-23 explains how to send backup requests to the scheduler. After requests are sent to the scheduler, they are jobs and are eligible to run.

Creating Dataset Files

This section describes how to create dataset files, which describe the file system data that Oracle Secure Backup should back up. "Backup Datasets" on page 2-3 provides a conceptual overview of datasets. *Oracle Secure Backup Reference* describes the dataset language syntax.

This section contains the following topics:

About Dataset Files

When configuring your dataset files, it may 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 One Host in Every Dataset File

A typical strategy is to create one dataset file for every host that you want to back up. For example, assume that your administrative domain includes clients `brhost2`, `brhost3`, and `brhost4`. You could create the dataset files `brhost2.ds`, `brhost3.ds`, and `brhost4.ds` as shown in the following examples. Each of the examples excludes core dumps and editor backup files.

Example 7–1 includes all files in the `/`, `/usr`, and `/home` file systems on host `brhost2` except for core dumps and editor backup files.

Example 7–1 brhost2.ds

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

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

Example 7–2 includes all files in the `/` and `/usr` file systems on host `brhost3` except for core dumps and editor backup files.

Example 7–2 brhost3.ds

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

    include path /
    include path /usr
}
```

Example 7–3 includes all files in the `C:\Documents and Settings` folder on host `winhost1` except for log files.

Note: Surround path names containing spaces with single or double quotes, for example, `"C:\Documents and Settings"`.

Example 7–3 winhost1.ds

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

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 7–4 uses `obtool` to schedule three backups jobs on Saturday morning.

Example 7–4 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`, 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 7–5 specifies the backup of the `/` and `/home` file systems on hosts `brhost2`, `brhost3`, and `brhost4`.

Example 7–5 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
```

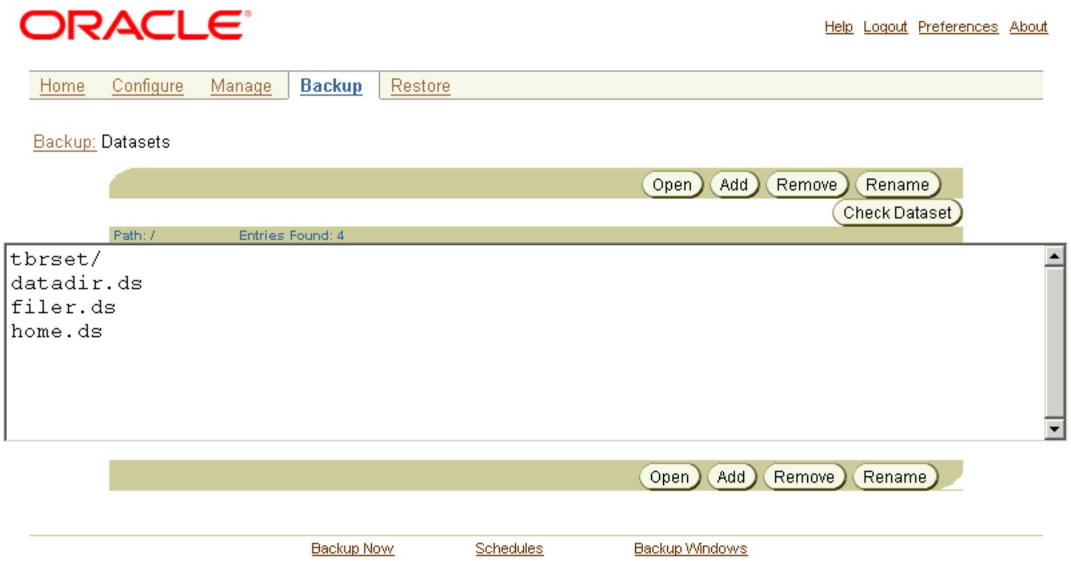
Unless an unusual event occurs, such as a tape device failure or a client host that is not available, Oracle Secure Backup attempts to back up the hosts in the order listed in the dataset file to the same volume set on the same media server.

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 7–1. This page lists all dataset files and dataset directories. Dataset directories appear in the Path box 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 7–1 Datasets Page



ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Open Add Remove Rename
Check Dataset
Open Add Remove Rename
Backup Now Schedules Backup Windows

Backup: Datasets

Path: / Entries Found: 4

```
tbrset/
datadir.ds
filer.ds
home.ds
```

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

Creating a Dataset File

To create a dataset file:

1. In the Datasets page, click the **Add** button to create a new dataset file.

   > **Note:** When you create a new dataset file, the initial contents of the dataset are defined by a dataset template.

2. In the **Dataset type** list, select **File** or **Directory**.

   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 data files.

   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, it is equivalent to naming all of the dataset files contained within the dataset directory tree.

   > **Note:** Dataset directories can be nested up to 10 levels deep.

3. In the **Name** field, enter a name for the dataset file.
4. Update the dataset statements displayed in the template file to define your backup data. Refer to *Oracle Secure Backup Reference* for dataset syntax and examples of datasets.
5. Choose one of the following:

- Click the **Save** button to accept your entries and return to the **Datasets** page.
- Click **Cancel** to void the operation and move back one page.

Oracle Secure Backup displays a message in the Status box if your dataset file has errors. See "Checking a Dataset File" on page 7-9 for details on errors.

Checking a Dataset File

This section explains how to check a dataset file for errors. You can check a dataset file at any time during editing.

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.

To check a dataset file for errors:

1. In the Datasets page, select a dataset file name from the **Path** box.

   Note: You can only check a dataset file, not a dataset directory.

2. Click the **Check Dataset** button.

   If the dataset syntax has no errors, the Web tool displays a message verification.

   If the dataset syntax has an error, the Web tool displays a message indicating the error.

3. Fix any errors that appear and recheck the dataset syntax.

Editing a Dataset File

To edit parameters for an existing dataset file:

1. In the Datasets page, select the name of the dataset file from the **Path** box.
2. Click the **Open** button.

   The Web tool displays a page with details of the dataset file.

3. Make needed changes and select one of the following:
   - Press **Save** to accept your changes and return to the Datasets page. Oracle Secure Backup automatically checks the dataset file for errors.
   - Click **Cancel** to void the operation and move back one page.

Removing a Dataset File

To remove a dataset file or directory:

1. In the Datasets page, select the name of the dataset file or directory from the **Path** box.
2. Click the **Remove** button.

   The Web tool prompts you to confirm the removal of the dataset file or directory.

3. Click **Yes** to remove the dataset file or directory.

   The dataset file or directory is removed and you are returned to the Datasets page.

Renaming a Dataset

To rename a dataset file or directory:

1. In the Datasets page, select the name of the dataset file or directory from the **Path** box.
2. Click the **Rename** button.

   The Web tool prompts you for the new name.
3. In the **Rename** box, enter the new name for the dataset file or directory.
4. Click **Yes** to accept the new name.

   The dataset file or directory is renamed and you are returned to the Datasets page.

Configuring Backup Windows

This section describes backup windows, which are user-specified time ranges within which Oracle Secure Backup can perform scheduled backup jobs. The default backup window is daily 00:00-24:00 and should only be changed if necessary for your environment.

This section contains the following topics:

- Displaying the Backup Windows Page
- Creating a Backup Window
- Specifying a Day Range
- Specifying a Single Date
- Removing a Backup Window

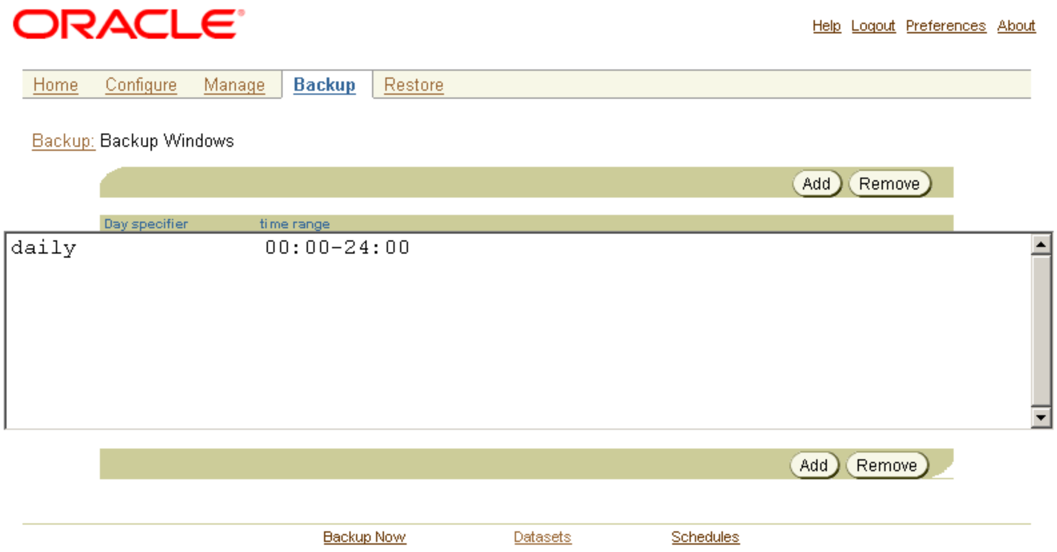
> **See Also:** "Scheduled and On-Demand Backups" on page 2-4 for a conceptual overview of backup windows

Displaying the Backup Windows Page

In the Backup page, click **Backup Windows** to display the page shown in Figure 7–2. In the central box, the Web tool displays any existing backup windows.

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

Figure 7–2 Backup Windows Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Backup: Backup Windows
Add Remove
Day specifier
time range
Add Remove
Backup Now Datasets Schedules

```
daily                   00:00-24:00
```

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

Creating a Backup Window

To create a backup window:

1. From the Backup window, click **Backup Windows**.
2. Click the **Add** button to add a new backup window.
3. In the **Type** list, select a backup window type. Your choices are:
   - **Day range**

     If you select this option, proceed to the instructions in "Specifying a Day Range" on page 7-11.
   - **Date**

     If you select this option, proceed to the instructions in "Specifying a Single Date" on page 7-12.

Specifying a Day Range

To specify a day range:

1. Select the days for which you want to set the backup window. Your choices are:
   - **Select daily**

     Specify this option to set the backup window for each day of the week.
   - **Select weekdays**

     Specify this option to set the backup window for Monday through Friday.
   - **Select weekend**

     Specify this option to set the backup window for Saturday and Sunday.
2. In the **Time range** box, enter a local time range. Oracle Secure Backup starts scheduled backups 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 (for example, 1430, which indicates 2:30 pm). Time ranges are expressed in 24-hour format. The time range is local-time based 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, 20:00-24:00 indicates 8:00 pm as the open time and midnight at the end of the same day as the close time.

3. Click **OK** or **Cancel**.

Specifying a Single Date

This section explains how to backup one day a month only

1. In the **Month**, **Day**, and **Year** boxes, specify the date on which you want the backup to run.
2. In the **Time range** box, select a local time range (hour and minutes) of day in which to execute a backup job. The time is expressed in 24-hour format.
3. Click **OK** or **Cancel**.

Removing a Backup Window

To remove an existing backup window:

1. In the **Backup Windows** page, select the name of the backup window that you want to remove.
2. Click the **Remove** button.

   The Web tool prompts you to confirm the removal of the backup window.
3. Click **Yes** to remove the backup window.

Configuring Backup Schedules

This section explains how to create and configure backup schedules. This section contains the following topics:

About Backup Schedules

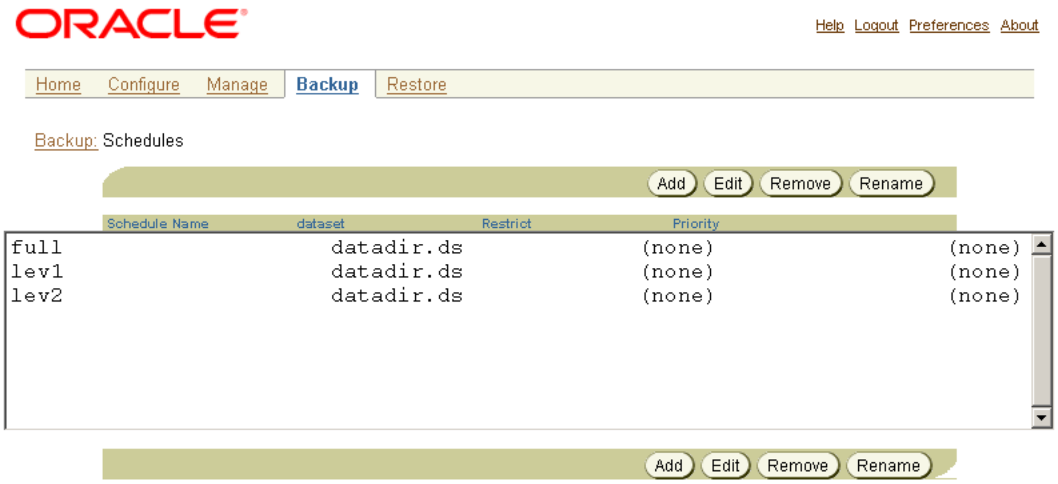
A backup schedule tells Oracle Secure Backup what data to back up and when. In the backup schedule you specify:

- 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
- 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

Displaying the Schedules Page

In the Backup page, click **Schedules** to display the page shown in Figure 7–3. In the central box, the Web tool displays any existing backup schedules. You can perform all backup schedule creation and configuration tasks in this page or in pages to which it provides links.

Figure 7–3 Backup Schedules Page



Schedule Name	dataset	Restrict	Priority
full	datadir.ds	(none)	(none)
lev1	datadir.ds	(none)	(none)
lev2	datadir.ds	(none)	(none)

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

Creating a Backup Schedule

To create a backup schedule:

1. In the Schedules page, click the **Add** button to open the New Schedules page.
2. In the **Schedule** box, enter a name for the schedule.

   The name you enter must start with an alphanumeric character. It can contain letters, numerals, dashes, underscores, or periods. The maximum character length of 127 characters. You cannot uses spaces in the name you enter.
3. In the **Priority** box, enter a priority number for the backup job. The default priority is 100.

   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.
4. In the **Datasets** box, select one or more dataset files or directories that you want to include in the backup job.

5. In the **Restrictions** box, optionally select a restriction. You can restrict scheduled backups to specific devices. If you do not select a restriction (default), then the backups defined by the schedule can use any available device on any media server, at the discretion of the Oracle Secure Backup scheduling system.
6. In the **Comments** box, optionally enter any information that want to store with the backup schedule.
7. Click **Apply**, **OK**, or **Cancel**.

Editing a Backup Schedule

To edit properties for an existing backup schedule:

1. In the Schedules page, click the **Edit** button.

   The Web tool displays a page with details of the backup schedule.
2. Make changes to the schedule properties.
3. Choose one of the following:
   - Click **Apply**, **OK**, or **Cancel**.
   - 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 "Configuring Triggers" on page 7-15 for more information.

Removing a Backup Schedule

To remove an existing backup schedule:

1. From the **Backup** menu, click **Schedules** in the submenu under **Settings**.
2. Select the name of the backup schedule that you want to remove from the **Schedule name** box.
3. Click the **Remove** button.

   A message appears prompting you to confirm the removal of the schedule.
4. Click **Yes** to remove the backup schedule.

   You are returned to **Schedules** page and the message "Success: name removed" appears in the **Status** box.

Renaming a Backup Schedule

To rename a backup schedule:

1. From the **Backup** menu, click **Schedules** in the submenu under **Settings**.
2. Select the name of the backup schedule that you want to rename from the **Schedule name** box.
3. Click the **Rename** button.

   A message appears prompting you to enter the new name.
4. Enter a new name for the backup schedule.
5. Click **Yes** to accept the new name.

You are returned to **Schedules** page and a message appears in **Status** box telling you that the schedule was successfully renamed.

Viewing Schedule Properties

To view schedule properties:

1. From the **Backup** menu, click **Schedules** in the submenu under **Settings**.
2. Select the name of the schedule from which you want to view properties from the **Schedule name** box.
3. Click the **Edit** button.

   The Web tool displays a page with the properties for the schedule name you selected.
4. Click **Triggers**.

   The Triggers page appears.
5. Select the trigger that you want to view and click **Preview**.

Configuring Triggers

This section explains how to create and configure backup schedules. This section contains the following topics:

- About Triggers
- Creating a Trigger
- Editing a Trigger
- Removing a Trigger
- Displaying a Trigger Schedule

About 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.

Creating a Trigger

To create a trigger:

1. In the Schedules page, select the schedule for which you want to create a trigger and click the **Edit** button.
2. Click the **Triggers** button.

   The Web tool displays the Triggers page.
3. In the **Trigger type** box, select a time representation you want to use to define when to perform the backup job. Your choices are the following:

   - **One time**

     Select this option to perform a backup only once. If you select this option, see "Creating a One-Time Backup Trigger" on page 7-18 to continue.

- **Day** (default)

  Select this option to perform a backup one or more days during the week. If you select this option, proceed to the instructions in "Creating a Daily Backup Trigger" on page 7-16.

- **Month**

  Select this option to perform a backup one day every month. If you select this option, proceed to the instructions in "Creating a Monthly Backup Trigger" on page 7-18.

- **Quarter**

  Select this option to perform a backup one day every quarter. If you select this option, proceed to the instructions in "Creating a Quarterly Backup Trigger" on page 7-18.

- **Year**

  Select this option to perform a backup one day during the year. If you select this option, proceed to the instructions in "Creating a Yearly Backup Trigger" on page 7-19.

Creating a Daily Backup Trigger

To create a daily backup trigger:

1. In the Schedules page, select the schedule for which you want to create a trigger and click the **Edit** button.
2. Click the **Triggers** button.

   The Web tool displays the Triggers page.
3. Select a backup level from the **Backup level** box. Your choices are:

   - **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. Notably, the **incr** option does not apply to Network Appliance filers.

   - **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 offsite storage without disturbing your schedule of incremental backups.

4. In the **Backup at** lists, select the time at which you want to start the backup. The time is in military format and is expressed in hours and minutes.
5. In the **Media family** box, select a media family to which the data of this scheduled backup should be assigned.
6. In the **Expire after** box, optionally choose an expiration time period for the backup job.
7. Select the days which Oracle Secure Backup will run the scheduled backup. Your choices are the following:
   - **Select daily**

     Check this box to trigger the schedule to run on all 7 days of the week. For example, trigger the backup to run every day at 8:00 a.m.
   - **Select weekdays**

     Check this box to trigger the backup to run on weekdays only (Monday through Friday). For example, trigger the backup to run weekdays at 8:00 a.m.
   - **Select weekend**

     Check this box to trigger the backup to run on weekends only (Saturday and Sunday). For example, trigger the backup to run weekends at 8:00 a.m.
   - Alternatively, from both the **Select weekdays** and **Select weekends** boxes you can select a mix of individual days on which you can trigger scheduled backups to run. For example, trigger the backup on Monday, Tuesday, and Saturday at 8:00 a.m.
8. From the **Week in month** group, select an option 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. In the **Except** list, specify weekday exceptions. 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. In the **Time** list, select a time for the exception. 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. In the **Specify day** lists, select the day of the exception. For example, you can specify **last Monday**. By using the values in the previous steps, you can tell Oracle

Secure Backup to trigger every weekend except after the last Monday of the month.

12. Select among the following:

    - Click **Add** to accept your entries and add the trigger.

      The schedule is displayed in the main tax. The schedule displays the level of the backup, the time at which it is to begin, and the days on which the backup is to be performed.

    - Click **Remove** to delete the trigger.
    - Click **Cancel** to void the operation and move back one page.

Creating a One-Time Backup Trigger

To create a one-time backup trigger:

1. In the Schedules page, select the schedule to which you want to add a trigger and click the **Edit** button.

   The Web tool displays a page with details of the backup schedule.

2. Click the **Triggers** button.
3. Select **One time** from the **Trigger type** box.
4. Follow Steps 3 through 6 in the section entitled "Creating a Daily Backup Trigger" on page 7-16.
5. In the **Month**, **Day**, and **Year** boxes, select the date that you want the one-time backup to run.
6. Click **Add** to accept your entries and add the trigger.

   The Web tool returns you to the Triggers page. The schedule is displayed in the central text box.

Creating a Monthly Backup Trigger

To schedule a monthly backup trigger:

1. In the Schedules page, select the schedule for which you want to create a trigger and click the **Edit** button.
2. Click the **Triggers** button.

   The Web tool displays the Triggers page.

3. In the **Trigger type** box, select **Month**.
4. Follow Steps 3 through 6 in the section entitled "Creating a Daily Backup Trigger" on page 7-16.
5. In the **Day in month** group, select a day of the month.
6. Click **Add** to accept your entries and add the trigger.

   The Web tool returns you to the Triggers page. The schedule is displayed in the central text box.

Creating a Quarterly Backup Trigger

To schedule a quarterly backup trigger:

1. In the Schedules page, select the schedule for which you want to create a trigger and click the **Edit** button.

2. Click the **Triggers** button.

   The Web tool displays the Triggers page.

3. In the **Trigger type** box, select **Quarter**.

4. Follow Steps 3 through 6 in the section entitled "Creating a Daily Backup Trigger" on page 7-16.

5. 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 last 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.

6. Click **Add** to accept your entries and add the trigger.

   The Web tool returns you to the Triggers page. The schedule is displayed in the central text box.

Creating a Yearly Backup Trigger

To create a yearly backup trigger:

1. In the Schedules page, select the schedule for which you want to create a trigger and click the **Edit** button.

2. Click the **Triggers** button.

   The Web tool displays the Triggers page.

3. In the **Trigger type** box, select **Year**.

4. Follow Steps 3 through 6 in the section entitled "Creating a Daily Backup Trigger" on page 7-16.

5. 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)

6. Click **Add** to accept your entries and add the trigger.

   The Web tool returns you to the Triggers page. The schedule is displayed in the central text box.

Editing a Trigger

To edit a trigger:

1. In the Schedules page, select the schedule for which you want to edit a trigger and click the **Edit** button.

2. Click the **Triggers** button.

   The Web tool displays the Triggers page.

3. Click the **Edit** button.

4. Make needed changes.
5. Click **Apply** or **Cancel**.

Removing a Trigger

To remove a trigger:

1. In the Schedules page, select the schedule for which you want to edit a trigger and click the **Edit** button.
2. Click the **Triggers** button.

   The Web tool displays the Triggers page.
3. In the central box, select the trigger to be removed.
4. Click **Remove**.

Displaying a Trigger Schedule

To display a trigger schedule:

1. In the Schedules page, select the schedule for which you want to edit a trigger and click the **Edit** button.
2. Click the **Triggers** button.

   The Web tool displays the Triggers page.
3. In the central box, select the trigger to be displayed.
4. Click the **Preview** button.

Performing On-Demand File System Backups

This section contains the following topics:

- About On-Demand File System Backups
- Displaying the Backup Now Page
- Creating an On-Demand Backup Request
- Removing a Backup Request
- Sending Backup Requests to the Scheduler

About On-Demand File System Backups

On-demand backups are ad hoc or one-time-only backups of the data in a dataset. For example, you can instruct Oracle Secure Backup to back up the Oracle home on client host `brhost2`. "Scheduled and On-Demand Backups" on page 2-4 provides a conceptual overview of on-demand backups.

Before You Begin

Before you can back up file system data on demand, you must perform the following tasks:

- Set up users, hosts, devices, media families, and classes.

  This section assumes that you have configured the administrative domain as described in Chapter 4, "Setting Up the Administrative Domain" and Chapter 5, "Configuring Backup and Media Settings". Note that two class rights apply especially to on-demand backups: `perform backups as self` and `perform backups as privileged user`.

