

# **Oracle® Secure Backup**

Migration Guide

Release 10.1

**B25049-01**

March 2006

Oracle Secure Backup Migration Guide, Release 10.1

B25049-01

Copyright © 2006, Oracle. All rights reserved.

Primary Author: Lance Ashdown

Contributing Authors: Judy Ferstenberg, Arun Sathyamurthy

Contributors: Donna Cooksey, George Stabler, Steve Wertheimer

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, and PeopleSoft are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface .....</b>	<b>v</b>
Audience .....	vi
Documentation Accessibility .....	vi
Related Documents .....	vi
Conventions .....	vii
 <b>1 Migrating from Reliaty Backup to Oracle Secure Backup .....</b>	
<b>Introduction to Oracle Secure Backup for Reliaty Backup Users .....</b>	<b>1-2</b>
Support for Oracle Database .....	1-2
Database Backup Storage Selectors .....	1-2
Oracle Database File Exclusion .....	1-3
Backup Pieces and Sections .....	1-3
Content-Managed Expiration Policies .....	1-3
Delayed Start Time for RMAN Restore Operations .....	1-3
Terminology Changes .....	1-4
Changes to Directory and File Names .....	1-4
Changes to Users and Classes .....	1-5
Oracle Class Rights .....	1-5
Oracle Class of Users .....	1-5
User Preauthorization .....	1-5
Login Token