- Create a dataset file that describes the data you want to back up. This task is described in "Creating a Dataset File" on page 7-8.
- Log in to the administrative domain as an Oracle Secure Backup user with the rights to perform the backup, and UNIX or Windows account needed to access the data to be backed up.

On-Demand Backup Work Flow

Perform the following steps to direct Oracle Secure Backup to create on-demand backups of file system data:

1. Create one or more backup requests.

   As explained in "Jobs and Requests" on page 2-11, Oracle Secure Backup saves each backup request privately in your Web tool or `obtool` session until you send it to the scheduler. In this state, it is not eligible to run.

   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 "Preferences" for more information.

2. At any time, add to, review or change this list of backup requests.

   You can add to, review, or change the list of restore requests at any time.

3. Send your backup requests to the scheduler.

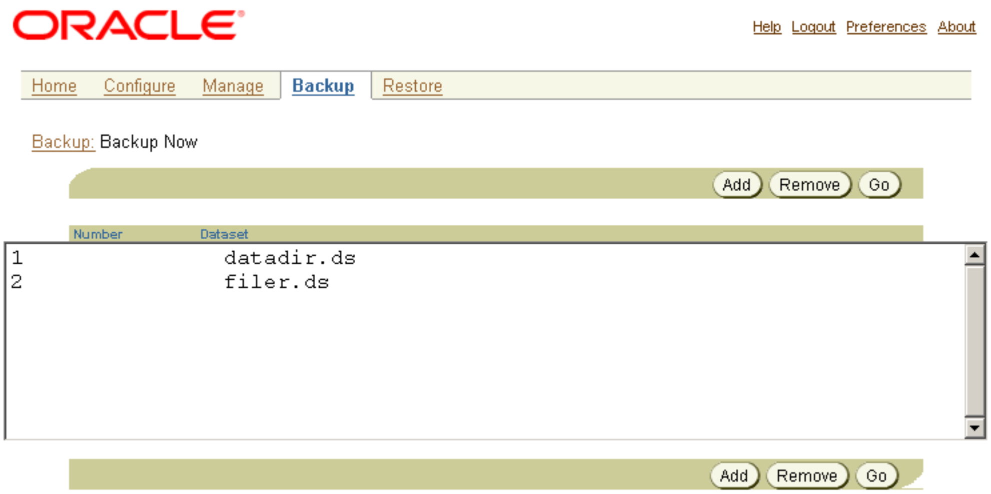
   As explained in "Jobs and Requests" on page 2-11, this action turns each backup request into a dataset job, making it eligible to run.

Displaying the Backup Now Page

In the Backup page, click **Backup Now** to display the page shown in Figure 7–4. In the central box, each backup request that you have created but not yet sent to the scheduler displays. 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 7–4 Backup Now Page



ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Backup: Backup Now
Add Remove Go
Number Dataset

```
1              datadir.ds
2              filer.ds
```

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

Creating an On-Demand Backup Request

To create an on-demand backup request:

1. In the Backup Now page, click the **Add** button to display the Options page.
2. In the **Datasets** box, select one or more dataset files or directories.
3. In the **Backup date** and **Backup time** boxes, select a future date and time for the backup to run. If you leave these fields unchanged, then Oracle Secure Backup considers your backup job as eligible to run immediately.
4. Using the **Expire after** box and list, optionally enter a time interval. For example, enter **3** and select **days** to specify a duration of 3 days. By default the expiration is **disabled**, which means that it will never expire. Refer to the *duration* placeholder description in *Oracle Secure Backup Reference* for more information.

   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** boxes.
5. Select a backup level from the **Backup level** box. 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. Notably, the **incr** option does not apply to Network Appliance filers.

- **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 offsite storage without disturbing your schedule of incremental backups.

6. In the **Media family** box, select a media family to which the date of this backup should be assigned. As explained in "Media Families" on page 2-23, a media family is a named classification of backup volumes.
7. In the **Restrictions** box, optionally enter the names of devices to which backups controlled by this database backup storage selector are restricted. Restrictions come in the following forms:

   - *device*, which specifies a particular device
   - *@hostname*, which specifies any drive attached to the specified host
   - *device@hostname*, which specified any drive-host attachment

   If this option is left blank, then Oracle Secure Backup uses device polling to find any available device for use in backup and restore operations.
8. In the **Priority** box, optionally change the priority of the backup job. The default value is **100**. 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.
9. Choose whether you want the backup to operate in **unprivileged** or **privileged** mode (see "Privileged and Unprivileged Backups" on page 2-5). Unprivileged mode is the default.
10. Click **OK** or **Cancel**.

Removing a Backup Request

This section explains how to remove a backup request you have created, but have not yet sent to the scheduler.

To remove a backup request:

1. From the **Backup** menu, click **Backup Now** in the submenu under **Operations**.

   The **Backup Now** page appears.
2. Select a backup request from the **Number/Dataset** box in the central panel.
3. Click the **Remove** button.

   A message appears in the status area advising you of the **Number** of the backup removed.

Sending Backup Requests to the Scheduler

To send all pending backup requests to the scheduler:

1. In the Backup Now page, click the **Go** button

   The Web tool sends each backup request that appears in the central box to the Oracle Secure Backup scheduler.

   The Web tool displays a message in the status area 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 central box is empty upon completion of the **Go** operation.

2. See "Displaying Job Transcripts" on page 10-4 to view the output for each job.

Backing Up Critical Data on the Administrative Server

"Administrative Data" on page 1-7 explains the importance of administrative data for the domain. If you lose the critical data stored on the administrative server, then you lose the configuration data for the domain as well as all backup and volume records.

It is recommended that you back up critical data on your administrative server as part of your normal backup routine. For example, you could make a full backup of the Oracle Secure Backup home every two weeks and an incremental backup every night. As part of your disaster recovery scenario, you should periodically make a backup of the Oracle Secure Backup home and related helpful files and store it in a safe place offsite. For example, you could back up this data every month.

It is recommended that you create one media family especially for your daily backups and one for your offsite backups. In this way, the tapes have readily identifiable volume IDs if you need to identify them quickly in a media failure or disaster recovery situation.

To back up critical data on the administrative server:

1. Create a dataset that includes the following directories and files on the administrative server:

   - Oracle Secure Backup home directory
   - The `/etc/obconfig` file (Linux and UNIX only)
   - The `/usr/etc/ob` file (Linux and UNIX only)

   Example 7–6 shows a sample dataset for the critical files on a Linux administrative server named `ashost`.

Example 7–6 ashost.ds

```
include host ashost {
    include path /usr/local/oracle/backup
    include path /etc/obconfig
    include path /usr/etc/ob
}
```

Example 7–7 shows a sample dataset for the critical files on a Windows administrative server named `winserver`.

Example 7–7 winserver.ds

```
include host winserver {
   include path "C:\Program Files\Oracle\Backup"
```

```
}
```

2. Create a privileged backup request, either on-demand or scheduled, that specifies the dataset created in the preceding step.
3. If the backup request is on-demand, then submit the request to the Oracle Secure Backup scheduler.

   If you are creating an offsite backup, proceed to the following steps.
4. After the backup job executes, save a transcript of the backup as a file and print the file. The following example uses the `catxcr` command in `obtool` to save the transcript of the `admin/4.1` backup job:

   ```
   obtool catxcr --level 0 admin/4.1 > /tmp/ashost.out
   ```

   You can also navigate to the `/usr/etc/ob/xcr` directory, which contains job transcripts. For example, you can display `admin@4.1` as follows:

   ```
   # cd /usr/etc/ob/xcr
   # ls
   admin@1.1       admin@3.1       admin@5.1       admin@7.1
   admin@2.1       admin@4         admin@6.1
   # more admin@4.1
   [4100000001]2006/01/23.15:16:12
   __________________________________
   [4100000001]2006/01/23.15:16:12
   [4100000002]2006/01/23.15:16:12 Transcript for job admin/4.1 running on ella
   [4100000002]2006/01/23.15:16:12
   [3100000003]2006/01/23.15:16:23 Info: mount data verified.
   [3100000004]2006/01/23.15:16:23 Info: volume in ellatape is
   ```
5. Optionally, print a copy of the SCSI parameters that you used to create the device special files for your tape devices (see *Oracle Secure Backup Installation Guide* for instructions on obtaining SCSI data).
6. Clearly mark the volume and store it in a safe location together with the printed job transcript and SCSI parameter summary.

See Also: "Restoring Critical Data on the Administrative Server" on page 8-10

8

Restoring File System Data

This chapter explains how to restore file system objects backed up by Oracle Secure Backup. This chapter contains the following topics:

- Overview of File System Restore Operations
- Performing a Catalog-Based Restore Operation
- Performing a Raw Restore Operation
- Restoring Critical Data on the Administrative Server

See Also:

- "Database Backup and Recovery" on page 2-10 for an overview of Oracle Secure Backup restore functionality
- *Oracle Secure Backup Reference* for a description of the restore commands in `obtool`

Overview of File System Restore Operations

This chapter assumes that you have read "File System Restore Operations" on page 2-9. You can restore file system data in the following ways:

- By browsing the catalog

  In this case, you browse the catalog to select the files to restore (see "Backup Catalog" on page 2-6).

- By identifying the media on which the backup is located

  In a raw restore operation, you specify a backup image file number and the volume ID of the volume on which it is stored.

- By using `obtar`

  In this case, you use `obtar` to access tapes directly. It is recommended that only expert users restore files by means of `obtar`.

This chapter explains how to perform catalog-based and raw restore operations. Restoring files with `obtar` is considered an advanced practice.

> **See Also:** Chapter 12, "Using obtar" to learn how to use `obtar`

Overview of Restore Operations

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 a user with the rights needed to browse and restore files. You need the following rights:

   - `perform restores as privileged user` right if you restore files in privileged mode or restore to an NDMP host.
   - `perform restores as self` right if you restore files in unprivileged mode.
   - `browse backup catalogs with this access` right set to a value other than `none` if you want to browse the catalog. The possible access values are `privileged`, `notdenied`, `permitted`, `named`, and `none`.

2. Identify the backups that you want to restore.

   For a catalog-based restore, locate the files in the catalog. "Browsing the Backup Catalog" on page 8-4 explains how to perform this task.

   For a raw restore, identify the volumes and backup section file numbers from which to restore the backups. "Displaying Backup Sections" on page 10-9 explains how to perform this task.

3. Create one or more restore requests.

   To create catalog-based restore requests, see "Sending Catalog-Based Restore Requests to the Scheduler" on page 8-7.

   To create raw restore requests, see "Sending Raw Restore Requests to the Scheduler" on page 8-10.

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 "Preferences" on page 3-7 for more information.

4. Delete the queued restore requests (if needed).

   To remove a catalog-based restore request, see "Removing a Catalog-Based Restore Request" on page 8-7.

   To remove a raw restore request, see "Removing a Raw Restore Request" on page 8-10.

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.

   To create catalog-based restore jobs, see "Sending Catalog-Based Restore Requests to the Scheduler" on page 8-7.

   To create raw restore jobs, see "Sending Raw Restore Requests to the Scheduler" on page 8-10.

Performing a Catalog-Based Restore Operation

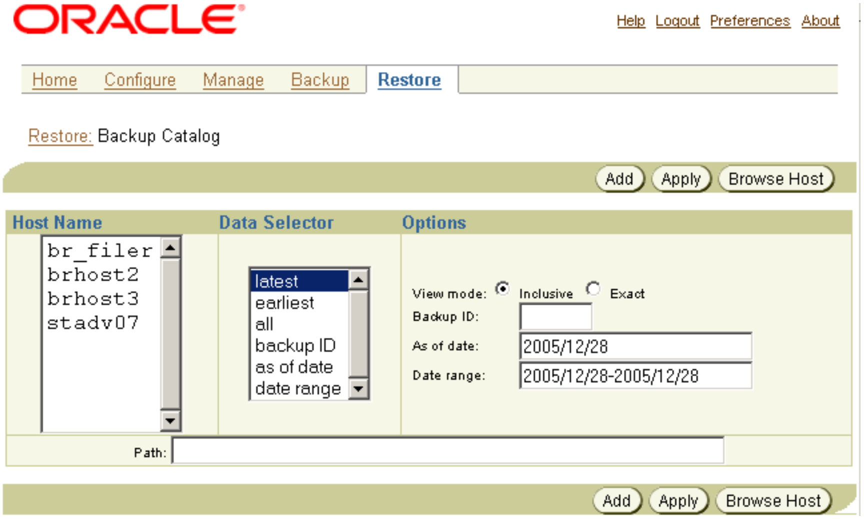
This section describes how to create a restore request by browsing a backup catalog. This section contains the following topics:

- Displaying the Backup Catalog Page
- Browsing the Backup Catalog
- Creating a Catalog-Based Restore Request
- Removing a Catalog-Based Restore Request
- Sending Catalog-Based Restore Requests to the Scheduler
- Listing All Backups of a Client

Displaying the Backup Catalog Page

In the Restore page, click **Backup Catalog** to display the Backup Catalog page, which is shown in Figure 8–1. You can use this page to browse the catalog for backups of files and directories.

Figure 8–1 Backup Catalog Page



ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Add Apply Browse Host
Add Apply Browse Host

Restore: Backup Catalog

Host Name: br_filer, brhost2, brhost3, stadv07

Data Selector: latest, earliest, all, backup ID, as of date, date range

Options

View mode: ● Inclusive ○ Exact

Backup ID:

As of date: 2005/12/28

Date range: 2005/12/28-2005/12/28

Path:

Browsing the Backup Catalog

To browse the catalog and designate specific data to restore:

1. In the Browse Catalog page, select a host name from the **Host Name** list box. The host should be the one on which the data was originally backed up.
2. In the **Data Selector** box, select one or more data selectors. See *Oracle Secure Backup Administrator's Guide* for a description of valid values for data selectors. Note the following data selector options:
   - If you select **backup ID**, enter one or more comma-delimited backup IDs in the **Backup ID** text box. "Listing All Backups of a Client" on page 8-7 explains how to obtain a backup ID from the list of backups for this client.
   - If you select **as of date**, enter a date and optionally a time in the **As of date** box. For example, enter `5/2`.
   - If you select **date range**, enter the range in the **Date range** text box. For example, enter `2005/5/1-2005/5/31`.
3. Select a **View mode**. See "Catalog View Modes" on page 2-8 for a description of the inclusive and exact view modes.
4. In the **Path** box, you can optionally enter the path name of the directory to browse. If you do not enter a path, then Oracle Secure Backup displays the top-most directory in the client's naming hierarchy.
5. Click **Browse Host**.

   Oracle Secure Backup displays the Browse Host page with the selected directory contents displayed.
6. 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 Web tool displays the contents of the selected directory, with the directory name in gray if you have visited it, in orange if you have not.
7. You can change the Data Selector at any time without leaving this page as follows:
   - Optionally, adjust the selections in the **Data Selector** list box.

- Optionally, update the **Backup ID**, **As of date**, or **Date range** text boxes if any apply.
- Click **Apply**.

  Oracle Secure Backup redisplays the page with the new data selector applied. If the view mode is inclusive, 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.

8. You can change the View mode without leaving this page as follows:
   - 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

In "Browsing the Backup Catalog" on page 8-4, you located the data you want to restore. In this section, you specify various restore options in order to finalize the restore request.

To create a catalog-based restore request:

1. Check the box next to 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 check box selections. If you do not, then Oracle Secure Backup discards those selections.

   The New Restore page appears.

3. Optionally, enter an alternate path name for each file or directory to restore. For example, enter `/tmp`.

   The original path name of each object you previously selected appears in 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. Optionally, select **Device** radio button to select a tape drive to use to perform the restore. By default, Oracle Secure Backup automatically selects the best drive.

5. Choose whether you want the restore to operate in unprivileged or privileged mode. Unprivileged mode is the default.

An unprivileged restore runs under your UNIX user identity or Windows account identity, as configured in your Oracle Secure Backup user profile (see "Configuring Users" on page 4-26.) Your access to file system data, therefore, is constrained by the rights of the UNIX user or Windows account having that identity.

> **Note:** On UNIX systems, a privileged restore job runs under the root user identity. On Windows systems, the job runs under the same account identity as the Oracle Secure Backup service on the Windows client.

6. Optionally enter one or more `obtar` options in the **Obtar option(s)** box. 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. Check the **No high speed positioning** box if you do not want to use available position data to speed the restore.
8. Click **NDMP incremental restore** to direct 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 file system backups created with `obtar`.

   Normally, restore operations are additive: each file and directory restored from a full or an incremental backup is added to its destination directory. If files have been added to a directory since the most recent Oracle Secure Backup backup, then a restore operation 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 a normal restore of `/home`, the directory would contain `file1` and `file2`; after an NDMP incremental restore of `/home`, the directory would contain only `file2`.

9. Click **Replace existing files** to overwrite any existing files with those restored from the backup image.

   Alternatively, click **Keep existing files** to keep any existing files instead of overwriting them with files from the backup image.

10. If you are restoring to a Windows system, click **Replace in use files** to replace in-use files with those from the backup image. Windows deletes each in-use file when the last user closes it.

    Alternatively, click **Keep in use files** to leave 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 box. Oracle Secure Backup should display 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 8-4.

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 any 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** box.

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 any host from the **Host Name** list box.
2. Click **Browse Host**.

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

   The Web tool sends each restore request that appears in the **Restore items** box 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 box is empty upon completion of the **Go** operation.
4. Display the transcript of the job to ensure that it completed successfully. See "Displaying Job Transcripts" on page 10-4 to learn how to display job output.

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 any 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

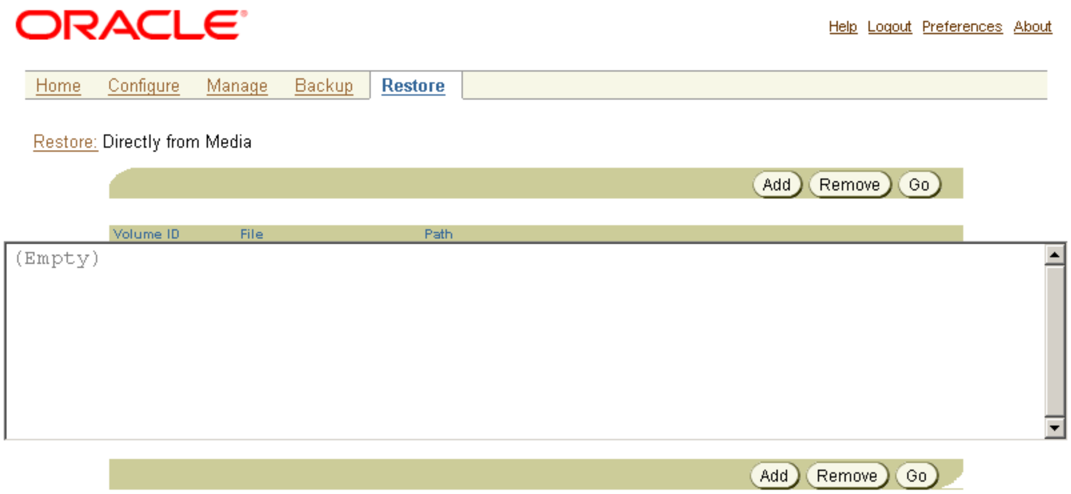
This section explains how to restore data without using a backup catalog. This section contains the following topics:

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

Displaying the Directly From Media Page

In the Restore page, click **Directly from Media** to display the page shown in Figure 8–2. You can use this page to perform a raw restore operation.

Figure 8–2 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

> **Note:** 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 (volume ID or barcode) of the tape volumes to which they were backed up
- 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. In the Device section, you can optionally click **Device** to select a tape drive to use for the restore operation. By default, Oracle Secure Backup automatically selects the best drive.

3. Choose whether you want the restore to operate in unprivileged or privileged mode. Unprivileged mode is the default.

4. In the **File Number** text box, enter the backup image file number from which to restore data. See "Volume Sets" on page 2-21 to learn about file numbers.

5. In the **Volume ID(s)** box, enter the first volume ID from which to begin data restore. See "Volume Sets" on page 2-21 to learn about volume IDs.

6. Optionally, enter the volume tag of the first volume from which to begin restoring in the **Tag(s)** text box. As explained in "Volumes" on page 2-20, tag is the machine-readable barcode affixed to the volume.

   Note: Enter a Volume ID, a tag, or both. You cannot leave both fields blank.

7. Optionally enter one or more `obtar` options in the **Obtar option(s)** box.

   See the *Oracle Secure Backup Reference* for details on `obtar` options.

8. Check **NDMP incremental restore** to direct certain NAS data servers to apply incremental restore rules.

   Normally, restore operations are additive: each file and directory restored from a full 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.

9. Click **Replace existing files** to overwrite any existing files with those restored from the backup image.

   Alternatively, click **Keep existing files** to keep any existing files instead of overwriting them with files from the backup image.

10. If you are restoring to a Windows system, click **Replace in use files** to replace in-use files with those from the backup image. Windows deletes each in-use file when the last user closes it.

    Alternatively, click **Keep in use files** to leave any in-use Windows files unchanged.

11. Select **All** to restore the entire contents of the backup image file you selected.

    Alternatively, select **File** to restore a specific file or directory. If you select **File**, then do the following:

    - Enter the name of the file or directory to restore in the text box to the right of the **File** radio button.
    - 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** box. If you do not, leave this field blank.

12. In the **To host** list, select a host to which to restore the data.
13. In the **Alternate path** text box, enter a path name 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`.
14. Click **OK** to accept your selections or **Cancel** to discard them.

    Oracle Secure Backup returns you to the **Restore from Media** page. If you clicked **OK**, the raw restore request you just made appears in the list box. 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 box.

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 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 box is empty upon completion of the **Go** operation.
2. Display the transcript of the job to ensure that it completed successfully. See "Displaying Job Transcripts" on page 10-4 to learn how to display job output.

Restoring Critical Data on the Administrative Server

This section assumes that you have been making regular backups of the administrative server as recommended in "Backing Up Critical Data on the Administrative Server" on page 7-24. This section describes the basic procedure for restoring the `admin` directory in the event of media failure or loss of the administrative server.

The instructions for installing Oracle Secure Backup on the administrative server are explained in "Loading and Installing the Oracle Secure Backup Software on Linux or UNIX" in *Oracle Secure Backup Installation Guide*. You should refer to this manual when reinstalling Oracle Secure Backup.

The sample output in the following procedure restores the administrative data on a UNIX host named `ella`. This host has an attached tape library that contains a single tape drive. Note that the sample output is often truncated or reformatted because of space constraints.

To restore the administrative data after a media failure:

1. If the administrative server is a Linux or UNIX media server, then gather the SCSI information needed to create the device special files. If you saved a print copy of this information with your backup volume, then you can use this saved information; otherwise, obtain the SCSI information as described in *Oracle Secure Backup Installation Guide*.

2. Run `setup` to load the Oracle Secure Backup software from the installation media. The following example loads Linux and UNIX packages:

```
# /cdrom/cdrom0/setup
Welcome to Oracle's setup program for Oracle Secure Backup.  This
program loads Oracle Secure Backup software from the CD-ROM to a
filesystem directory of your choosing.

This CD-ROM contains Oracle Secure Backup version 10.1.060119.

Please wait a moment while I learn about this host... done.

Would you like to load the Oracle Secure Backup software into your
current directory /export/home/oracle/backup?
(Oracle recommends using /usr/local/oracle/backup as the Oracle
  Secure Backup home)
A 'yes' answer proceeds to use the current directory [yes]:

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
You may load any of the following Oracle Secure Backup packages:
    1. linux32 (RH 2.1, RHEL 3, RHEL 4, SuSE 8, SuSE 9)
       administrative server, media server, client
    2. solaris64 (Solaris 2.8 and later, SPARC)
       administrative server, media server, client

Enter a space-separated list of packages you'd like to load.  To load all
packages, enter 'all' [2]:
.
.
.
Loading of Oracle Secure Backup software from CD-ROM is complete.
You may unmount and remove the CD-ROM.
Would you like to continue Oracle Secure Backup installation with
'installob' now?  (The Oracle Secure Backup Installation Guide
contains complete information about installob.)
Please answer 'yes' or 'no' [yes]:
```

3. Install the Oracle Secure Backup software, assigning this host the role of administrative server. Note that the following message is expected behavior: `Error: can't connect to local observiced.`

```
Welcome to installob, Oracle Secure Backup's UNIX installation program.
.
```

```
.
.
Please wait a few seconds while I learn about this machine... done.

Have you already reviewed and customized install/obparameters for your
Oracle Secure Backup installation [yes]? yes

Verifying that installation parameters are correct... done.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

You can choose to install Oracle Secure Backup in one of two ways:
    (a) interactively, by answering questions asked by this program, or
    (b) in batch mode, by preparing a network description file

Use interactive mode to install Oracle Secure Backup on a small number
of hosts.  Use batch mode to install Oracle Secure Backup on any number
of hosts.

Which installation method would you like to use (a or b) [a]?a
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Oracle Secure Backup is not yet installed on this machine.

Oracle Secure Backup's Web server has been loaded, but is not yet configured.

You can install this host one of three ways:
    (a) administrative server
        (the host will also be able to act as a media server or client)
    (b) media server
        (the host will also be able to act as a client)
    (c) client

If you are not sure which way to install, please refer to the Oracle
Secure Backup Installation Guide. (a,b or c) [a]?

Beginning the installation.  This will take just a minute and will produce
several lines of informational output.

Installing Oracle Secure Backup on ella (solaris version 5.9)

You must now enter a password for the Oracle Secure Backup 'admin' user.
Oracle suggests you choose a password of at least 8 characters in length,
containing a mixture of alphabetic and numeric characters.

Please enter the admin password:
Re-type password for verification:
.
.
.
    initializing the administrative domain
Error: can't connect to local observiced - error opening single sign on wallet
    WARNING: administrative domain initialization failed (1) -- see the
             message above.
    generating links for admin installation with Web server
.
.
.
NOTE: The Oracle Secure Backup device driver has been successfully installed.
```

```
Is ella connected to any tape libraries that you'd like to use with
Oracle Secure Backup [no]? yes
```

4. If the administrative server is also a media server, then specify the SCSI information for the attached tape devices. The following example configures `ella` as an administrative server and specifies SCSI information for an attached tape library and tape drive:

```
How many Oracle Secure Backup tape libraries are attached to ella [1]?

Please describe each tape library by answering the following questions.

    Oracle Secure Backup logical unit number [0]:
    SCSI bus name-instance [glm1]:
    SCSI target ID [3]: 1
    SCSI lun 0-7 [0]:

Is the information you entered correct [yes]?

Is ella connected to any tape drives that you'd like to use with
Oracle Secure Backup [no]? yes

How many Oracle Secure Backup tape drives are attached to ella [1]?

Please describe each tape drive by answering the following questions.

    Oracle Secure Backup logical unit number [0]:
    SCSI bus name-instance [glm1]:
    SCSI target ID [4]: 0
    SCSI lun 0-7 [0]:

Is the information you entered correct [yes]?

- - - - - - - - - - - - - - - - - - - - - - - - - - -

Beginning device driver configuration and device special file creation.

NOTE: table for devlinks...
   type=ddi_pseudo;name=ob;addr=0,0;minor=glm1  obt0
/dev/obt0 created
NOTE: table for devlinks...
   type=ddi_pseudo;name=ob;addr=1,0;minor=glm1  obl0
/dev/obl0 created

- - - - - - - - - - - - - - - - - - - - - - - - - - -

NOTE: You must configure the new devices via the Web interface or via
      the command line using the obtool 'mkdev' command.

- - - - - - - - - - - - - - - - - - - - - - - - - - -

Would you like to install Oracle Secure Backup on any other machine [yes]? no
Installation summary:

   Installation  Host                OS        Driver      OS Move     Reboot
       Mode      Name                Name      Installed?  Required?  Required?

    admin         ella                solaris64 no          no         no
Oracle Secure Backup is now ready for your use.
```

5. Obtain the process ID for `observiced` and then terminate the process. For example:

```
# ps -auwx | grep observiced
root     975  0.4  1.222336 5960 pts/2    S 14:00:36  0:02 observiced -s
# kill -9 975
# ps -auwx | grep observiced
#
```

6. Force a reinitialization of the administrative domain. Note that you need to specify a new password for the `admin` user. For example:

```
# obtool --initnewdomain --force
Please enter a password for the "admin" user.
Password:
Password (again):
```

7. If the administrative server is a media server, then reconfigure your tape devices through the Web tool or `obtool`; otherwise you must add a separate media server to the domain that you can use to restore the data. The following example configures a tape library and tape drive attached to `ella`:

```
ob> lshost
ella            admin,client                      (via OB)   in service
ob> mkdev --type library --attach ella:/dev/obl0 ellalib
Info: added "mediaserver" role to host ella.
ob> mkdev --type tape --library ellalib --dte 1 --uselist all --attach
    ella:/dev/obt0 ellatape
ob> lshost
ella            admin,mediaserver,client          (via OB)   in service
```

8. Force an inventory of the tape library and then list the volumes. For example:

```
ob> inventory --drive ellatape --force
ob> lsvol -L ellalib
Inventory of library ellalib:
    in    1:             occupied
    in    2:             occupied
    in    3:             occupied
    in    4:             occupied
    in    5:             occupied
    in    6:             occupied
    in    8:             occupied
    in    9:             occupied
    in    10:            occupied
    in    dte:           occupied
ob>
```

9. Use the `identifyvol` command to populate the Oracle Secure Backup catalog with metadata about the volumes in the library. If you know that the volumes in the library do not contain a backup of the `admin` directory, then load the disaster restore volume that you store offsite (see "Backing Up Critical Data on the Administrative Server" on page 7-24).

   An `identifyvol` command of slots `1` through `9` reveals the following information about the contents of the volumes in the library:

```
ob> identifyvol --import -D ellatape 1-9
Seq  Volume        Volume      Archive    Client     Backup   Archive Create
 #     ID           Tag       File Sect    Host       Level     Date & Time
  1 full-000001                  1    1   jfersten-sun2   0 2006/01/17 07:05:22
  1 full-000001                  2    1   jfersten-sun2   0 2006/01/17 08:41:05
  1 full-000001                  3    1   jfersten-sun2   0 2006/01/17 09:26:13
  1 full-000001                  4    1   jfersten-sun2   0 2006/01/17 09:28:17
  1 full-000001                  5    1   jfersten-sun2   0 2006/01/17 11:02:18
  1 full-000001                  6    1   ella           0 2006/01/20 14:49:54
  1 full-000001                  7    1   ella           0 2006/01/20 15:21:10
  1 full-000001                  8    1   ella           0 2006/01/23 15:16:25
End of volume; the next volume in the volume set is full-000001.

Seq  Volume        Volume      Archive    Client    Backup   Archive Create
 #     ID           Tag       File Sect    Host      Level     Date & Time
  1 VOL000001                    1    1   jfersten-sun2   0 2006/01/17 07:14:23
End of volume set.

Seq  Volume        Volume      Archive    Client    Backup   Archive Create
 #     ID           Tag       File Sect    Host      Level     Date & Time
  5 offsite-000080               2    5   atreyu         0 2003/05/05 10:34:10
  5 offsite-000080               3    1   bigguy         0 2003/05/06 02:10:29
  5 offsite-000080               4    1   ivan           0 2003/05/06 03:39:06
  5 offsite-000080               5    1   pikachu        0 2003/05/06 03:39:14
End of volume set.

Seq  Volume        Volume      Archive    Client    Backup   Archive Create
 #     ID           Tag       File Sect    Host      Level     Date & Time
  1 test1-000002                 1    1   jfersten-sun2   0 2005/12/16 08:57:42
End of volume set.

Seq  Volume        Volume      Archive    Client    Backup   Archive Create
 #     ID           Tag       File Sect    Host      Level     Date & Time
  2 full-000002                  8    2   ella           0 2006/01/23 15:16:25
End of volume set.

Seq  Volume        Volume      Archive    Client    Backup   Archive Create
 #     ID           Tag       File Sect    Host      Level     Date & Time
  2 VOL000002                    5    2   jfersten-sun2   0 2005/11/15 10:16:31
  2 VOL000002                    6    1   fez             0 2005/11/16 09:04:01
  2 VOL000002                    7    1   fez             0 2005/11/16 09:37:52
  2 VOL000002                    8    1   jfersten-sun2   0 2005/11/17 15:16:52
  2 VOL000002                    9    1   fez             0 2005/11/17 15:31:13
  2 VOL000002                   10    1 N nh4flrlab53     0 2005/11/18 13:24:21
End of volume set.

Seq  Volume           Volume      Archive    Client    Backup   Archive Create
 #     ID              Tag       File Sect    Host      Level     Date & Time
  1 ella-OSB-home-000001          1    1   ella           0 2006/01/24 13:05:00
  1 ella-OSB-home-000001          2    1   ella           3 2006/01/24 13:37:55
  1 ella-OSB-home-000001          3    1   ella           0 2006/01/24 15:38:12
  1 ella-OSB-home-000001          4    1   ella           3 2006/01/24 15:39:04
End of volume set.

Seq  Volume           Volume      Archive    Client    Backup   Archive Create
 #     ID              Tag       File Sect    Host      Level     Date & Time
  1 VOL000001                    1    1   jfersten-sun2   0 2005/09/07 07:29:07
  1 VOL000001                    2    1   fez             0 2005/09/07 07:34:47
  1 VOL000001                    3    1   jfersten-sun2   0 2005/09/09 06:17:44
  1 VOL000001                    4    1   jfersten-sun2   0 2005/11/07 15:48:29
  1 VOL000001                    5    1   jfersten-sun2   0 2005/11/15 10:16:31

End of volume; the next volume in the volume set is VOL000001.
Error: this tape is not labeled.
```

The tape from slot 7 has the volume ID prefix ella-OSB-home. This is the tape that contains the needed backups of the admin directory. At this stage, you cannot use obtool or the Web tool to restore files from tape, but you can use obtar to identify and restore the needed files.

10. Load the volume containing the admin directory into the tape drive. For example:

```
ob> loadvol -D ellatape 7
```

11. Use obtar -tvf to display the contents of the volume and obtain the path to your admin directory. The following sample output (which has been truncated) shows that the admin directory is in a nondefault location:

```
# obtar -tvf ellatape -F 1
drwxrwxrwxroot 0 Jan 20 08:48 2006 /export/home/oracle/backup-cdrom060119jwf/
.
.
.
drwxrwxrwxroot 0 Jan 20 08:48 2006
                                /export/home/oracle/backup-cdrom060119jwf/admin
```

12. Use obtar -x to restore the admin directory to a location that does not conflict with existing files or directories. As explained in "Restoring Data to a Different Location" on page 12-9, you can use obtar -x with the -s syntax to specify a new path. The following example restores the admin directory from backup file 1 to /export/home (the backslash indicates line continuation and is not a literal):

```
# obtar -xvf ellatape -F 1 /export/home/oracle/backup-cdrom060119jwf/admin \
  -s,/export/home/oracle/backup-cdrom060119jwf,/export/home,
/export/home/admin/
/export/home/admin/config/
/export/home/admin/config/class/
/export/home/admin/config/class/admin
/export/home/admin/config/class/operator
.
.
.
```

If you have a full backup of this directory as well as incremental backups, then restore the incremental backups to the same directory. The following example restores an incremental backup of the admin directory from backup file 2 to /export/home (the backslash indicates line continuation and is not a literal):

```
# obtar -xvf ellatape -F 2 /export/home/oracle/backup-cdrom060119jwf/admin \
  -s ,/export/home/oracle/backup-cdrom060119jwf,/export/home,
Searching tape for requested file.  Please wait...

/export/home/admin/
/export/home/admin/config/
/export/home/admin/config/class/
/export/home/admin/config/dataset/
.
.
.
```

Also restore the /usr/local/ob directory to the same location. The following example restores an incremental backup of the admin directory from backup file 2 to /export/home:

```
# obtar -xvf ellatape -F 2 /usr/etc/ob -s ,/usr/etc,/export/home,
Searching tape for requested file.  Please wait...
```

```
/export/home/ob/
/export/home/ob/.hostid
/export/home/ob/wallet/
/export/home/ob/wallet/b64certificate.txt
/export/home/ob/wallet/cwallet.sso
.
.
.
```

13. Use the ps command to obtain the process IDs for the Oracle Secure Backup daemons (see "Daemons and Services" on page 2-27) and then terminate them. For example:

```
# ps -awux | grep ob
root      2041  0.1  1.322720 6368 pts/2    S 14:19:33  0:34 observiced -s
.
.
.
# kill -9 2014 2043 2062 2063 2064 2065 2066 2067 2100 2197
# ps -awux | grep ob
#
```

14. Move the admin directory in the Oracle Secure Backup home to a new location and then move the restored admin directory to the Oracle Secure Backup home. For example:

```
# pwd
/export/home/oracle/backup
# mv admin admin.orig
# mv /export/home/admin .
```

Follow the same procedure for the /usr/etc/ob directory:

```
# mv /usr/etc/ob /usr/etc/ob.orig
# mv /export/home/ob /usr/etc/ob
```

15. Restart observiced as follows:

```
# /etc/observiced
```

Your environment is now restored to the point of your last backup of the admin directory. You can use obtool or the Web tool to review your administrative domain configuration.

Part IV

Managing Operations

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

This part contains the following chapters:

9 Managing Devices and Media

This chapter explains how to manage tapes and tape devices with Oracle Secure Backup. This chapter contains the following topics:

- Managing Tape Drives
- Managing Tape Libraries
- Managing Device Reservations

Managing Tape Drives

This section explains how to mount and unmount volumes in a tape drive. This section contains the following topics:

- About Volume Mount Modes
- Displaying the Drives Page
- Mounting a Volume in a Tape Drive
- Unmounting a Volume from a Tape Drive

About Volume Mount Modes

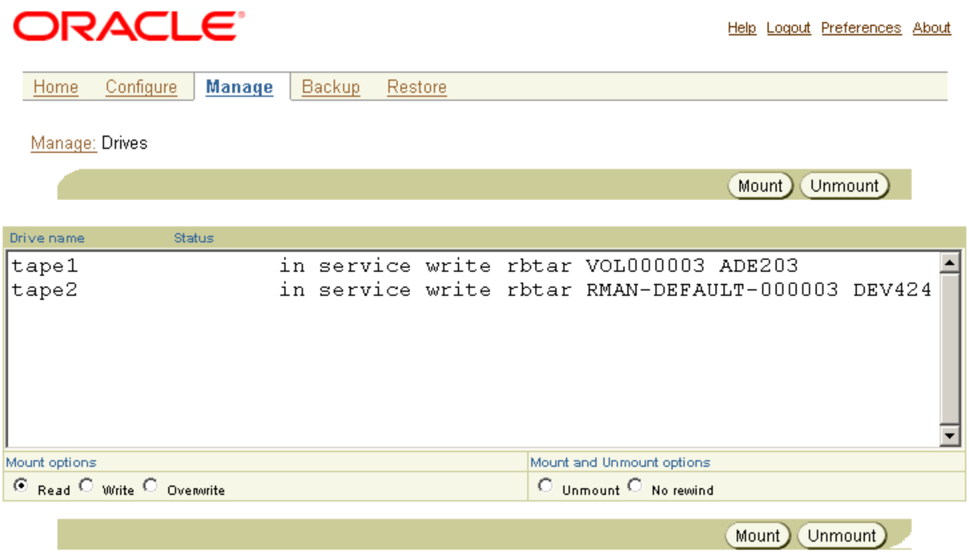
A volume is a single unit of media, such as 8mm tape. The mount mode indicates the way in which Oracle Secure Backup can use a volume physically loaded into a tape drive. Valid mount mode values are as follows:

- Read-Only
- Write/Append
- Overwrite
- Not mounted

Displaying the Drives Page

In the Manage page, click **Drives** to display the page shown in Figure 9–1. This page lists all dataset files and directories. You can use this page to mount and unmount volumes.

Figure 9–1 Drives Page



```
tape1               in service write rbtar VOL000003 ADE203
tape2               in service write rbtar RMAN-DEFAULT-000003 DEV424
```

Mount options
● Read ○ Write ○ Overwrite

Mount and Unmount options
○ Unmount ○ No rewind

See Also: *Oracle Secure Backup Reference* to learn about the `mountdev` and `unmountdev` commands in `obtool`

Mounting a Volume in a Tape Drive

To mount a volume in a tape drive:

1. In the Drives page, select a drive from the main box.

   The Web tool displays the names all drives that are attached to one or more media servers. A drive can have one of the following status values:

   – **in service**

     This value indicates that the drive is logically available to Oracle Secure Backup.

   – **not in service**

     This value indicates that the drive is not logically available to Oracle Secure Backup.

   – **unmounted**

     This value indicates that the drive is unmounted.

   – **mounted**

     This value indicates that the drive is mounted.

2. 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 tells 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 the volume.

   - **Overwrite**

     Specify this option to automatically mount a volume on the 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, you are granting permission to overwrite an unexpired volume. An unexpired volume is not eligible to be overwritten according to its expiration policy (see "Volume Expiration Policies" on page 2-24).

     Caution: Use this mode only in situations that warrant or require overwriting unexpired volumes.

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

   - **Unmount**

     Select this option to performs an unmount operation on the selected 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.

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

   The Web tool displays the drive name and volume ID in the status area.

   > **See Also:** "Backup Image and Volume Labels" on page 2-20 for details about volumes and volume IDs

Unmounting a Volume from a Tape Drive

To unmount a volume in a tape drive:

1. In the Drives page, select a drive from the main box.

   The Web tool displays the names all drives that are attached to one or more media servers. A drive can have one of the following status values:

   – **in service**

     This value indicates that the drive is logically available to Oracle Secure Backup.

   – **not in service**

     This value indicates that the drive is not logically available to Oracle Secure Backup.

   – **unmounted**

     This value indicates that the drive is unmounted.

   – **mounted**

     This value indicates that the drive is mounted.

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

   - **Unmount**

     Select this option to performs an unmount operation on the selected 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.

3. 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.

Managing Tape Libraries

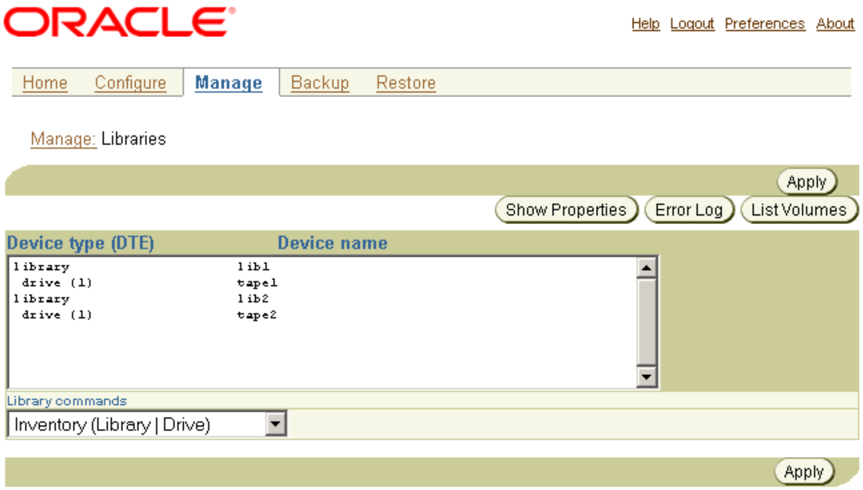
This section explains how to view and control tape libraries. This section contains the following topics:

- Displaying the Libraries Page
- Executing Library Commands
- Displaying Library Properties
- Displaying Tape Drive Properties
- Displaying Library Volumes

Displaying the Libraries Page

In the Manage page, click **Libraries** to display the page shown in Figure 9–2. This page lists the tape libraries in the administrative domain. You can perform all tape library configuration tasks in this page or in pages to which it provides links.

Figure 9–2 Libraries Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Manage: Libraries
Apply
Show Properties
Error Log
List Volumes
Library commands
Inventory (Library | Drive)
Apply

Device type (DTE)	Device name
library	lib1
drive (1)	tape1
library	lib2
drive (1)	tape2

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

Executing Library Commands

To manage a library or tape drive:

1. In the main text box, select a library or tape drive.
2. From the **Library commands** pull-down menu, choose one of the following commands shown in Table 9–1. 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 library or a drive. For those commands that apply to libraries, however, you can optionally specify a drive, because specification of a drive always implies the library in which it resides.

Table 9–1 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 9-6	`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 9-7	`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 9-7	`exportvol`

Table 9–1 (Cont.) Library Commands

Menu Command	Applies to	Description	Section	obtool Command
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 9-8	`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 volume you are extracting.	"Extracting a Volume" on page 9-9	`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 the location from which you are moving a tape and the location to which you are moving it.	"Moving a Volume" on page 9-9	`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 9-10	`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 9-10	`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 9-10	`identifyvol`
Load Volume	Drive	Moves a volume from the indicated storage element to the selected drive.	"Loading a Volume" on page 9-10	`loadvol`
Unload Volume	Drive	Moves a tape from the selected drive to the storage element you specify.	"Unloading a Volume" on page 9-11	`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 9-12	`labelvol`
Unlabel Volume	Drive	Loads selected volumes and physically removes their Oracle Secure Backup volume labels and backup data.	"Unlabeling a Volume" on page 9-12	`unlabelvol`
Clean	Drive	Requests that a cleaning be performed on the selected tape drive.	"Cleaning a Tape Drive" on page 9-12	`clean`
Borrow	Drive	Borrows the selected drive.	"Borrowing a Tape Drive" on page 9-13	`borrowdev`
Return	Drive	Returns a currently borrowed drive.	"Returning a Tape Drive" on page 9-13	`returndev`
Reuse Volume	Drive	Loads selected volumes and relabels them so as to be reusable.	"Reusing a Volume" on page 9-13	`reusevol`

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

   The 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 library inventory and enables you to force a physical inventory of the selected library.

To update the inventory:

1. In the Libraries page, select a library or drive in the main text box.

2. From the **Library commands** list, select **Inventory (Library | Drive)**.
3. Optionally, check the **Force** box to force an inventory. Instead of reading from its cache, the library updates the inventory by physically scanning all library elements.
4. Click **Apply**, **OK**, or **Cancel**.

Importing a Volume

This command moves one or more volumes from the import/export mechanism of a library to storage elements.

To import a volume:

1. In the Libraries page, select a library or drive in the main text box.
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 9-10. 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** box, 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 library.

To export a volume:

1. In the Libraries page, select a library or drive in the main text box.
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** box, enter the volume IDs or barcodes of the volumes you want to export.
   - In the **Storage element range** box, 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 library and specifies the properties of the inserted volumes.

To insert a volume:

1. In the Libraries page, select a library or drive in the main text box.
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**

     Select this option and enter the volume ID of the tape.
   - **Barcode**

     Select this option and 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** box, 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 library. You specify the source of volumes you are extracting.

To extract a volume:

1. In the Libraries page, select a library or drive in the main text box.
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 range of storage elements containing the extracted volumes. In the text box, 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 library or drive in the main text box.
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**

       Select this option and enter the volume ID of the tape to be moved.
     - **Barcode**

       Select this option and 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 box, enter a storage element number. For example, enter **1**.

5. In the **Element spec** box, 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 library.

To open the import/export door:

1. In the Libraries page, select a library in the main text box.
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 the library.

To close the import/export door:

1. In the Libraries page, select a library in the main text box.
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 their volume labels, and returns the volumes to their original storage elements. You can use this command to verify the state of occupied library slots and update the library inventory accordingly.

To identify a volume:

1. In the Libraries page, select a drive in the main text box.
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 drive to be used in the volume identification.
5. Check the **Import** box 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** box, enter the range of storage elements 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 drive:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Load Volume (Drive)**.

3. In the **Drive** list, select the 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**

       Select this option and enter the volume ID of the tape to be loaded.

     – **Barcode**

       Select this option and 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 box, enter a storage element number. For example, enter **1**.
6. From the **Load volume options** groups, optionally check 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 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 drive.
7. Click **Apply**, **OK**, or **Cancel**.

Unloading a Volume

This command moves a tape from the selected drive to the element you specify.

To unload a volume:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Unload Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the drive that contains the loaded volume.
5. In the **Source element address** box, 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 new volume labels to these volumes. This command erases all existing data on the selected volumes.

To label a volume:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Label Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the drive into which the volume should be loaded.
5. Optionally, check the **Force** box to force the labeling of a volume. Checking 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. Check the **Barcode** box and enter the barcode for the volume.
7. Enter an element range in the **Storage element range** box. 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 drive in the main text box.
2. From the **Library commands** list, select **Unlabel Volume (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the 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** box, enter an 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 drive:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Clean (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the drive into which the cleaning tape should be loaded.

5. Click **Force** to force the drive to be cleaned. If there is a tape loaded in the drive, then selecting this option unloads the tape, loads the cleaning tape, cleans the drive, and then reloads the tape that was originally in the drive.
6. In the **Source element address** box, 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 drive. You need to belong to a user class having the `manage devices and change device state` right.

You can borrow a drive if a backup or restore is requesting assistance. Borrowing the drive temporarily overrides the device reservation made by the requesting job and enables you to execute arbitrary library or drive commands. Afterwards, you can return the drive and resume the job.

To borrow a drive:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Borrow (Drive)**.
3. In the **Drive** list, select the drive to be borrowed.
4. Click **Apply**, **OK**, or **Cancel**.

Returning a Tape Drive

After a drive has been borrowed, you can return the drive.

To return a borrow drive:

1. In the Libraries page, select a drive in the main text box.
2. From the **Library commands** list, select **Return Device (Drive)**.
3. In the **Drive** list, select the drive to be returned.
4. Click **Apply**, **OK**, or **Cancel**.

Reusing a Volume

This command loads selected volumes and deletes their backup images. 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 the 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 drive in the main text box.
2. From the **Library commands** list, select **Reuse (Drive)**.
3. Click **Apply** to accept your selection.
4. In the **Drive** list, select the drive to be returned.
5. In the **Storage element range** box, enter a range of elements containing the volumes to be reused.
6. Click **Apply**, **OK**, or **Cancel**.

Displaying Library Properties

This section explains how to display properties for a library.

To view library properties:

1. In the Libraries page, select a library in the main text box.
2. Click **Show Properties**.

   The Web tool displays a page with the properties for the 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 main text box.
2. Click **Show Properties**.

   The Web tool displays a page with the properties for the drive you selected.
3. Click **Close** to return to the Libraries page.

Displaying Library Volumes

This section explains how to display the volumes currently contained in a library.

To display library volumes:

1. In the Libraries page, select a library in the main text box.
2. Click **List Volumes**.

   The Web tool displays a page with the volumes for the 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 libraries and tape drives.

To display error messages:

1. In the Libraries page, select a library or drive in the main text box.
2. Select a library or drive from the **Library Management** box.
3. Click **Error Log**.

   The Web tool displays a page with error messages displays for the library or drive you selected.
4. Optionally, check **Since (date)** and specify a date range for specific error messages.
5. Optionally, check **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

This section explains how to manage device reservations. This section contains the following topics:

- About Device Reservations
- Displaying the Device Reservations Page
- Reserving Devices
- Unreserving Devices
- Displaying the Error Log

About Device Reservations

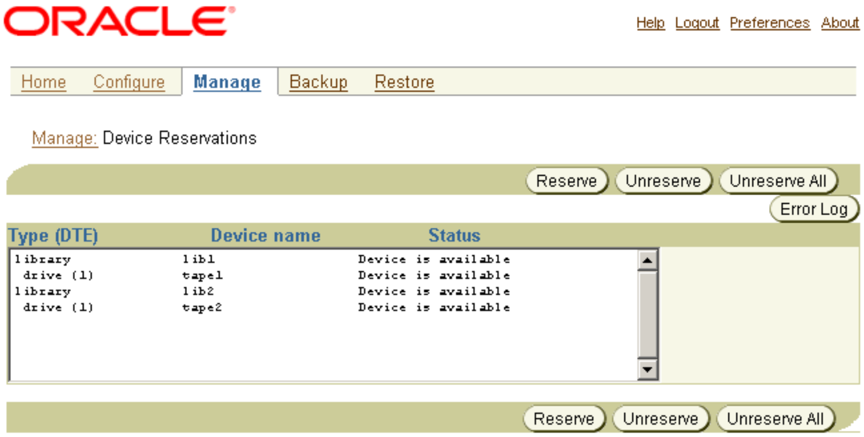
In the normal course of operations, Oracle Secure Backup temporarily assigns exclusive use of shared resources to its processes and jobs. It does so using a built-in resource reservation system managed by the administrative server's service daemon.

You may encounter certain situations in which you desire exclusive and explicit use of a device. When such cases arise, you may direct Oracle Secure Backup to reserve a 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 device.

Displaying the Device Reservations Page

In the Manage page, click **Device Reservations** to display the page shown in Figure 9–3. This page lists devices that you can reserve. You can perform all device reservation tasks in this page or in pages to which it provides links.

Figure 9–3 Device Reservations Page



Type (DTE)	Device name	Status
library	lib1	Device is available
drive (1)	tape1	Device is available
library	lib2	Device is available
drive (1)	tape2	Device is available

> **See Also:** *Oracle Secure Backup Reference* to learn about the `resdev` and `unresdev` commands in `obtool`

Reserving Devices

This section explains how to reserve a device for your exclusive use. You can also unreserve a specific device or unreserve all of your devices at once.

To reserve a device:

1. In the Device Reservations page, select a library or tape drive in the main text box.
2. Click **Reserve**.

   The device is now reserved solely for your use. The reservation persists until you end your Web tool session or unreserve the device.

Unreserving Devices

This section explains how to unreserve a device that has been previously reserved. You can unreserve a specific device or unreserve all of your devices at once.

To reserve a device:

1. In the Device Reservations page, select a library or tape drive in the main text box.
2. Click **Unreserve** to reserve only the specified device or **Unreserve all** to unreserve all reserved devices.

   The devices reserved in this instance of the Web tool are now available for other activities.

Displaying the Error Log

This section explains how you can display errors for a library or drive.

To display the error log for a device:

1. In the Device Reservations page, select a library or tape drive in the main text box.
2. Click **Error Log**.

   The Web tool displays a page with error messages for the device that you selected.
3. Optionally, click **Since (date)** and specify a date range for specific error messages.
4. Optionally, click **Read device dump file** and enter the filename and path of the file you want to read.
5. 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 Devices page.

10

Performing Maintenance

This chapter describes how to perform maintenance tasks with Oracle Secure Backup. This chapter contains the following topics:

- Managing Backup and Restore Jobs
- Browsing Volumes
- Managing Backup Images
- Managing Backup Sections
- Managing Checkpoints
- Managing Daemons

Managing Backup and Restore Jobs

As explained in "Jobs and Requests" on page 2-11, 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 the following topics:

- Displaying the Jobs Page
- Displaying Jobs
- Displaying Job Properties
- Displaying Job Transcripts
- Removing a Job
- Running a Job
- Canceling a Job

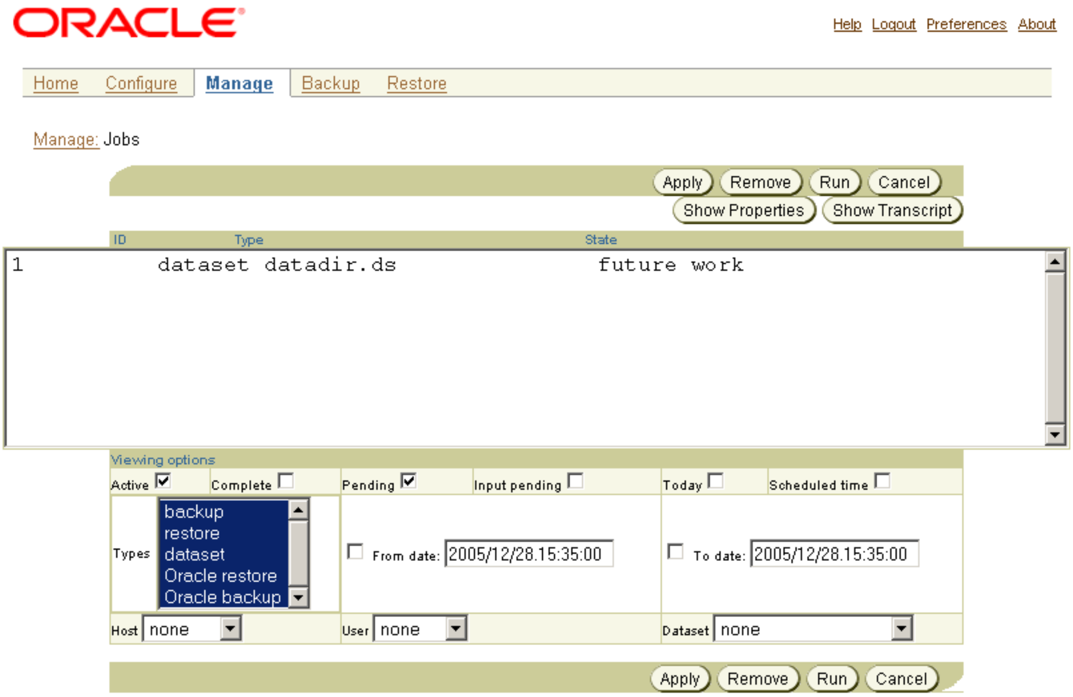
Displaying the Jobs Page

In the Manage page, click **Jobs** to display the page shown in Figure 10–1. 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 10–1 Jobs Page


ORACLE
Help Logout Preferences About
Home Configure Manage Backup Restore
Manage: Jobs
Apply Remove Run Cancel
Show Properties Show Transcript
Viewing options
Apply Remove Run Cancel

```
ID        Type                      State
1         dataset datadir.ds        future work
```

Active ☑ Complete □ Pending ☑ Input pending □ Today □ Scheduled time □

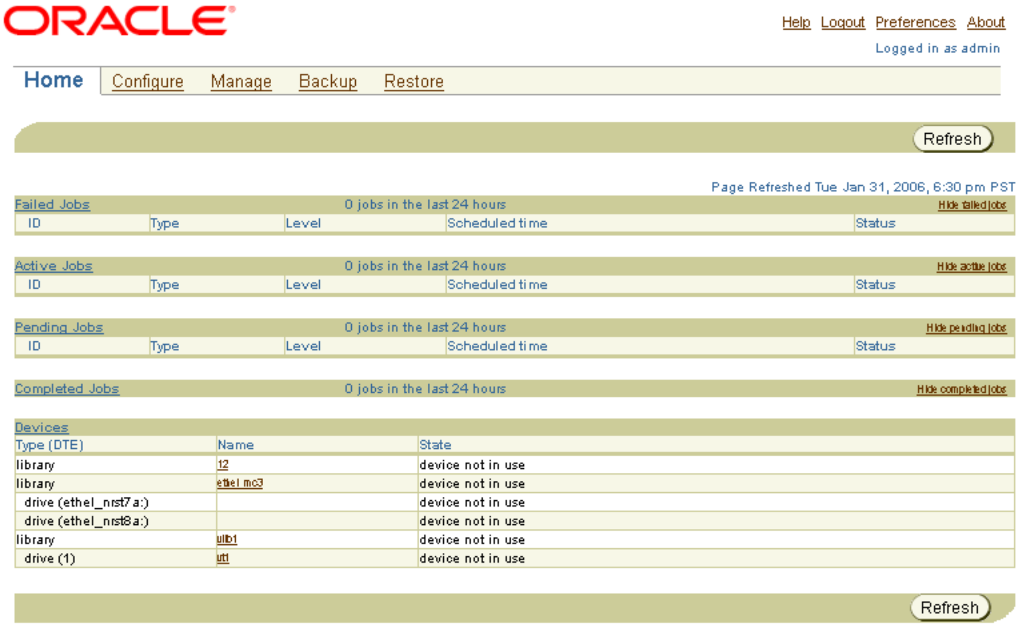
Types: backup, restore, dataset, Oracle restore, Oracle backup

□ From date: 2005/12/28.15:35:00 □ To date: 2005/12/28.15:35:00

Host: none User: none Dataset: none

Note that you can also monitor and manage jobs from the Oracle Secure Backup home page, which is shown in Figure 10–2. The home page contains sections that show failed, active, pending, and completed jobs.

Figure 10–2 Home Page



Page Refreshed Tue Jan 31, 2006, 6:30 pm PST

Failed Jobs — 0 jobs in the last 24 hours

ID	Type	Level	Scheduled time	Status

Active Jobs — 0 jobs in the last 24 hours

ID	Type	Level	Scheduled time	Status

Pending Jobs — 0 jobs in the last 24 hours

ID	Type	Level	Scheduled time	Status

Completed Jobs — 0 jobs in the last 24 hours

Devices

Type (DTE)	Name	State
library	12	device not in use
library	ethel mc3	device not in use
drive (ethel_nrst7a:)		device not in use
drive (ethel_nrst8a:)		device not in use
library	ulib1	device not in use
drive (1)	ut1	device not in use

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 backup jobs that are 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 backup jobs that are 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 a 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 Backups" on page 2-2 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.

To display a job transcript:

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

   The Web tool displays a page with the transcript.
3. Scroll down the page to view more information.

   At the end of the page, you can modify the transcript viewing criteria.
4. In the **Level** list, optionally select a message level.

Oracle Secure Backup tags each message it writes to a transcript with a severity level. These levels range from 0 to 9. The severity level describes the importance of the message.

When displaying a transcript, you can direct Oracle Secure Backup to display only messages of a certain severity level or higher. Its default level is 4 (Request), meaning normal messages produced by Oracle Secure Backup. Refer to the `catxcr` command description in *Oracle Secure Backup Reference* for more information.

5. Optionally, check **Suppress input** to suppress input requests. When a request for input is recognized, Oracle Secure Backup prompts for a response. Specifying this option suppresses this action.
6. Optionally, check **Show line numbers** to prefix each line with its message number.
7. Optionally, select one of the following options to control the transcript display:
   - **Start at line**

     Select this option and enter a number in which to you want the transcript view to start. For example, if you enter '10,' 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.
8. In the **Page refresh (in seconds)** box, optionally enter a number of seconds. The default is 60 seconds.
9. Choose one of the following:
   - Click **Apply** to apply your selections.
   - Click **Close** to close the page.

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 10-6, 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 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 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.

You can direct Oracle Secure Backup to start a job:

- Immediately
- In an order different from that chosen by the scheduler
- On a specific device or a 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 device on which to run the job. If the job was restricted to another device or set of devices, then your selection here overrides that restriction. Note that you if you select **Now** in the next step, you must choose a device.
4. Optionally select one of the following options:
   - **Now**

     Select this option to run the job immediately. If the preceding 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, 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

As explained in "Backup Images and Media" on page 2-18, volumes are the media on which backup data is stored. This section describes how to display information about volumes.

This section includes the following topics:

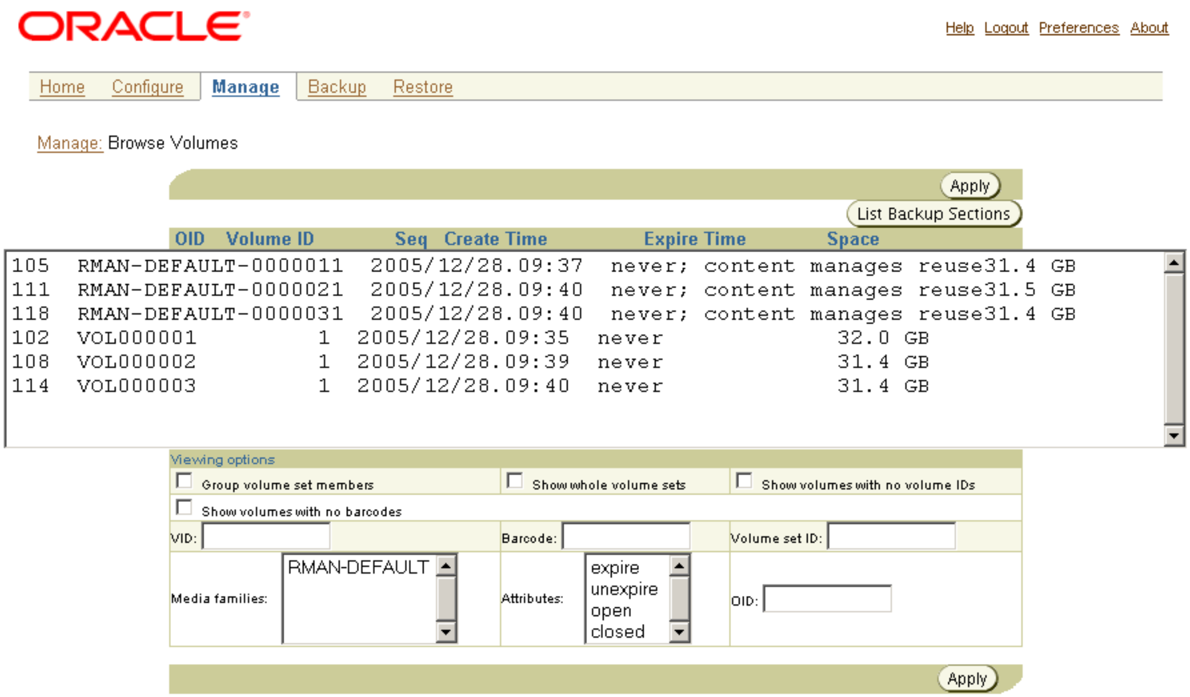
- Displaying the Browse Volumes Page
- Displaying Volumes
- Displaying Backup Sections

Displaying the Browse Volumes Page

In the Manage page, click **Volumes** to display the page shown in Figure 10–3. This page lists all volumes in the volume catalog.

> **Note:** To list volumes in a specified library, navigate to the Libraries page described in "Displaying the Libraries Page" on page 9-5 and click **List Volumes**.

Figure 10–3 Browse Volumes Page



Manage: Browse Volumes

```
OID   Volume ID            Seq  Create Time       Expire Time        Space
105  RMAN-DEFAULT-0000011  2005/12/28.09:37  never; content manages reuse31.4 GB
111  RMAN-DEFAULT-0000021  2005/12/28.09:40  never; content manages reuse31.5 GB
118  RMAN-DEFAULT-0000031  2005/12/28.09:40  never; content manages reuse31.4 GB
102  VOL000001          1  2005/12/28.09:35  never                     32.0 GB
108  VOL000002          1  2005/12/28.09:39  never                     31.4 GB
114  VOL000003          1  2005/12/28.09:40  never                     31.4 GB
```

☐ Group volume set members ☐ Show whole volume sets ☐ Show volumes with no volume IDs

☐ Show volumes with no barcodes

VID: Barcode: Volume set ID:

Media families: RMAN-DEFAULT

Attributes: expire, unexpire, open, closed

OID:

> **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. Refer to *Oracle Secure Backup Reference* to learn about the volume attributes.

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 2-24)

     – **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 information about backup sections 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 ListSections 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

As explained in "Backup Sets and Backup Images" on page 2-10, 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.

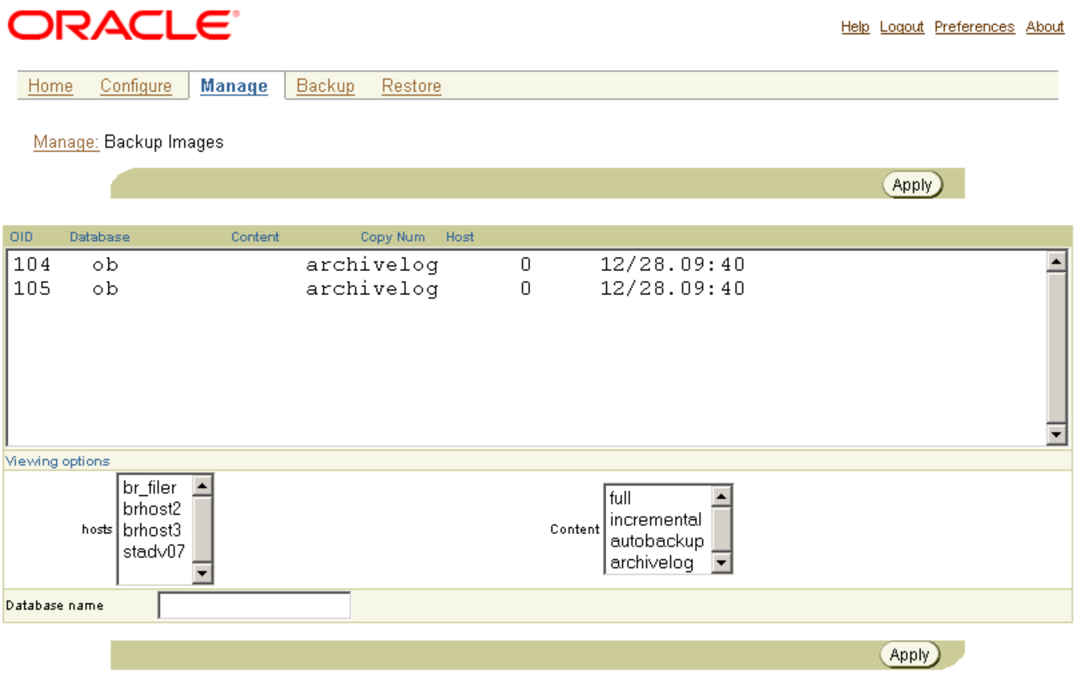
This section includes the following topics:

- 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 10–4. This page lists the backup images generated by RMAN.

Figure 10–4 Backup Images Page



```
OID  Database        Content      Copy Num  Host
104   ob            archivelog      0      12/28.09:40
105   ob            archivelog      0      12/28.09:40
```

> **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 all backup images 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

As explained in "Backup Images and Sections" on page 2-19, a backup section is the part of a backup image that fits on one tape. If a single backup image spans multiple tapes, the portion of the image on each tape is a separate section.

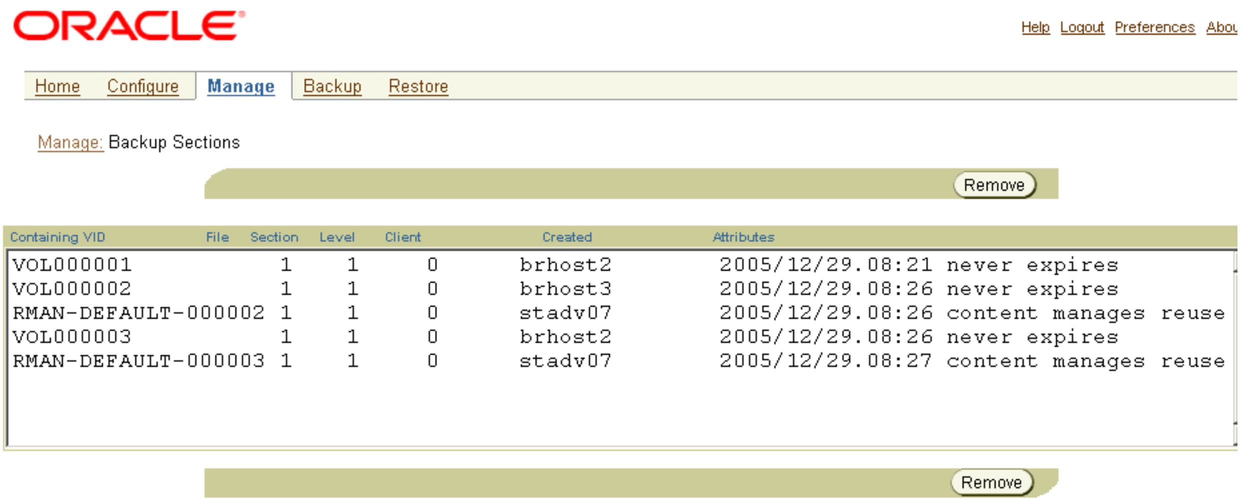
This section includes the following topics:

- 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 10–5. This page lists the backup sections recorded in the catalog.

Figure 10–5 Backup Sections Page



```
Containing VID      File  Section  Level  Client     Created          Attributes
VOL000001            1     1     0     brhost2     2005/12/29.08:21 never expires
VOL000002            1     1     0     brhost3     2005/12/29.08:26 never expires
RMAN-DEFAULT-000002  1     1     0     stadv07     2005/12/29.08:26 content manages reuse
VOL000003            1     1     0     brhost2     2005/12/29.08:26 never expires
RMAN-DEFAULT-000003  1     1     0     stadv07     2005/12/29.08:27 content manages reuse
```

> **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 content-managed volumes.

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.

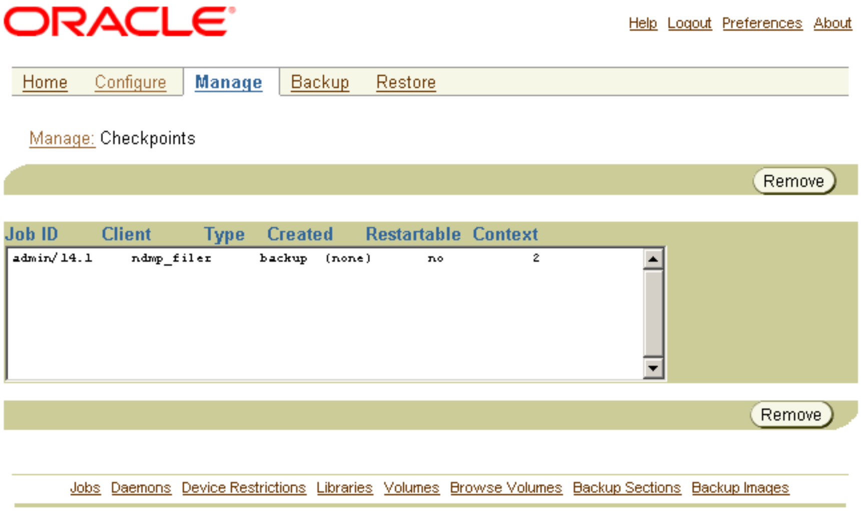
Managing Checkpoints

As explained in "Restartable Backups" on page 2-6, you can restart backups of some filers 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 10–6. This page displays all checkpoints for hosts in the administrative domain.

Figure 10–6 Manage Checkpoints Page



Job ID	Client	Type	Created	Restartable	Context
admin/14.1	ndmp_filer	backup	(none)	no	2

> **See Also:** *Oracle Secure Backup Reference* to learn about the checkpoint commands in `obtool`

Removing a Checkpoint

Although normally not required, you can manually remove checkpoint data for any job. This action has the effect of reclaiming disk space as follows:

- On the administrative server immediately
- On the client at the start of the next backup job, or within 24 hours, whichever occurs first

> **Note:** If you remove a checkpoint for an incomplete backup job, then the job restarts from its beginning if it fails before completing.

To remove a checkpoint:

1. 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

As explained in "Daemons and Services" on page 2-27, 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.

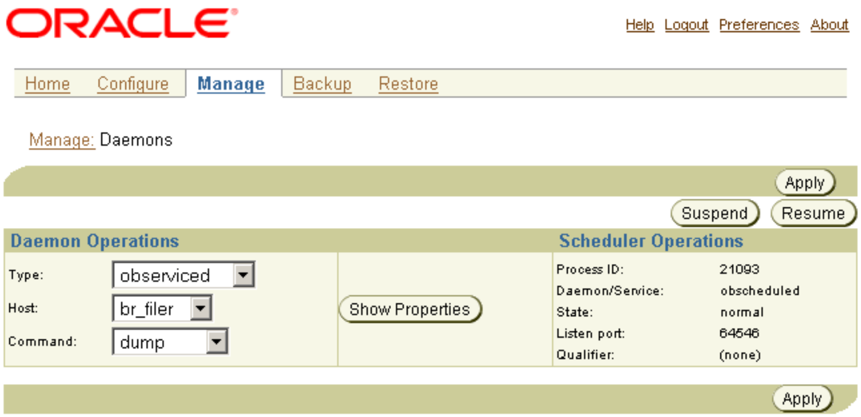
This section contains the following topics:

- 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 10–7. This page enables you to manage the Oracle Secure Backup daemons.

Figure 10–7 Daemons Page



Type: observiced
Host: br_filer
Command: dump

Process ID:	21093
Daemon/Service:	obscheduled
State:	normal
Listen port:	64546
Qualifier:	(none)

> **See Also:** *Oracle Secure Backup Reference* to learn about the daemon commands in `obtool`

Performing Daemon Operations

Oracle Secure Backup daemons respond to a common set of control commands. Sending these commands is rarely needed and is considered advanced usage.

To send a command to a daemon:

1. In the **Type** list, select the daemon that you want to control. Refer to "Types of Daemons" on page 2-28 for a description of the daemons.
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.

To view daemon properties:

1. In the **Type** list, select the daemon that you want to control. Refer to "Types of Daemons" on page 2-28 for a description of the daemons.
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 library that the daemon is servicing. For `obixd`, this is the name of the client host 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 V

Advanced Topics

This part contains the following chapters:

11

Configuring Security: Advanced Topics

This chapter provides a detailed explanation of security in an Oracle Secure Backup domain and how to configure it. This chapter contains the following topics:

- Planning Security for an Administrative Domain
- Configuring Security for the Administrative Domain
- Managing Certificates with obcm

> **See Also:** "Network Backup Security" on page 2-31 for an overview of security architecture of an administrative domain

Planning Security for an Administrative Domain

If security is of primary concern in your environment, then you may find it helpful to plan for the security implementation in the following stages:

1. Identifying Principals and Assets
2. Identifying Your Backup Environment Type
3. Choosing Secure Hosts for the Administrative and Media Servers
4. Determining the Distribution Method of Host Identity Certificates

After completing these stages, you can proceed to the implementation phase as described in "Configuring Security for the Administrative Domain" on page 11-7.

Identifying Principals and Assets

The first step in planning security for an administrative domain is determining the assets and principals associated with the domain.

The assets of the domain include the following:

- The database and file system data requiring backup
- Metadata about the database and file system data
- Passwords
- Identities
- Hosts and storage devices

Principals are users who either have access to the assets associated with the administrative domain or to the network that forms the superset of the domain. Principals include the following users:

- Backup administrators

  These Oracle Secure Backup users have administrative rights in the domain, access to the tapes containing backup data, and the rights required to perform backup and restore operations.

- Database administrators

  Each database administrator has complete access to his or her own database.

- Hosts owners

  Each host owner has complete access to the file system of this host.

- System administrators

  These users may have access to the corporate network and to the hosts in the administrative domain (although not necessarily root access).

- Onlookers

  These users do not fall into any of the preceding categories of principals, but can access the network that forms the superset of the Oracle Secure Backup domain. Onlookers may own a host outside of the domain.

Principals stand in a variety of relationships to the assets. These relationships partially determine the level of security in the Oracle Secure Backup administrative domain.

One way to view the security level of the domain is in terms of which principals have access to assets that they do not own. In the highest level of security, the only principal with access to an asset is the owner. For example, only the owner of a client host has the ability to read or modify data from this host. In a medium level of security, the asset owner and the administrator of the domain both have access to the asset. In the lowest level of security, any principal can access any asset in the domain.

Identifying Your Backup Environment Type

After you have identified the assets and principals involved in your administrative domain, you can characterize the type of environment in which you are deploying the domain. The type of environment partially determines which security model to use.

The following criteria partially distinguish types of network environments:

- Scale

  The number of principals and assets associated with a domain plays an important role in domain security. A network that includes 1000 hosts and 2000 users has more points of entry for an attacker than a network of 5 hosts and 2 users.

- Sensitivity of data

  The sensitivity of data is measured by how dangerous it would be for the data to be accessed by a malicious user. For example, the home directory on a rank-and-file corporate employee's host is presumably less sensitive than a credit card company's subscriber data.

- Isolation of communication medium

  The security of a network is contingent on the accessibility of network communications among hosts and devices in the domain. A private, corporate data center is more isolated in this sense than an entire corporate network.

The following sections describe types of network environments in which Oracle Secure Backup administrative domains are typically deployed. The sections also describe the security model typical for each environment.

Single System

The most basic administrative domain consists of an administrative server, media server, and client. As shown in Figure 1–3, "Administrative Domain with One Host", a single host can assume all three roles.

This type of environment has the following characteristics:

- Scale

  The number of hosts, devices, and users in the administrative domain is small.

- Sensitivity of data

  The data in this scenario is assumed to be on the low end of the sensitivity range. For example, the domain may consist of two servers used to host personal Web sites within a corporate network.

- Isolation of communication medium

  This type of network is isolated from the wider network.

Principals and Assets The assets include only a few hosts and a tape device. The users may include only the backup administrator and system administrator, which could conceivably be the same person. The backup administrator is the administrative user of the Oracle Secure Backup domain and is in charge of backups on the domain. The system administrator manages the hosts, devices, and networks used by the domain.

Security Model In this scenario, the domain is fairly secure because it has only a few, isolated hosts accessed by a few trusted users. Thus, the administrator of the domain would probably not make security administration a primary concern. In this scenario, the backup administrator could reasonably expect almost no overhead for maintaining and administering security in the Oracle Secure Backup domain.

Data Center

This administrative domain is of medium size and is deployed in a secure environment such as a data center.

This type of environment has the following characteristics:

- Scale

  The number of hosts, devices, and users in the administrative domain is much larger than in the single system scenario, although still a small subset of the network at large.

- Sensitivity of data

  The data in this scenario is assumed to be on the high end of the sensitivity range. An example could be a network of hosts used to store confidential employee data.

- Isolation of communication medium

  Network backups are conducted on a separate, secure, dedicated network.

Principals and Assets The assets are physically secure machines in a dedicated network. The administrative domain could potentially include a dozen media servers that service the backups of a few hundred databases and file systems.

Principals include the following users:

- The backup administrator accesses the domain as an Oracle Secure Backup administrative user.
- The system administrator administers the machines, devices, and the network.
- Database administrators can access their own databases and possibly have physical access to their database machines.
- Host administrators can access their file systems and possibly have physical access to their machines.

Security Model As with the single system scenario, the administrative domain exists in a network environment that is already secure. Administrators secure hosts, drives, and tapes by external means. Active attacks by a hacker are not likely. Thus, administrators assume that security maintenance and administration for the domain requires almost no overhead. Backup and system administrators are concerned with performance, that is, whether Oracle Secure Backup moves data between hosts efficiently.

Corporate Network

In this environment, one or more administrative domains, multiple media servers, and numerous client hosts exist in a corporate network.

This type of environment has the following characteristics:

- Scale

  The number of hosts, devices, and users in the administrative domains is extremely large.

- Sensitivity of data

  Data backed up includes both highly sensitive data such as HR information as well as less sensitive data such as the home directories of low-level employees.

- Isolation of communication medium

  Backups probably occur on the same corporate network used for email, Internet access, and so on, and are protected by a firewall from the broader Internet.

Principals and Assets The assets include basically every piece of data and every computer in the corporation. Each administrative domain—and there may be several—could have multiple users. Some host owners could have their own Oracle Secure Backup account to initiate a restore of their host's file system or database.

Security Model The security requirements for this backup environment are different from the single system and data center examples. Given the scope and distribution of the product, compromised client hosts are highly likely. For example, someone could steal a laptop used on a business trip. Malicious employees could illicitly log in to computers or run `tcpdump` or similar utilities to listen to network traffic.

The compromise of a client host should not lead to the disablement or compromise of an entire administrative domain. A malicious user on a compromised machine should not be able to access data that was backed up by other users on other hosts. This user should also not be able to affect normal operation of the other hosts in the administrative domain.

Security administration and performance overhead is expected. Owners of sensitive assets should encrypt their backups so that physical access to backup media does not reveal the backup contents. These users should perform encryption and decryption on the client host itself so that sensitive data never leaves the host in unencrypted form.

> **Note:** The RMAN Backup Encryption feature provides encryption for database backups on disk or tape. Oracle Secure Backup does not encrypt file system backup data stored on tape.

Choosing Secure Hosts for the Administrative and Media Servers

Your primary task when configuring security for your domain is providing physical and network security for your hosts and determining which hosts should be the administrative and media servers.

When choosing administrative and media servers, remember that *a host should only be an administrative or media server if it is protected by both physical and network security.* For example, a host in a data center could be a candidate for an administrative server because it presumably belongs to a private, secured network accessible to a few trusted administrators.

Oracle Secure Backup *cannot itself provide physical or network security for any host nor verify whether such security exists*. For example, Oracle Secure Backup cannot stop malicious users from performing the following illicit activities:

- Physically compromising a host

  An attacker who gains physical access to a host can steal or destroy the primary or secondary storage. For example, a thief could break into an office and steal servers and tapes. Encryption can reduce some of the threat to data, but not all. Note that an attacker who gains physical access to the administrative server compromises the entire administrative domain.

- Accessing the operating system of a host

  Suppose an onlooker steals a password by looking at the fingers of the owner of a client host as he types his password. This malicious user could telnet to this host and delete, replace, or copy the data from primary storage. The most secure backup system in the world cannot protect data from attackers if they can access the data in its original location.

- Infiltrating or eavesdropping on the network

  Although backup software can in some instances communicate securely over insecure networks, it cannot always do so. Network security is an important part of a backup system, especially for NDMP-based communications.

- Deliberating misusing an Oracle Secure Backup identity

  If a person with Oracle Secure Backup administrator rights turns bad, he can wreak havoc on the administrative domain. For example, he could overwrite the file system on every host in the domain. No backup software can force a person to behave morally.

Determining the Distribution Method of Host Identity Certificates

After you have analyzed your backup environment and considered how to secure it, you can decide how hosts in the domain obtain their identity certificates. As explained in "Host Authentication and Communication" on page 2-32, Oracle Secure Backup uses SSL to establish a secure and trusted communication channel between domain hosts. Each host has an identity certificate signed by the Certification Authority (CA) that uniquely identifies this host within the domain. The identity certificate is required for authenticated SSL connections.

As explained in "Certification Authority" on page 2-33, the administrative server of the domain is the CA for the administrative domain. After you configure the administrative server, you can create the media servers and clients in the domain. You can create the media servers and clients in either of the following modes:

- automated certificate provisioning mode

  In this case, no manual administration is required. When you configure the hosts, the CA issues identity certificates to the new hosts over the network.

- manual certificate provisioning mode

  In this case, you must manually import the identity certificate for each host into its wallet.

Automated mode is easier to use but is vulnerable to unlikely man-in-the-middle attacks in which an attacker steals the name of a new host right before you invite it to join the domain. This attacker could use the stolen host identity to join the domain illicitly. Manual mode is more difficult to use than automated mode, but is not vulnerable to the same kinds of attacks.

In manual mode, the administrative server does not transmit certificate responses to the new host. Instead, you must carry a copy of the signed identity certificate on physical media to the new host and then use the `obcm` utility to import the certificate into the wallet of the new host. The `obcm` utility verifies that the certificate request in the wallet matches the signed identity certificate. A verification failure indicates that a rogue host likely attempted to masquerade as the new host. You can reissue the `mkhost` command after the rogue host has been eliminated from the network.

When deciding between manual and automated certificate provisioning modes, consider the following question: Is the extra protection provided by manual certificate provisioning mode worth the administrative overhead? The single system and data center environments have isolated network communications; thus, automated mode is probably the better choice. The corporate network is much more vulnerable to the man-in-the-middle attack, so manual mode is a more reasonable option. Nevertheless, the number of hosts in the domains is probably very large, so the administrative overhead is significant.

Configuring Security for the Administrative Domain

This section describes how to configure security for the administrative domain. This section includes the following topics:

- Providing Certificates for Hosts in the Administrative Domain
- Setting the Size for Public and Private Keys
- Enabling and Disabling Encryption for Backup Data in Transit
- Enabling and Disabling SSL for Host Authentication and Communication

Providing Certificates for Hosts in the Administrative Domain

Configuring the domain involves the following tasks:

- Configuring the Administrative Server
- Configuring Media Servers and Clients

Configuring the Administrative Server

If you install Oracle Secure Backup on a host and specify this host as the administrative server, then this server is the CA. Oracle Secure Backup configures the host as the CA automatically as part of the standard installation. You do not need to take additional steps to provide a signing certificate for this server.

> **Note:** You can also initialize the domain by running the `obtool --initnewdomain` command manually.

Oracle Secure Backup automatically performs the following actions:

1. Creates a host object corresponding to the administrative server in the object repository on the administrative server.
2. Creates a wallet to contain the administrative server's certificates. The wallet resides in the directory tree of the Oracle Secure Backup home. Oracle Secure Backup uses the host ID as the wallet password.
3. Creates a request for a signing certificate in the wallet.
4. Creates a signed certificate in response to the request and stores the certificate in the wallet.
5. Creates a request for an identity certificate in the wallet.
6. Creates a signed certificate in response to the request and stores it in the wallet.
7. Creates the obfuscated wallet in the local wallet directory.

The administrative server now has the signing certificate, which it needs to sign the identity certificates for other hosts, and its identity certificate, which it needs to establish authenticated SSL connections with other hosts in the domain.

Configuring Media Servers and Clients

Oracle Secure Backup creates security credentials for a new host when you use the Web tool or execute the mkhost command in obtool to configure the host. As explained in "Determining the Distribution Method of Host Identity Certificates" on page 11-6, the procedure differs depending on whether you add hosts in automated or manual certificate provisioning mode.

Configuring Media Servers and Clients in Automated Certificate Provisioning Mode If you create the new hosts in automated mode, then you do not need to perform additional steps. Oracle Secure Backup creates the wallet, keys, and certificates for the host automatically as part of the normal host configuration.

When you execute the mkhost command, Oracle Secure Backup automatically performs the following steps over a secure (but nonauthenticated) SSL connection:

1. Oracle Secure Backup creates a host object corresponding to the new host in the administrative server's object repository.
2. Oracle Secure Backup sends a "set host ID" message to observiced on the new host.
3. The observiced on the new host performs the following actions during processing of the "set host ID" message:
   a. observiced creates a wallet to contain the host's certificates. The wallet resides in the directory tree of the Oracle Secure Backup home. Oracle Secure Backup uses the host ID as the wallet password.
   b. observiced creates a request for an identity certificate in the wallet.
   c. observiced returns a status message indicating success or failure of the operation.
4. The observiced on the new host sends a certificate request message to the observiced running on the administrative server. The request contains the new host's identity certificate to be signed by the CA.
5. On the administrative server, observiced signs the new host's identity certificate and returns the signed certificate and trusted certificates to the new host in the response to the certificate request message.
6. On the new host, observiced performs the following actions as part of processing the certificate response message:
   a. observiced stores the signed identity certificate in the wallet along with the trusted certificates of the CA.
   b. observiced creates the obfuscated wallet in the file system of the Oracle Secure Backup home.
   c. observiced returns a status message indicating success or failure of the operation.

The new host now owns a key pair, an identity certificate, and the trusted certificates. The host has everything it needs to create secure, two-way authenticated SSL connections with other hosts in the administrative domain.

Configuring Media Servers and Clients in Manual Certificate Provisioning Mode If you choose to add new hosts in manual mode, then you must perform the following steps for each new host:

1. Issue the mkhost command to configure the host.

In response to the mkhost command, Oracle Secure Backup performs the same steps as it does in automated mode, but stops short of step 5. In manual mode, the observiced running on the administrative server does not transmit certificates to the new host over the network.

2. Export the signed certificate for the new host from the administrative server by using the obcm utility. This task is described in "Exporting Signed Certificates" on page 11-12.
3. Copy the signed identity certificate to some type of physical media and physically transfer the media to the new host.
4. Import the signed certificate into the wallet of the new host by using the obcm utility. This task is described in "Importing Signed Certificates" on page 11-12.

The obcm utility checks that the public key associated with the certificate for the new host corresponds to the private key stored in the wallet with the certificate request. If the keys match, then the new host is a member of the domain. If the keys do not match, then an attacker probably attempted to pass off their own host as the new host during processing of the mkhost command. You can execute the mkhost command again after the rogue host has been eliminated from the network.

Setting the Size for Public and Private Keys

As a general rule, the larger the size of the public and private key, the more secure it is. On the other hand, the smaller the key, the better the performance. The default key size for all hosts in the domain is 1024 bits. If you accept this default, then you do not need to perform any additional configuration.

Oracle Secure Backup enables you to set the key to any of the following bit values, which are listed in descending order of security:

- 4096 (very secure)
- 3072 (very secure)
- 2048 (secure)
- 1024 (secure)
- 768 (not secure)
- 512 (not secure)

You can set the key size in the follow ways:

- Setting the Key Size in obparameters

  The obparameters file specifies the default key size in the security policy. The key size for all hosts in the domain defaults to this value.

- Setting the Key Size in the certkeysize Security Policy

  You can change the default key size in the security policy at any time. Any hosts configured after the change default to the new key size.

- Setting the Key Size in mkhost

  You can override the default key size for any individual host. Thus, different hosts in the domain can have different key sizes.

Setting the Key Size in obparameters

You can set the key size in the obparameters file when you install Oracle Secure Backup on the administrative server. When you install Oracle Secure Backup interactively, the install script gives you an opportunity to modify obparameters.

To set the key size in obparameters when installing interactively:

1. Before running the install script on the administrative server, or when the install script prompts you to modify obparameters, open the file in a text editor.
2. Search for the following string: certificate key size. Set the key size to the desired default value. Example 11–1 sets the default key size to 2048 bits.

Example 11–1 Setting the Key Size in obparameters

```
identity certificate key size: 2048
```

3. Save and close the file after making any other changes to obparameters.
4. Proceed with the installation.

Oracle Secure Backup uses the key size in obparameters to set the initial value for the certkeysize security policy. This security policy specifies the default security key size for hosts in the domain. You can change or override this default when configuring an individual host.

> **See Also:** *Oracle Secure Backup Installation Guide* to learn how to configure the obparameters file

Setting the Key Size in the certkeysize Security Policy

You can set the key size in the certkeysize security policy through obtool or the Web tool. Oracle Secure Backup uses the modified key size the next time you configure a new host. You can change the certkeysize value at any time, but the change only applies to the next mkhost command.

To set the certkeysize security policy:

1. Log in to obtool as a user with the modify administrative domain's configuration right.
2. Set the certkeysize policy to the desired default value. Example 11–2 shows how to use obtool to set the key size to 3072 bits.

Example 11–2 Setting the Key Size in the Security Policy

```
ob> cdp security
ob> setp certkeysize 3072
```

> **See Also:** "Setting a Policy" on page 4-5 to learn how to set a policy

Setting the Key Size in mkhost

You can set the key size when you use the mkhost command or Web tool to configure a new host. If you specify the --certkeysize option on the mkhost command, the value overrides the default certificate key size set in the security policy. The key size applies only to the newly configured host and does not affect the key size of any other current or future hosts.

Because larger key sizes require more computation time to generate the key pair than smaller key sizes, the key size setting can affect the processing time of the mkhost command. While the mkhost command is executing, obtool may display a status message every 5 seconds. obtool displays a command prompt when the process has completed (see Example 11–3).

To set the key size in the mkhost command:

1. Log in to obtool as a user with the modify administrative domain's configuration right.
2. Issue the mkhost command to set the key size for a new host. Example 11–3 shows how to set the key size to 4096 bits when configuring new client stadf56. This setting applies only to host stadf56.

Example 11–3 Setting the Key Size in mkhost

```
ob> mkhost --inservice --role client --certkeysize 4096 stadf56
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
ob> lshost stadf56
stadf56          client                            (via OB)   in service
```

See Also: *Oracle Secure Backup Reference* to learn how to use the mkhost command

Enabling and Disabling Encryption for Backup Data in Transit

As explained in "Data Encryption" on page 2-36, the default is for backup data to be encrypted while it is transferred within the administrative domain. For example, if a backup job backs up the root directory on client C to media server M, then the file system backup data is encrypted while being sent from C to M.

You can disable encryption for backup data in transit by setting the encryptdataintransit security policy to no.

To enable backup encryption in the encryptdataintransit security policy:

1. Log in to obtool as a user with the modify administrative domain's configuration right.
2. Use the setp command to switch the encryptdataintransit policy to no. Example 11–4 shows how to perform this task.

Example 11–4 Enabling Encryption for Backup Data

```
ob> cdp security
ob> setp encryptdataintransit no
```

See Also: "Setting a Policy" on page 4-5 to learn how to set a policy

Enabling and Disabling SSL for Host Authentication and Communication

As explained in "Host Authentication and Communication" on page 2-32, by default Oracle Secure Backup uses authenticated and encrypted SSL connections for all inter-host control message traffic.

You can disable SSL encryption by setting the securecomms security policy to off. Disabling SSL may help to improve performance, but be aware of the inherent security risks in this action.

To set the securecomms security policy:

1. Log in to obtool as a user with the modify administrative domain's configuration right.
2. Use the setp command to switch the securecomms policy to off. Example 11–5 shows how to perform this task.

Example 11–5 Disabling SSL for Host Authentication and Communication

```
ob> cdp security
ob> setp securecomms off
```

See Also: "Setting a Policy" on page 4-5 to learn how to set a policy

Managing Certificates with obcm

This section explains how to use the obcm utility. You can use this utility to import certificates, export certificates, and export certificate requests.

You need to use obcm when you add new hosts in the domain in manual rather than automated certificate provisioning mode. In this case, the CA does not issue a signed certificate to a new host over the network, so you must export the signed certificate from the administrative server, manually transfer the certificate to the newly configured host, and then import the certificate into the host's wallet.

Both an identity certificate and a wallet exist as files on the operating system. The operating system user running obcm must have write permissions in the wallet directory. By default, the wallet used by Oracle Secure Backup is located in the following locations:

- /usr/etc/ob/wallet (UNIX and Linux)
- C:\Program Files\Oracle\Backup\db\wallet (Windows)

obcm always accesses the wallet in the preceding locations. You cannot override the default location.

Exporting Signed Certificates

Use obcm on the administrative server to export a signed certificate for a newly configured host.

To export a signed identity certificate:

1. Log on to the administrative server.
2. Assuming that your PATH variable is set correctly, enter obcm at the operating system command line to start the utility. The operating system user running obcm must have write permissions in the wallet directory.
3. Enter the following command, where *hostname* is the name of the host requesting the certificate and *certificate_file* is the file name of the exported request:

   ```
   export --certificate --file certificate_file --host hostname
   ```

   For example, the following command exports the signed certificate for host brhost2 to file /tmp/brhost2_cert.f:

   ```
   export --certificate --file /tmp/brhost2_cert.f --host brhost2
   ```

Importing Signed Certificates

Use obcm on the new host to import a signed certificate into the host's wallet.

To import a signed certificate into the wallet of a new host:

1. Log on to the host whose wallet will contain the certificate.
2. Assuming that your `PATH` variable is set correctly, enter `obcm` at the operating system command line to start the utility. The operating system user running `obcm` must have write permissions in the wallet directory.
3. Copy the signed identity certificate to a temporary location on the file system.
4. Enter the following command at the `obcm` prompt, where *signed_certificate_file* is the file name of the certificate:

   ```
   import --file signed_certificate_file
   ```

   Because only one Oracle Secure Backup wallet exists on the host, you do not need to specify the `--host` option. For example, the following example imports the certificate from `/tmp/brhost2_cert.f`:

   ```
   import --file /tmp/brhost2_cert.f
   ```

   Note that `obcm` issues an error message if the certificate being imported does not correspond to the certificate request in the wallet.
5. Remove the certificate file from its temporary location on the operating system. For example:

   ```
   rm /tmp/brhost2_cert.f
   ```

12

Using obtar

The primary user interfaces for file system backup and restore operations are the Web tool and obtool. The underlying engine that Oracle Secure Backup uses to back up and restore data is obtar. You can use the obtar command-line interface directly, although this practice is recommended only for advanced users. This chapter includes the following topics:

- About obtar
- Backing Up Data with obtar
- Restoring Data with obtar
- Listing and Cataloging the Contents of Backups and Volumes with obtar
- Pre-Labeling Tape Volumes with obtar
- Optimizing Your Use of obtar

> **See Also:** *Oracle Secure Backup Reference* for obtar command syntax, semantics, and examples

About obtar

obtar is the underlying Oracle Secure Backup engine that moves file system data to and from tape. obtar, which is a descendent of the original Berkeley UNIX tar(1) command, enables you to use features not exposed through obtool or the Web tool.

The main purpose of obtar is to back up and restore file systems. You can specify files or directories on the obtar command line or in a Backup Description File (BDF), which is an ASCII file that contains a list of path names to include and exclude from a backup image.

> **Note:** When you specify a dataset file for a backup job with the Web tool or obtool, Oracle Secure Backup turns the dataset file into a BDF internally and supplies it as input to obtar.

You can operate the obtar utility in a number of modes, for example, obtar -g or obtar -x. Table 12–1 groups these modes into basic tasks.

Table 12–1 obtar Operations

Operation	Modes	Description	Section
Back up file system data	-g, -c	Use obtar -g to create archives for the directories and files specified in a backup description file (BDF). Use obtar -c to create an archive of the directories and files specified on the command line.	"Backing Up Data with obtar" on page 12-2
Restore file system data	-x	Use obtar -x to restore files and directories.	"Restoring Data with obtar" on page 12-8
List and catalog contents of backups	-t, -z, -zz	Use obtar -t to list the table of contents for a backup image and -tG to add the contents of the image to the Oracle Secure Backup catalog. Use obtar -z to display an archive or volume label on the tape in the specified device; use obtar -zz to display a brief table of archives for the volume. Note that you can also specify -z when running in the -g and -c modes.	"Listing and Cataloging the Contents of Backups and Volumes with obtar" on page 12-11
Label, reuse, or unlabel a volume	-Xlabel, -Xreuse, -Xunlabel	Use obtar -Xlabel to write a volume label to the tape contained in the specified device. Use obtar -Xreuse to mark the volume in the specified device as being reusable. Use obtar -Xunlabel to remove the label from the volume in the specified device. These options effectively erase the contents of the tape.	"Pre-Labeling Tape Volumes with obtar" on page 12-14

If you back up directories and files so that the necessary Oracle Secure Backup catalog data is generated (such as when using the -g, -G, or -N options), then you can use obtool or the Web tool to browse the catalog and restore the files. If you do not generate the catalog files, however, then you can still perform a raw restore operation.

Backing Up Data with obtar

You can use obtar to perform backup tasks that range from on-demand backups of single files to full and incremental backups of entire file systems and networks.

You initiate a backup by executing the `obtar -g` or `obtar -c` command. The host on which you execute the `obtar` command is called the operator host. The host that contains the data you want to back up is called the client host.

This section contains the following topics:

- Creating Backup Images on Tape
- Using Backup Description Files
- Making Incremental Backups
- Creating a Single Backup Image
- Backing Up Windows Database Components

Creating Backup Images on Tape

The data that you back up is saved in a special structure called a backup image, which was called an archive in previous product versions. The backup images created with `obtar` adhere to the IEEE POSIX.1 data recording format. You can create a backup image on media that is loaded into a tape device.

> **Note:** Oracle Secure Backup does not have native virtual tape support.

One of the options you can use with `obtar -g` is `-f`, which specifies the name of the tape device on which to create the backup image. The argument to `-f` is the name of a tape device that you have configured through the Web tool or with the `mkdev` command in `obtool`. If you do not specify the `-f` option, then `obtar` uses the device specified by the `TAPE` environment variable, if it is defined.

When you are backing up a large amount of data, `obtar` may need to continue a backup image from one volume to the next. If the tape drive resides in a library, then `obtar` automatically unloads the current volume and searches the inventory of the library for another eligible volume on which to continue the backup. The way that you install and configure `obtar` indicates whether or not it considers a device to reside inside a library.

If you are using a standalone tape drive (a drive that is not in a library), then `obtar` rewinds the tape and then unloads it, displaying a message like the following on the operator host, where *`vol-id`* refers to the next volume in the volume set:

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

`obtar` then prompts you to load the next volume and press the Return key when you are ready:

```
Please insert new tape on device
and press <return> when ready:
```

The backup continues onto the next volume.

Using Backup Description Files

When you use `obtar -g`, you specify the data you want to back up in backup description file. A backup description file (BDF) is an ASCII file that contains a list of path names to include and exclude from a backup image. Typically, you create a BDF for each host whose data you plan to back up, and execute a separate `obtar -g` command for each of those BDFs.

The following example backs up the data described in `all_bdf` to the volume in `tape1`:

```
obtar -g all_bdf -f tape1
```

A BDF consists of a list of statements, with one statement on each line. Each statement consists of a one-character directive, which must be in column 1, and a path name or host name.

You can specify the following types of statements:

- A host name statement specifies the name of the client host to be backed up. The host name statement begins with a colon (`:`) directive, as in `:dlsun1976`.
- An inclusion statement specifies a directory or file to include in the backup image. This statement begins with the plus (+) directive, as in `+/private/lashdown`.
- An exclusion statement specifies a directory or file to exclude from the backup image. A BDF can include the following types of exclusion statements:
  - A global exclusion statement specifies a path name or wildcard pattern that is to be excluded at every level in the tree. This type of statement has the following format:

    ```
    !pathname
    ```

  - An Oracle database exclusion statement specifies that Oracle database files be excluded at every level in the tree. This type of statement has the following format:

    ```
    ~files
    ```

  - A top-level exclusion statement specifies a path name or wildcard pattern that is to be excluded if found directly under the current top-level tree. This type of statement has the following format:

    ```
    -pathname
    ```

- An include file statement specifies a file to include in the BDF. An include file statement begins with the dot (`.`) directive, as in `./home/bdf`. You might use an include file to specify a list of exclusions statements that are common to all BDFs.

Example 12–1 shows an example of a BDF. Comment lines are preceded by # (pound sign).

Example 12–1 Sample BDF

```
# Use the host named chicago as the client
# host
:chicago

# Back up all files and directories in the /home
# directory
+/home

# Do not back up any directories or files with the
# extension ".bak" that are in the /home directory
# or any of its subdirectories
!*.bak
```

```
# Do not back up any directories or files that begin
# with the letters "tmp" that are directly under
# the /home directory
-tmp*

# Do not back up any Oracle database files in the /home
# directory or any of its subdirectories
~files
```

See Also:

- *Oracle Secure Backup Reference* for BDF syntax
- *Oracle Secure Backup Reference* for `obtar -g` syntax
- "Listing the Contents of a Backup Image" on page 12-11 to learn about the `-z` option, which is usable with `obtar -g`

Making Incremental Backups

"Full and Incremental File System Backups" on page 2-2 provides an overview of incremental backups. With a full backup, `obtar` backs up all data, whether or not it has changed since the last backup. With an incremental backup, `obtar` backs up only the data that has changed since a previous backup. You can request that `obtar` back up only data that has changed since a previous full backup, or data that has changed since a particular level of incremental backup.

Note: If you specify a backup level other than 0, and if `obtar` encounters data that has never been backed up before, then `obtar` reverts to a level 0 backup and sends a message to standard output.

`obtar` uses the client host's `backup-dates` file, which is stored in the administrative data on the administrative server (see "Administrative Data" on page 1-7), to determine when the last backup at a particular level was performed.

To perform incremental backups you must use `obtar -g`. You specify a backup level with the `obtar -L` option. Table 12–2 lists arguments to the `-L` option.

Table 12–2 Arguments to the -L Option

Argument	Description
`0-9`	Enables you to save only those files that have changed since the last backup at a lower level. `obtar` supports ten backup levels to be compatible with the UNIX `dump` utility, which also provides ten backup levels. This type of backup is known as a cumulative incremental backup. Backup level 0 is the same as `full`; level 1 is the same as `exincr`.
`full`	Saves all files specified in the BDF.
`incr`	Saves any files modified since an incremental backup at any level. This type of backup is known as a differential incremental backup and is equivalent to a backup at level 10.
`exincr`	Saves only the data that was modified since the last full backup. This backup is equivalent to a backup at level 1.
`offsite`	Equivalent to a full backup except that `obtar` keeps a record of the backup in such a manner that it does not affect the full/incremental backup schedule. This option is useful when you wish to create a backup image for offsite storage without affecting your schedule of incremental backups.

obtar -L also enables you to back up only those files modified since a specified date and time.

obtar supports ten backup levels to be compatible with the UNIX dump utility, which also provides ten backup levels.

The following example demonstrates one way that you might create a backup schedule. Suppose that you determine that most changes to data occur during the week and that 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 through Thursday nights
- Level 2 incremental backups on Friday night

On Sunday, you specify the following command to perform a full backup using the BDF all_bdf (you do not need to specify -L full because obtar performs a full backup by default):

```
obtar -g all_bdf
```

On Monday, you perform an incremental backup, which backs up only the data changed since the full backup on Sunday:

```
obtar -g all_bdf -L 1
```

On Tuesday, Wednesday, and Thursday you perform level 1 backups, which back up any data changed since Sunday, effectively supplanting the level 1 incremental backup made on the previous day:

```
obtar -g all_bdf -L 1
```

On Friday, you perform a level 2 backup, which backs up any data changed since the Thursday backup:

```
obtar -g all_bdf -L 2
```

Given the preceding backup schedule, a restore operation on Monday would require the volumes written during the full backup on Sunday. A restore operation on Tuesday through Friday would require the volumes from the following backups:

- The full backup from Sunday
- The most recent incremental backup

A restore operation on Saturday or Sunday would require the volumes from the following backups:

- The full backup from Sunday
- The level 1 incremental backup from Thursday
- The level 2 incremental backup from Friday

See Also: *Oracle Secure Backup Reference* for obtar -L syntax

Creating a Single Backup Image

You can use obtar -c to create a single backup image. You might use obtar -c to perform an on-demand backup or to back up data to a volume that you could transport to another site.

To create a backup image on a tape, specify a tape drive name with the `-f` option. The following example backs up the directory `/doc` to the volume loaded on the tape drive named `tape1`:

```
obtar -c -f tape0 /doc
```

See Also:

- *Oracle Secure Backup Reference* for `obtar -c` syntax, semantics, and examples
- "Listing the Contents of a Backup Image" on page 12-11 to learn about the `-z` option, which is usable with `obtar -c`

Backing Up Windows Database Components

You need to take special action to back up Windows components that maintain non-relational databases. These components include the following:

- Active Directory
- Certificate Service
- Cluster Configuration
- Removable Storage Manager

The preceding Windows database components define special-purpose APIs with which the associated data is backed up and restored. This section describes how to back up these Windows database components.

Understanding Windows Database Identifiers

Oracle Secure Backup uses text strings to identify the type and name of a database. These text strings appear in place of a path name (or leaf name) where Oracle Secure Backup consumes or creates the identity of data to back up or restore (or that has been backed up). These locations are as follows:

- File header (in the backup image)
- Interim ASCII index file
- Backup catalog for each client host
- `obtar` command-line interface
- `obtar` Backup Description File (BDF)

Database identifiers are comma-delimited, as in the following example:

```
database,db-type[,db-name]
```

In the preceding syntax, `database` is a literal text string, whereas *`db-type`* is one of the strings that you define. If the database has a name, then it follows the *`db-type`* and is separated from it with a comma.

Active Directory

To backup the Directory Services database, use a database identifier with a *`db-type`* of `ActiveDirectory` in a BDF or on a `obtar` command line:

```
database,ActiveDirectory
```

Note that *`db-type`* is case-insensitive. For Active Directory, there is no associated *`db-name`* in the database identifier.

To back up the Active Directory database, Directory Services must be running. To restore the Active Directory database, you must restart in Directory Service Restore mode as follows:

1. Restart Windows.
2. When the Starting Windows progress bar appears, press **F8**.
3. From the Windows 2000 Advanced Options menu, select **Directory Service Restore Mode**.

The preceding steps will restart the computer as a standalone server. Because the Security Access Manager (SAM) then uses a minimal set of user/group definitions stored in the registry, you may have to adjust the Oracle Secure Backup service account to enable the Oracle Secure Backup service (`observiced`) to log in successfully.

Certificate Service

To backup the Certificate Service database, use a database identifier with a *`db-type`* of `CertificateService` in a BDF or on a `obtar` command line:

```
database,CertificateService
```

The *`db-type`* is case-insensitive. For Certificate Service, there is no associated *`db-name`* in the database identifier.

To back up the Certificate Service database, the Certificate Service must be running. To restore the database, Certificate Service must be stopped. Similar to the Exchange and SQL databases, you can ask Oracle Secure Backup to automatically start and stop the Certificate Service with the `windowscontrolcertificatecervice` policy.

Cluster Configuration

To backup the Cluster Configuration database, use a database identifier with a *`db-type`* of `ClusterConfiguration` in a BDF or on a `obtar` command line:

```
database,ClusterConfiguration
```

The *`db-type`* is case-insensitive. For Cluster Configuration, there is no associated *`db-name`* in the database identifier (only the local database is backed up).

The Cluster Configuration service must be running for both a backup and restore of the Cluster Configuration database.

Removable Storage Manager

To backup the Removable Storage Manager database, use a database identifier with a *`db-type`* of `RemovableStorageManager` in a BDF or on a `obtar` command line:

```
database,RemovableStorageManager
```

The *`db-type`* is case-insensitive. For the Removable Storage Manager, there is no associated *`db-name`* in the database identifier.

The Removable Storage Manager must be running for both a backup and restore of the Removable Storage Manager database.

Restoring Data with obtar

The `obtar -x` option enables you to extract files from a backup image. You can extract the entire contents of a backup image or only part of the backup image.

To restore data to your own directories, you do not need any special rights. To restore data into directories that are not owned by you, you must be either be logged in as `root` or you must specify the `-R` option with the `obtar` command. If you use `-R`, then you must be logged in as a user belonging to a class with the `perform restores as privileged user` right.

Restoring Data to Its Original Location

The following command extracts the contents of backup image 4, which is on the volume loaded on device `tape1`:

```
obtar -x -f tape1 -F 4
```

To display the contents of the backup image as it is being extracted, use the `-v` option. For example, the following command extracts the contents of backup image 4 and displays the contents:

```
obtar -x -v -f tape1 -F 4

doc/
doc/chap1
doc/chap2
test/
test/file1
test/file2
```

The following command prevents `obtar` from overwriting any files in the `/doc` directory that have the same names as files in the backup image:

```
obtar -x -f tape1 -k /doc
```

The following command restores the contents of a raw file system partition:

```
obtar -x -f tape0 /dev/rdsk/dks0d10s1
```

The partition is assumed to have been previously formatted and to be currently unmounted.

> **See Also:** *Oracle Secure Backup Reference* for `obtar -x` syntax, semantics, and examples

Restoring Data to a Different Location

Use the `-s` option with `obtar -x` to extract the data to a location other than its original location. This option is particularly useful if you have backed up data by using absolute path names. If you do not use `-s`, then `obtar` restores the data into the original directory, overwriting any existing data with that same name.

When you use `-s`, `obtar` substitutes the *`replacement`* string for *`prefix`* in the path name being restored. *`prefix`* must include the leftmost part of the original path name. For example, if you backed up the directory `/home/jane/test`, and if you wanted the data restored to `/home/tmp/test`, then you would specify the string as follows: `-s,/home/jane,/home/tmp,`.

If you omit the *`replacement`* string, then `obtar` assumes a `null` string, which causes `obtar` to remove the *`prefix`* from every *`pathname`* where it is found. The delimiter character, shown as a comma (`,`) in the syntax statement, can be any character that does not occur in either the *`prefix`* or the *`replacement`* string.

The following command extracts the /doc directory and restores it to a directory named /tmp/doc:

```
obtar -x -f tape1 -s ,/doc,/tmp/doc, /doc
```

Using Advanced Restore Features

This section describes additional obtar restore options.

Ensuring that obtar Reads Full Blocks

If you are using obtar with UNIX pipes or sockets, then the system may return partial blocks of data even if more data is coming. This behavior can cause obtar to fail. You can use the -B option to cause obtar to do multiple reads to fill a block.

For example, suppose you want to restore data from a device that is attached to a host where Oracle Secure Backup is not installed. The following command restores the /doc directory from a device attached to the host named logan:

```
rsh logan cat /dev/nrst0 | obtar -x -B -f - /doc
```

Note that if you specify a remote device with the -f option, you do not need to use -B because obtar's network protocol guarantees the reading and writing of full blocks.

Changing Timestamps

Ordinarily, obtar restores data with its original timestamp. When you specify the -m option, obtar changes the timestamp of the data to the current date and time.

In the following example, the timestamp for all directories and files in the /old directory is changed to the current date and time:

```
obtar -x -m -f tape0 /old
```

Specifying Position Numbers

If you are using a device that supports direct-to-block positioning, then you can use the -q option to rapidly locate particular data on a volume. The argument to -q is a position-string that you obtain from the ls --backup --position command in obtool. When you use -q, obtar positions the volume directly to the location you specify.

For example, you can use the ls command in obtool to identify the position of the file /home/gms/output/test001:

```
obtool ls --backup --position /home/gms/output/test001

test001
Backup Date & Time ID  Volume ID Volume Tag File Sect  Level Position
2006/01/11.10:16:28 3  VOL000106   00000110   11    0    000045020008
```

After obtaining the position data, you can specify the -q option with obtar -t as shown in the following example:

```
obtar -t -f tape1 -q 000045020008
```

Avoiding File Overwrite

When restoring files, obtar will overwrite existing files unless explicitly told not to. On systems that support file locking, this replacement of existing files occurs even for files that are currently in use. Specify -u on the obtar command line to avoid overwriting files that are currently in use.

Listing and Cataloging the Contents of Backups and Volumes with obtar

This section describes how you can use obtar to list the contents of individual backup images on a volume and to list volume and backup image labels for a single backup image or an entire volume.

This section contains the following topics:

- Listing the Contents of a Backup Image
- Cataloging the Contents of a Backup Image
- Displaying Volume Labels

Listing the Contents of a Backup Image

You can use obtar -t to display the names of files and directories contained in a backup image. You can list the entire contents of a backup image or just part of the backup image. Note that obtar -t does not display backups of files on NDMP-accessed devices.

The following command displays the contents of the backup image located at the current position of the volume loaded on device tape1:

```
obtar -t -f tape1

project/
project/file1
project/file2
project/file3
```

To display the contents of a particular backup image on a volume set, use the -F option. For example, the following command displays the contents of backup image 4:

```
obtar -t -f tape1 -F 4

doc/
doc/chap1
doc/chap2
test/
test/file1
test/file2
```

To display additional information about a backup image, use the -v option. The following command uses the -v option to display additional information about backup image 4:

```
obtar -t -v -f tape1 -F 4

drwxrwxr-x jane/rd       0 Feb 24 16:53 2000 doc/
-rw-r--r-- jane/rd     225 Feb 24 15:17 2000 doc/chap1
-rwxrwxr-x jane/rd     779 Feb 24 15:17 2000 doc/chap2
drwxrwxr-x jane/rd       0 Feb 24 16:55 2000 test/
-rwxrwxr-x jane/rd     779 Feb 24 16:54 2000 test/file1
-rw-r--r-- jane/rd     225 Feb 24 16:54 2000 test/file2
```

To display information about a particular file or directory that is contained in the backup image, include the file or directory name as the last argument on the command line. For example, the following command displays information about the directory test, which is contained in backup image 4:

```
obtar -t -f tape1 -F 4 test
```

```
test/
test/file1
test/file2
```

You can specify more than one path name from the backup image. The following command displays information about the directories `test` and `doc` (`obtar` lists the directories in the order they appear in the backup image):

```
obtar -t -f tape1 -F 4 test doc

doc/
doc/chap1
doc/chap2
test/
test/file1
test/file2
```

See Also: *Oracle Secure Backup Reference* for `obtar -t` syntax, semantics, and examples

Cataloging the Contents of a Backup Image

You can catalog the contents of a backup image by specifying `obtar -Gt`. You can catalog either RMAN or file system backups, but note that `obtar -t` does not catalog NDMP backups. You can only catalog one image at a time.

Example 12–2 catalogs backup image 1 on the volume loaded into tape drive `tape1` (only partial output is shown). In this example, the image contains a file system backup of the `/home/someuser` directory on host `stadf56`.

Example 12–2 Cataloging a File System Backup Image

```
# obtar -f tape1 -tG -F 1

Volume label:
    Volume tag:         DEV100
    Volume ID:          VOL000001
    Volume sequence:    1
    Volume set owner:   root
    Volume set created: Tue Nov 22 15:57:36 2005

Archive label:
    File number:        1
    File section:       1
    Owner:              root
    Client host:        stadf56
    Backup level:       0
    S/w compression:    no
    Archive created:    Tue Nov 22 15:57:36 2005

/home/someuser/
/home/someuser/.ICEauthority
/home/someuser/.Xauthority
/home/someuser/.aliases
/home/someuser/.bash_history
/home/someuser/.bash_logout
/home/someuser/.bash_profile
/home/someuser/.bashrc
.
```

```
.
.
```

Example 12–3 also catalogs backup image 1 on the volume loaded into tape drive `tape1`. In this example, the image contains an RMAN backup of archived redo logs.

Example 12–3 Cataloging an RMAN Backup Image

```
# obtar -f tape1 -tG -F 1

Volume label:
    Volume tag:         ADE202
    Volume ID:          RMAN-DEFAULT-000002
    Volume sequence:    1
    Volume set owner:   root
    Volume set created: Mon Feb 13 10:36:13 2006
    Media family:       RMAN-DEFAULT
    Volume set expires: never; content manages reuse

Archive label:
    File number:        1
    File section:       1
    Owner:              root
    Client host:        stadv07
    Backup level:       0
    S/w compression:    no
    Archive created:    Mon Feb 13 10:36:13 2006
    Backup piece name:  05hba0cd_1_1
    Backup db name:     ob
    Backup db id:       1585728012
    Backup copy number: non-multiplexed backup
    Backup content:     archivelog
```

> **See Also:** *Oracle Secure Backup Reference* for `obtar -tG` syntax, semantics, and examples

Displaying Volume Labels

You can use `obtar -z` to display a backup image's volume label. You can also use the `-z` option with `obtar -t` and `obtar -g` to display a volume label, or with `obtar -c` to create a volume label.

For example, the following command causes `obtar` to display the volume label for the fourth backup image on a volume loaded on device `tape1`:

```
obtar -z -f tape1 -F 4

Volume label:
   Volume ID:          VOL000105
   Volume sequence:    1
   Volume set owner:   jane
   Volume set created: Tue Mar 2 10:13:14 2002
Backup image label:
   File number:        4
   File section:       1
   Owner:              jane
   Client host:        chicago
   Backup level:       0
   S/w compression:    no
   Archive created:    Tue Mar 2 10:13:14 2002
```

When you use `obtar -z`, `obtar` reads the backup image. Whenever `obtar` reads a backup image, it positions the volume after the backup image just read, and before the volume label of the next backup image. For example, if you entered another `obtar -z` command after the preceding command, `obtar` would display the volume label of backup image 5, if it exists:

```
obtar -zf tape0

Volume label:
   Volume ID:          VOL000003
   Volume sequence:    1
   Volume set owner:   gms
   Volume set created: Wed May 01 14:08:23 2000
Backup image label:
   File number:        5
   File section:       1
   Owner:              gms
   Client host:        campy
   Backup level:       0
   S/w compression:    no
   Archive created:    Wed May 01 14:08:23 2000
```

You can use `obtar -zz` to display all labels on the volume, as in the following example:

```
obtar -zzf tape0

Seq  Volume    Volume    Backup Image    Client    Backup    Backup Image Create
#    ID        Tag       File Sect       Host      Level     Date & Time
1    VOL000003             1   1         campy       0       05/01/00 14:08:23
1    VOL000003             2   1         phred       0       05/01/00 15:37:00
1    VOL000003             3   1         mehitibel   0       05/01/00 15:38:08
```

> **See Also:** *Oracle Secure Backup Reference* for `obtar -z` and `-zz` syntax, semantics, and examples

Pre-Labeling Tape Volumes with obtar

You can use `obtar` to pre-label tape volumes, thereby associating a printed label (the volume tag) on the tape with the recorded contents of the tape.

Use the following steps to pre-label a tape volume:

1. Before using a volume for the first time, assign a unique identifier to it. The identifier can be between 1 and 31 characters long. Write this identifier on a printed label (the volume tag) on the outside of the tape, or use a pre-printed label.
2. Place the write-enabled volume in any accessible tape drive.
3. From any host on which Oracle Secure Backup is installed:
   a. Log in as `root`, or log in to Oracle Secure Backup as a user belonging to a class having the `manage devices and change device state` right.
   b. Enter `obtar` options in the following format:

      ```
      obtar -Xlabel -Xtag:volume-tag -f tape-device
      ```

`obtar` writes the *volume-tag* to the specified *tape-device*. For example, the following command labels the tape volume found in `tape0` with the tag `WKLY58010`:

```
obtar -Xlabel -Xtag:WKLY58010 -f tape0
```

You can omit the -Xtag option if the volume has a machine-readable tag (barcode) and resides in a library equipped with a barcode reader.

> **Note:** Labeling, reusing, and unlabeling a tape volume effectively erases any data stored on it. Perform any of these operations only if the volume contains no useful data.

After you have labeled a tape, obtar retains the association between the volume tag and the volume ID. The tag is the external identifier, whereas the ID is the internal one. Each time obtar displays the label for that volume, it also displays the volume tag. Similarly, when obtar prompts you for a volume (at restore time) it displays both the volume ID and tag.

When you label a volume, you can optionally tell obtar to limit that volume's use to a specified media family. In this case, obtar does not allow data destined for media families other than the one you specify to be written to the volume.

To select the media family for the volume, include the option, -Xfa:*family-name* on the obtar command line. For example, to label the tape in the tape drive rdrive MMR-2006 and restrict its usage to media family INCR, enter the following:

```
obtar -Xlabel -Xtag:MMR-2006 -f rdrive -Xfa:INCR
```

When obtar displays the label of a volume that's permanently restricted to a certain media family, it includes the notation (permanent) next to the media family name:

```
Volume label:
Volume tag:         MMR-2006
Volume ID:          INCR-000007
Volume sequence:    1
Volume set owner:   root
Volume set created: Sun Dec 18 20:16 PM 2002
Media family:       INCR (permanent)
```

To remove the media family restriction, tell obtar to unlabel or reuse the volume. Unlabeling a volume causes all information stored on it to be effectively erased. This includes any existing volume label information. To unlabel a volume, enter the following.

```
obtar -Xunlabel -f device [-Xow]
```

Use the -Xow option only if you want obtar to disregard any expiration date extant in the volume label.

Reusing a volume is similar to unlabeling it, but a reuse operation directs obtar to preserve the existing volume label. To reuse a volume, enter the following.

```
obtar -Xreuse -f device [-Xow]
```

The -Xow option conveys the same semantic here as it does when used in the unlabel operation. It directs obtar to disregard the expiration date, if any, found in the volume label.

See Also: *Oracle Secure Backup Reference* for obtar -Xlabel, -Xunlabel and -Xreuse syntax, semantics, and examples

Optimizing Your Use of obtar

This section describes ways you can optimize your use of obtar, and provides information about some of the more advanced backup features of obtar.

This section includes the following topics:

- Using tar with Backup Images Created by obtar
- Backing Up Symbolic Links
- Creating Offsite Backups
- Backing Up and Restoring Raw File Systems
- Controlling Device Parameters
- Compacting Sparse Files
- Changing Criteria for Incremental Backups
- Changing Default Backup Behavior
- Using Shell Scripts to Perform Backups
- Excluding Subdirectories with .ob_no_backup Files
- Backing Up Across Mount Points
- Support for Oracle Secure Backup Catalog Files Over 2 GB
- Retaining Backup Statistics

Using tar with Backup Images Created by obtar

By default, obtar generates backup images that are fully compatible with tar. This section offers tips for using tar with backup images created with obtar.

When you create a backup image with obtar -g, obtar creates several files in the backup image that provide information about the backup image. obtar knows that these file are special and never extracts them from the backup image as actual files. To tar, the files appear to be ordinary files; when you use tar to extract a backup image, tar will create several files that have the prefix ###. When you restore a backup image with obtar -x, obtar does not create these files.

You can use any of the following obtar options and still maintain compatibility with tar:

```
-b, -B, -c, -f, -h, -l, -m, -p, -t, -v, -x
```

When you are using tar to extract a backup image that spans multiple volumes, note that each section of a backup image that spans multiple volumes is a valid tar file. obtar can correctly extract the contents of the backup image, but tar will encounter an early end-of-file condition after it extracts the first section of the backup image. At this point, you will have extracted only the first part of the data for the file that continues across the volume break. To restore the file completely, you need to do the following:

1. Move the first file fragment to a location that will not be overwritten as you continue the extraction.
2. Load the next volume and continue the extraction. The second file fragment will be extracted.
3. Use the UNIX cat command to append the second file fragment to the first file fragment to obtain the complete file. For example:

```
cat first_frag second_frag > complete_file
```

4. Delete the file fragments.

Backing Up Symbolic Links

When the data to be backed up includes symbolic links, `obtar` ordinarily backs up only the link text, not the data to which the link points. You can use the `-h` option to cause `obtar` to back up the data, not just the link text. The following command backs up the data that is pointed to in any paths in the BDF named `home_bdf`:

```
obtar -g home_bdf -f /dev/nwrst1 -h
```

If you include an explicit link path name in a BDF or when using `obtar -c`, then `obtar` backs up the data specified by that link whether or not you have used the `-h` option. If you do not want `obtar` to follow links explicitly mentioned in a BDF (or on the command line), however, then you can do so by specifying `-Xnochaselinks`.

Creating Offsite Backups

`obtar` supports a backup level called `offsite`. An offsite backup is equivalent to a full (level `0`) backup except that `obtar` keeps 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 wish to create a backup image for, say, offsite storage without disturbing your schedule of incremental backups. To request an offsite backup, specify `-L offsite`.

Backing Up and Restoring Raw File Systems

Normally, when `obtar` encounters a block or character special file when backing up a tree, it will only write the special file name and attributes to the backup image. If a block or character special file is mentioned at the top level of the backup tree, however, either explicitly or by means of a wildcard, `obtar` will back up the file name, attributes, and contents. For example, the following command will create a backup image consisting of all the special file names in the `/dev` directory, but will neither open nor read any special file:

```
obtar -cvf tape0 /dev
```

On the other hand, the following command will cause `obtar` to open `/dev/sd0a`, `/dev/sd13a`, `sd13b`, and so on and write the entire contents of the underlying raw file systems to the backup image:

```
obtar -cvf tape0 /dev/sd0a /dev/sd13*
```

Because this form of access bypasses the native UNIX file system, you can use it to back up raw file systems that contain non-UNIX data, for example, a disk partition containing a database.

> **Note:** You should never back up or restore a mounted file system. If a file system is mounted, activity by other processes may change the file system during the backup or restore, causing it to be internally inconsistent.

Also note the following considerations when backing up and restoring raw file systems:

- Because obtar has no idea what blocks are used or unused on the raw file system, the entire file system will always be saved (as opposed to a backup using the vendor-supplied UNIX file system, which will only save blocks in use).
- When restoring data to a raw file system, the size of the file system to which you are restoring must be at least the size of the file system that was backed up.
- When restoring a raw file system, all data currently on the file system will be lost and be totally overwritten by the data from the backup image.
- In order to restore a raw file system (or other block or character special file), the raw file system must have been previously formatted (using mkfs, mkvol, or similar tool), and the special file referring to the raw file system must preexist. Otherwise, the data will be restored as a normal file.

Controlling Device Parameters

You can use -M to set the format of Exabyte 8500, 8500c, and 8505 tape devices and turn hardware compression on or off. The syntax is as follows:

```
-M parameter:value
```

When you are using an Exabyte 8500, 8500c, or 8505 tape device, you can use -M to create backup images that can also be used with Exabyte 8200 tape devices. To set the format, specify the following:

```
-M format:{8200|8500}
```

Specify 8200 to change to 8200 format, and specify 8500 to change to 8500 format. If you do not specify either, obtar uses 8500 format.

You can also use -M to turn hardware compression on or off for any device that supports hardware compression. obtar turns hardware compression on by default. To set hardware compression, specify

```
-M compress:{on|off}
```

Specify on to turn hardware compression on, and specify off to turn hardware compression off.

If you turn hardware compression on when you create a backup image, when you restore the data, the device automatically uncompresses the data.

If you turn hardware compression on, do not specify the -Z option, which enables software compression.

If you are using the WangDAT 2600 device, changing the compression setting takes about 55 seconds because the drive automatically reformats the tape.

You can use two -M options to change format and compression with the same command. For example,

```
obtar -g my_bdf -f tapet0 -M format:8200 -M compress:off
```

Compacting Sparse Files

A sparse file is a file with holes—areas in the file that have never be written to. Ordinarily, obtar does not perform any special handling of sparse files. When you specify the -P option when you create a backup image with obtar -g or obtar -c, obtar compacts any sparse files in the backup image. When you subsequently restore the backup image, obtar restores the sparse files to their original format.

Note: This option does not apply to sparse files under Windows 2000, which are always backed up and restored in sparse form.

Changing Criteria for Incremental Backups

Normally, when `obtar` decides which files are to be included in an incremental backup, it uses the `mtimes` for the files, that is, the times at which the contents of the files were last modified. If files are added to a directory by using `mv` or `cp -p`, however, they may not get backed up because the modified times of such files are not changed from those of the original copies of the files. You can get around this problem by telling `obtar` to use the status change times (`ctimes`) rather than `mtimes` as the criteria for inclusion in an incremental backup.The status change time of a file is the time at which a file's inode was last modified.

Using `ctimes` results in the selection of all files that would have been selected using `mtimes` plus those that have been moved or copied into the directory. Specify this option by specifying `-Xuse_ctime` on the command line. For scheduled backups, you can include `-Xuse_ctime` in the `operations/backupoptions` policy.

Note the following drawback to using `-Xuse_ctime`. When using the `mtime` criteria, `obtar` resets the last accessed time (`atime`) of each file after it has been backed up. That is, the act of backing up a file does not change the `atime` of the file. If you are using `ctime` as the selection criteria, however, then `obtar` cannot reset the time last accessed because it will reset the file's change time, thus turning every incremental into a full backup. In other words, specifying `-Xuse_ctime` also turns on `-Xupdtu`.

The important points are as follows:

- If `-Xuse_ctime` is not specified, then incremental test is `mtime` and `atimes` are left unchanged and moved files may be missed.
- If `-Xuse_ctime` is specified, then incremental test is `ctime`; `atimes` reflect time of backup and moved files are caught.

Changing Default Backup Behavior

When you create a backup image with `obtar -g`, `obtar` ordinarily creates an index and a volume label and updates the backup dates file. You can use the `-S` option with `obtar -g` to suppress any or all of this behavior.

The syntax for the `-S` option is as follows:

```
-S{a|G|U|z}
```

The arguments to `-S` do the following:

- `a`

  Suppresses the creation of the index and a volume label, and the updating the backup date file

- `G`

  Suppresses the creation of the index data

- `U`

  Suppresses the updating of the backup dates file

- `z`

  Suppresses the creation of the volume label

Using Shell Scripts to Perform Backups

When you are performing regular backups, you may find it easier to execute the backups from shell scripts rather than from the command line.

The samples directory in the Oracle Secure Backup home contains a sample shell script called autoobtar. You may find it helpful to look at this file for ideas for creating your own shell scripts.

When you use shell scripts, you may want to use the obtar -y option, which generates a status file. The status file provides information about the backup session. The syntax of the -y option is as follows, where *pathname* is a file local to the operator host. If *pathname* already exists, obtar overwrites it:

```
-y pathname
```

Example 12–4 is a sample status file. Table 12–3 explains the status file entries.

Example 12–4 Sample Status File

```
status 0
devices 1
volumes VOL000017
file 5
host chicago
start_time Wed Mar 31 2005 at 15:40:04 (733610404)
end_time Wed Mar 31 2005 at 15:40:13 (733610413)
entries_scanned 12
entries_excluded 0
entries_skipped 0
mount_points_skipped 0
files 9
directories 3
hardlinks 0
symlinks 0
sparse_files 0
filesys_errors 0
unknown_type 0
file_kbytes 9
dev_kbytes 16
dev_iorate 174.3 KB/s
wrt_iorate 305.1 KB/s
path /home/pablo/test1 0
path /home/pablo/test1 0
path /home/pablo/test2 0
```

Table 12–3 Status File Entries

Entry	Meaning
status	Status code for the entire backup. Each status code is described in samples/obexit.sh. This value is 0 if no errors occurred.
volumes	Volume IDs used.
file	File number of the backup image on the volume.
host	Name of the client host.
start_time	Date and time the session began.
end_time	Date and time the session ended.
entries_scanned	Number of file system objects read.

Table 12–3 (Cont.) Status File Entries

Entry	Meaning
entries_excluded	Number of file system objects excluded from the backup image because of exclusion statements in the backup description file.
entries_skipped	Number of file system objects skipped during an incremental backup.
mount_points_skipped	Number of mount points skipped.
files	Number of files included in the backup image.
directories	Number of directories included in the backup image.
hardlinks	Number of hard links included in the backup image.
symlinks	Number of symbolic links included in the backup image.
sparse_files	Number of sparse files included in the backup image.
filesys_errors	Number of file system errors encountered.
unknown_type	Number of items that `obtar` could not recognize.
file_kbytes	Number of kilobytes of file data read to create the backup image.
dev_kbytes	Number of kilobytes of data written to the backup image.
dev_iorate	I/O rate for the period of backup image creation.
wrt_iorate	I/O rate between the start and end of actually writing data to tape.
path *pathname status*	Data included in the backup image, where *pathname* is the path name included and *status* is a status code, as described in `samples/obexit.sh`. `obtar` creates a path entry for each path name in the backup image.

Excluding Subdirectories with .ob_no_backup Files

You may wish to exclude part of a directory tree from a backup. For example, you specify `/home` in a BDF or on a `obtar` command line, but you wish to exclude `/home/bob` from the backup. If you are using datasets and the scheduler, then you can perform this task by the `exclude path` dataset directive.

An alternative is to create a file named `.ob_no_backup` in the directory to be excluded. For example:

```
touch /home/bob/.ob_no_backup
```

If you include the option `-Xmarkerfiles` on the command line, `obtar` looks for files named `.ob_no_backup`. On encountering a file with this name, `obtar` skips the containing directory and its subdirectories.

Backing Up Across Mount Points

By default, `obtar` does not cross local or remote mount points. A local mount point mounts a local file system; a remote mount point is a local mount for a file system accessed over the network.

You can use BDF mount point statements to override the default `obtar` behavior and cross mount points during backups. You can also control mount point behavior with `obtar` options. Table 12–4 summarizes the ways of controlling how `obtar` handles mount points.

Table 12–4 Controlling obtar Mount Point Behavior

Means of Mount Point Control	Description	Section
BDF mount point statements	Direct obtar to cross mount points	"Crossing Mount Points with BDF Mount Point Statements" on page 12-22
-l option	Causes obtar not to cross mount points and to ignore all BDF mount point statements	"Avoiding Mount Points with the -l Option" on page 12-23
-Xchkmnttab	Causes obtar to consult the local mount table (/etc/mnttab) rather than use a stat(2) operation and to skip remote mount points	"Avoiding Remote Mount Points with the -Xchkmnttab Option" on page 12-23
-Xcrossmp	Causes obtar to cross all mount points regardless of other mount point control options or BDF mount point statements	"Crossing Mount Points with the -Xcrossmp Option" on page 12-23

Crossing Mount Points with BDF Mount Point Statements

You can use mount point statements in a BDF to determine whether obtar crosses local and remote mount points during backups. The BDF mount point statements are as follows:

- @crossallmountpoints

  Specifies that all local and remote mount points should be crossed
- @crossremotemountpoints

  Specifies that only remote mount points should be crossed
- @crosslocalmountpoints

  Specifies that only local mount points should be crossed

The scoping rules for mount point statements are as follows:

- A mount point statement specified before all paths is applicable to all paths.
- A mount point statement specified immediately after a particular path is applicable only to this path.
- If a mount point statement is specified before all paths, then any mount point statement after it supplements the first mount point statement.

For example, suppose that you have a Linux host that mounts a local file system on /loc_mt1 and a remote file system on /rem_mt1. Example 12–5 would not back up files on either mounted file system.

Example 12–5 Avoiding Crossing Mount Points

```
obtar -czf tape1 /loc_mt1 /rem_mt1
```

To cross all mounted file systems, you could create a BDF named crossmount.bdf with the following syntax:

```
@crossallmountpoints
/loc_mt1
/rem_mt1
```

You could enter the command shown in Example 12–6 to back up both mounted file systems.

Example 12–6 Crossing Mount Points

```
obtar -g crossmount.bdf -z -f tape1
```

> **See Also:** *Oracle Secure Backup Reference* to learn about BDF mount point statements

Avoiding Mount Points with the -l Option

As explained in the preceding section, you can explicitly direct `obtar` to cross mount points by using mount point statements in a BDF. If you do not want `obtar` to cross local or remote mount points, even if the BDF includes mount point statements, then you can specify the `-l` option.

Assuming the scenario described in the preceding section, Example 12–7 would not back up the mounted file systems because `-l` is specified.

Example 12–7 Avoiding the Crossing of Mount Points

```
obtar -g crossmount.bdf -z -f tape1 -l
```

> **See Also:** *Oracle Secure Backup Reference* to learn about the `-l` option

Avoiding Remote Mount Points with the -Xchkmnttab Option

By default, `obtar` performs a `stat(2)` operation to determine whether a file represents a mount point. If a remotely mounted file system is down or not responding, then the `stat(2)` operation can cause the `obtar` process to hang.

The `-Xchkmnttab` option causes `obtar` to consult the local mount table (`/etc/mnttab`) before performing these `stat(2)` operations and to skip directories determined to be remote mount points. Local mount points are not skipped. Note the following aspects of `-Xchkmnttab` usage:

- The `-Xchkmnttab` option overrides statements in a BDF that direct `obtar` to skip or cross remote mount points.
- You can specify `-Xchkmnttab` either on the command line or in the `operations/backupoptions` policy.
- The `-Xchkmnttab` option is overridden by `-Xcrossmp`.

> **See Also:** *Oracle Secure Backup Reference* to learn about the `-Xchkmnttab` option

Crossing Mount Points with the -Xcrossmp Option

The `-Xcrossmp` option directs `obtar` to cross all mount points regardless of whether the `-l` or `-Xchkmnttab` options are specified or whether mount point statements are included in the BDF. You can include the `-Xcrossmp` option in the `operations/backupoptions` policy.

> **See Also:** *Oracle Secure Backup Reference* to learn about the `-Xcrossmp` option

Support for Oracle Secure Backup Catalog Files Over 2 GB

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 administrative servers that support the 2 GB file size include Solaris 2.8 and later (64-bit only).

Retaining Backup Statistics

`obtar` generates backup statistics in response to the `-y` *`statfile`* command line option, which is turned on automatically for any scheduled backup. In addition, you can retain these statistics in the media server's `observiced` log file by setting the `scheduler/retainbackupmetrics` policy.

A

NDMP Usage Notes

As an Oracle Secure Backup user, you do not have to be aware of NDMP in any substantive way except when you use third-party NDMP-enabled appliances. If you use Windows, Linux, or Solaris hosts with SCSI-connected or Fibre Channel-connected secondary storage hardware, then NDMP is basically invisible. There may be some cases, however, in which you need to be aware of the following behavior.

Constrained Error Reporting

NDMP specifies no programmatic means for data services to report many common errors. This restriction applies to a popular condition, "pathname not found," 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.

Backing Up Individual Files

Some 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.

Restored File Reporting

During restore operations, some NDMP data services do 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. This situation applies to Network Appliance's Data Ontap.

Glossary

administrative domain

A group of machines on your network that you manage as a common unit to perform backup and restore operations. An administrative domain must include one and only one administrative server. It can include the following:

- One or more client hosts
- One or more media 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 all clients 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.

apply backup frequency

The frequency with which Oracle Secure Backup checks the status of tape drives. When Oracle Secure Backup finds an available device, it assigns the next scheduled backup to the tape drive and starts the backup. Oracle Secure Backup checks all configured devices at this frequency and starts all backups that are ready to run as tape drives become available.

attachment

The physical or logical connection (the path in which data travels) of a tape device to a host in the administrative domain.

automated certificate provisioning mode

A mode of certificate management in which the Certification Authority (CA) signs and then transfers identity certificates to new hosts over the network. This mode of issuing certificates is vulnerable to a possible, although extremely unlikely, man-in-the-middle attack. Automated mode contrasts with manual certificate provisioning mode.

Backup Description File (BDF)

A text file used for obtar backup operations. It includes a host name and a list of directories to include or exclude from a backup image. Note that the Oracle Secure Backup scheduler transforms datasets into BDFs so that they are usable by `obtar`.

backup device

A tape drive that backs up data from primary storage media such as local disk to secondary storage media. Note that Oracle Secure Backup does not support optical tape drives.

backup encryption

The process of obscuring backup data so that it is unusable unless decrypted. Data can be encrypted at rest, in transit, or both.

backup ID

An integer that uniquely identifies a backup section.

backup image

The product of a backup operation. A single backup image can span multiple volumes in a volume set. The part of a backup image that fits on a single volume is called a backup section.

backup image file

The logical container of a backup image. A backup image consists of one file. One backup image consists of one or more backup sections.

backup image label

The data on a tape that identifies the backup image's file number, backup section number, and owner.

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 file system backups.

backup operation

A process by which data is copied from primary media to secondary media. You can use Oracle Secure Backup to make file system backups, which are backups of 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 execute 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

A portion of an backup image file that exists on a single tape. One backup image can contain one or more backup sections. Each backup section is uniquely identified by a backup ID.

backup transcript

A file that contains the standard output from a particular backup dispatched by the Oracle Secure Backup scheduler.

backup window

A time frame in which a backup operation can be executed.

barcode

A symbol code, also called a tag, that is physically applied to a volume for identification purposes. Oracle Secure Backup supports the use of tape libraries that have an automated means to read barcodes.

blocking factor

The number of 512-byte blocks to include in each block of data written to each tape drive. By default, Oracle Secure Backup writes 64K blocks to tape, which is a blocking factor of 128. Because higher blocking factors usually result in better performance, you can try a blocking factor larger than the `obtar` default. If you pick a value larger than is supported by the operating system of the server, then Oracle Secure Backup fails with an error.

bus

A collection of wires through which data is transmitted from one part of a computer to another.

busy file

A file that is currently open or being written to and is therefore inaccessible to all other users or application programs. Depending on the client configuration, busy files might not be backed up or restored.

CA

See Certification Authority (CA)

catalog

A repository that records backups in an Oracle Secure Backup administrative domain. You can use the 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.

Certificate Revocation List (CRL)

A list used in a public key infrastructure that enumerates the revoked certificates maintained by the Certification Authority (CA).

class

A named set of rights for Oracle Secure Backup users. A class can have multiple users, but each user can belong to one and only one class.

client host

Any machine or server whose files Oracle Secure Backup backs up or restores.

content-managed expiration policy

A volume with this type of expiration policy expires when all the backup pieces on the volume are marked as deleted. You can make Recovery Manager (RMAN) backups, but not file system backups, to content-managed volumes. You can use Recovery Manager (RMAN) to delete backup pieces.

cryptographic hash function

A one-way function that accepts a message as input and produces an encrypted string called a "hash" or "message digest" as output. Given the hash, it is computationally infeasible to retrieve the input. MD5 and SHA-1 are commonly used cryptographic hash functions.

cumulative incremental backup

A type of incremental backup in which Oracle Secure Backup copies only data that has changed at a lower backup level. For example, a level 3 incremental backup copies only that data that has changed since the most recent backup that is level 2 or lower.

daemons

Background processes that are assigned a task by Oracle Secure Backup during the execution of backup and restore operations. Some daemons run continually and others are started and stopped as required.

Data Management Application (DMA)

An application that controls a backup or restore operation over the NDMP through connections to a data service and tape service. The DMA is the session master, whereas the NDMP services are the slaves. In an Oracle Secure Backup administrative domain, `obtar` is an example of a DMA.

data service

An application that runs on a client and provides Network Data Management Protocol (NDMP) access to database and file system data on the primary storage system.

data transfer element (DTE)

A secondary storage device within a tape library. In libraries that contain multiple tape drives, DTEs are sequentially numbered starting with 1.

database backup storage selector

An Oracle Secure Backup configuration object that specifies characteristics of Recovery Manager (RMAN) SBT backups. The storage selector act as a layer between RMAN, which accesses the database, and the Oracle Secure Backup software, which manages the backup media.

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 dataset files. 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.

default backup start time

The time that appears in each new schedule entry you create.

defaults and policies

A set of configuration data that specifies how Oracle Secure Backup runs in an administrative domain.

device

A tape drive or tape library identified by a user-defined device name.

device discovery

The process by which Oracle Secure Backup automatically detects devices accessed through NDMP as well as configuration changes for such devices.

device special file

A file name in the `/dev` file system on UNIX or Linux that represents a hardware 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 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 Network Appliance filers.

digital signature

A set of bits computed by an Certification Authority (CA) to signify the validity of specified data. The algorithm for computing the signature makes it difficult to alter the data without invalidating the signature.

DMA

See Data Management Application (DMA)

domain

A group of machines and devices on a network that are administered as a unit with common rules and procedures. Within the internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

error rate

The number of recovered write errors divided by the total blocks written, multiplied by 100.

exclusion statement

Specifies a file or path to be excluded from a backup operation.

expiration policy

The means by which Oracle Secure Backup determines how volumes in a media family expire, that is, when they are eligible to be overwritten. A media family can either have a content-managed expiration policy or time-managed expiration policy.

Fiber Distributed Data Interface (FDDI)

A set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for wide-area networks.

Fibre Channel

A protocol used primarily among devices in a Storage Area Network (SAN).

file system backup

A backup of files on the file system initiated by Oracle Secure Backup. A file system backup is distinct from a Recovery Manager (RMAN) backup made through the Oracle Secure Backup SBT interface.

filer

A network-attached appliance that is used for data storage.

firewall

A system designed to prevent unauthorized access to or from a private network.

full backup

An operation that backs up all of the files selected on a client. Unlike in an incremental backup, files are backed up whether or not they have changed since the last backup.

heterogeneous network

A network made up of a multitude of machines, operating systems, and applications of different types from different vendors.

homogeneous network

A network comprised of similar components: one type of machine, server, and network operating system.

host

An addressable machine 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 certificates, communications between the hosts are encrypted by SSL. Almost all connections are two-way authenticated; exceptions include initial host invitation to join a 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 levels for file system backups. A cumulative incremental backup copies only data that changed since the most recent backup at a lower level. A differential incremental backup, which is equivalent to a level 10 backup, copies data that changed since an incremental backup at the same or lower level.

An incremental backup contrasts with a full backup, which always backs up all files regardless of when they last changed. A full backup is equivalent to an incremental backup at level 0.

job list

A catalog created and maintained by Oracle Secure Backup that describes past, current, and pending backup jobs.

job summary

A text file report produced by Oracle Secure Backup that describes the status of selected backup and restore jobs. Oracle Secure Backup generates the report according to a user-specified job summary schedule.

job summary schedule

A user-defined schedule for generating job summaries. You create job summary schedules with the `mksum` command in `obtool`.

LUN

Logical unit number of a device. LUNs make it possible for a number of devices to share a single SCSI ID.

manual certificate provisioning mode

A mode of certificate management in which you must manually export the signed identity certificate for a new host from the administrative server, transfer it to the new host, and manually import the certificate into the wallet of the new host. Unlike automated certificate provisioning mode, this mode is not vulnerable to a possible (if extremely unlikely) man-in-the-middle attack.

media family

A named classification of backup volumes that share the same volume sequence file, expiration policy, and write window.

media server

A machine or server that has one or more devices connected to it. A media server is responsible for transferring data to or from the devices that are attached to it.

mount mode

The mode indicates the way in which Oracle Secure Backup can use a volume physically loaded into a tape drive. Valid values are read-only, write/append, overwrite, and not mounted.

mover service

An application that runs on a media server in an Oracle Secure Backup administrative domain and provides access to secondary storage media over NDMP.

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 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 DMA, to back up servers running different operating systems. With NDMP, network congestion is minimized because the data path and control path are separated. Backup can occur locally—from file servers direct to tape drives—while management can occur centrally.

network description file

A text file that lists the hosts in your network on which Oracle Secure Backup should be installed. For each host, you can identify the Oracle Secure Backup installation type, the host name, and the list of tape drives attached. The `install` subdirectory in the Oracle Secure Backup home includes a sample network description file named `obndf`.

network drive

A hard disk physically attached to a server.

Network File System (NFS)

A client/server application that gives all network users access to shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). Users can manipulate shared files as if they were stored on local disk. With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

NT File System (NTFS)

One of the file systems for the Windows operating system. NTFS has features to improve reliability, such as transaction logs to help restore from disk failures.

no-rewind device

A tape is not rewound when Oracle Secure Backup finishes writing to it. This lets Oracle Secure Backup remain in position to write the next backup image.

obfuscated wallet

A wallet whose data is scrambled into a form that is extremely difficult to read if the scrambling algorithm is unknown. The wallet is read-only and is not protected by a password. An obfuscated wallet supports single sign-on (SSO).

object

An instance configuration data managed by Oracle Secure Backup: class, user, host, device, 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 or in a Backup Description File (BDF). `obtar` enables the use of features not exposed through obtool or the Web tool.

obtool

The principal command-line interface to Oracle Secure Backup. You can use this tool to perform all Oracle Secure Backup configuration, backup and restore, maintenance, and monitoring operations. The `obtool` utility is an alternative to the Web tool.

offsite backup

A backup that is equivalent to a full backup except that it does not affect the full/incremental backup schedule. An offsite backup is useful when you want to create an backup image for offsite 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 who runs backup operations, manages backup schedules, swaps tapes, and checks for errors.

operator assistance request

A request from Oracle Secure Backup that asks for the operator to perform a task, such as mounting a different volume during a backup.

operator host

When using obtar, this is the host on which you execute the `obtar` command.

Oracle Secure Backup home

The directory in which the Oracle Secure Backup software is installed. The Oracle Secure Backup home is typically `/usr/local/oracle/backup` on UNIX/Linux and `C:\Program Files\Oracle\Backup` on Windows. This directory contains binaries and configuration files. The contents of the directory differ depending on which role is assigned to the host within the administrative domain.

Oracle Secure Backup logical unit number

A number between 0 and 31 used to generate unique device special file names during device configuration (for example: `/dev/obt0`, `/dev/obt1`, and so on). Although it is not a requirement, unit numbers typically start at 0 and increment for each additional device of a given type, whether library or drive.

The Oracle Secure Backup logical unit number should not be confused with the SCSI logical unit number. The SCSI LUN is part of the hardware address of the device, whereas the Oracle Secure Backup logical unit number is part of the name of the device special file.

Oracle Secure Backup user

A defined account within an Oracle Secure Backup administrative domain. Oracle Secure Backup users exist in a separate namespace from operating system users.

overwrite

The process of replacing a file on your system by restoring a file that has the same file name.

PNI (Preferred Network Interface)

The network interface that should be used to transmit data to be backed up or restored. A network can have multiple physical connections between a client and the server performing a backup or restore on behalf of that client. For example, a network can have both Ethernet and Fiber Distributed Data Interface (FDDI) connections between a pair of hosts. PNI enables you to specify, on a client-by-client basis, which of the server's network interfaces should be used.

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 operations initiated with the `--privileged` option of the `backup` command. On UNIX and Linux systems, a privileged backup runs under the `root` user identity. On Windows systems, the backup runs under the same account (usually `Local System`) as the Oracle Secure Backup service on the Windows client.

public key

A number associated with a particular entity intended to be known by everyone who needs to 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.

recovery catalog

A schema in an Oracle database that contains metadata for use by Recovery Manager (RMAN). The recovery catalog is managed by RMAN and is independent of the Oracle Secure Backup catalog.

restore operation

Copies files from the volumes in a backup device to the designated system.

restore operator list

A list of operators to whom restore data requests are emailed.

retention period

The length of time that data in a volume set is not eligible to be overwritten. The retention period is an attribute of a time-managed media family. The retention period begins at the write window close time. For example, if the write window for a media family is 7 days, then a retention period of 14 days indicates that the data is eligible to be overwritten 21 days from the first write to the first volume in the volume set.

Recovery Manager (RMAN)

A utility supplied with Oracle Database used for database backup, restore, and recovery. RMAN is a separate application from Oracle Secure Backup. Unlike RMAN, you can use Oracle Secure Backup to back up any file on the file system—not just database files. Oracle Secure Backup includes an SBT interface that RMAN can use to back up database files directly to tape.

rights

Privileges within the administrative domain that are assigned to a class. For example, the perform backup as self right is assigned to the operator class by default. Every Oracle Secure Backup user that belongs to a class is granted the rights associated with this class.

roles

The functions that hosts in your network can have during backup and restore operations. There are three roles in Oracle Secure Backup: administrative server, media server, and client host. 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.

obtar

The underlying engine of Oracle Secure Backup that moves data to and from tape. obtar enables the use of features not exposed through obtool or the Web tool. In normal circumstances users do not use obtar directly.

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 executing scheduled backup operations. File system backups are triggered by a schedule, which you can create with the mksched command in obtool. In contrast, on-demand backups are one-time-only backups created with the backup command.

schedule poll frequency

The frequency with which Oracle Secure Backup determines whether manual changes have been made to any schedules. If Oracle Secure Backup finds changes, it updates the job list and starts any necessary backups.

scheduled backup

A file system backup that is scheduled through the mksched command in obtool or the Web tool (or is modified by the runjob command). A backup schedule describes which files should be backed up. A trigger defined in the schedule specifies when the backup job should run.

scheduler

A daemon (obscheduled) that runs on an administrative server and is responsible for managing all backup scheduling activities. The scheduler maintains a job list of backup jobs scheduled for execution.

service daemon

A daemon (observiced) that runs on each host in the administrative domain that 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)

Secure Sockets Layer (SSL)

A cryptographic protocol that provides secure network communication. SSL provides endpoint authentication through certificates. Data transmitted over SSL is protected from eavesdropping, tampering or message forgery, and replay attacks.

Small Computer System Interface (SCSI)

A parallel I/O bus and protocol that permits the connection of a variety of peripherals to host computers. Connection to the SCSI bus is achieved through a host adapter and a peripheral controller.

snapshot

A consistent copy of a volume or a file system. Snapshots are supported only for Network Appliance filers running Data ONTAP 6.4 or later.

SSL

See Secure Sockets Layer (SSL)

Storage Area Network (SAN)

A high-speed subnetwork of shared storage devices. A SAN is designed to assign data backup and restore functions to a secondary network where so that they do not interfere with the functions and capabilities of the server.

storage element

A physical location within a tape library where a volume can be stored and retrieved by a library's robotic arm.

storage device

A machine that contains disks for storing data.

tape drive

A 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. The drives are accessible through various protocols, including SCSI and Fibre Channel. A tape drive can exist standalone or in a tape library.

tape library

A medium changer that accepts SCSI commands to move volumes between storage elements and tape drives.

tape service

An NDMP Service that transfers data to and from secondary storage and allows the DMA to manipulate and access secondary storage.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The suite of protocols used to connect hosts for transmitting data over networks.

time-managed expiration policy

A media family expiration policy in which all volumes in a volume set can be overwritten when they reach their volume expiration time. Oracle Secure Backup computes the volume expiration time by adding the volume creation time for the first volume in the set, the write window time, and the retention period.

For example, you set the write window for a media family to 7 days and the retention period to 14 days. Assume that Oracle Secure Backup first wrote to the first volume in the set on January 1 at noon and subsequently wrote data on 20 more volumes in the set. In this scenario, all 21 volumes in the set expire on January 22 at noon.

You can make Recovery Manager (RMAN) backups or file system backups to volumes that use a time-managed expiration policy.

trigger

The part of a backup schedule that specifies the days and times at which the backups should occur.

trusted certificate

A certificate that is considered valid without the need for validation testing. Trusted certificates build the foundation of the system of trust. Typically, they are certificates from a trusted Certification Authority (CA).

Universal Unique Identifier (UUID)

An identifier used for tagging objects across a network.

unprivileged backup

File system backups created with the `--unprivileged` option of the `backup` command. When you create or modify an Oracle Secure Backup user, you associate operating system accounts with this user. Unprivileged backups of a host run under the operating system account associate with Oracle Secure Backup user who initiates the backup.

volume

A volume is a single unit of media, such as an 8mm tape. A volume can contain one or more backup images.

volume creation time

The time at which Oracle Secure Backup wrote backup image file number 1 to a volume.

volume expiration time

The date and time on which a volume in a volume set expires. Oracle Secure Backup computes this time by adding the write window duration, if any, to the volume creation time for the first volume in the set, then adding the volume retention period.

For example, assume that a volume set belongs to a media family with a retention period of 14 days and a write window of 7 days. Assume that the volume creation time for the first volume in the set was January 1 at noon and that Oracle Secure Backup subsequently wrote data on 20 more volumes in the set. In this scenario, the volume expiration time for all 21 volumes in the set is January 22 at noon.

volume ID

A unique alphanumeric identifier assigned by Oracle Secure Backup to a volume when it was labeled. The volume ID usually includes the media family name of the volume, a dash, and a unique volume sequence number. For example, a volume ID in the `RMAN-DEFAULT` media family could be `RMAN-DEFAULT-000002`.

volume label

The first block of the first backup image on a volume. It contains the volume ID, the owner's name, the volume creation time, and other information.

volume sequence file

A file that contains a unique volume ID to assign when labeling a volume.

volume sequence number

A number recorded in the volume label that indicates the order of volumes in a volume set. The first volume in a set has sequence number 1. The volume ID for a volume usually includes the media family name of the volume, a dash, and a unique volume sequence number. For example, a volume ID for a volume in the `RMAN-DEFAULT` media family could be `RMAN-DEFAULT-000002`.

volume set

A group of volumes spanned by a backup image. The part of the backup image that fits on a single volume is a backup section.

volume tag

A field that is commonly used to hold the barcode identifier, also called a volume tag, for the volume. The volume tag is found in the volume label.

wallet

A password-protected encrypted file. An Oracle wallet is primarily designed to store X.509 certificates and their associated public key/private key pair. The contents of the wallet are only available after the wallet password has been supplied, although 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 date

Defines the period of time, starting from the volume creation time, during which updates to a volume are allowed.

write-protect

To mark a file or media so that its contents cannot be modified or deleted. To write-protect a volume, you can mount a volume read-only in Oracle Secure Backup or alter the physical media with a write-protect tab.

write window

The period of time for which a volume set remains open for updates, usually by appending additional backup images. The write window opens at the volume creation time for the first volume in the set and closes after the write window period has elapsed. After the write window close time, Oracle Secure Backup does not allow further updates to the volume set until it expires (as determined by its expiration policy), or until it is relabeled, reused, unlabeled, or forcibly overwritten.

A write window is associated with a media family. All volume sets that are members of the media family remain open for updates for the same time period.

write window close time

The date and time that a volume set closes for updates. Oracle Secure Backup computes this time when it writes backup image file number 1 to the first volume in the set. If a volume set has a write window close time, then this information is located in the volume section of the volume label.

write window time

The length of time during which writing to a volume set is permitted.

Index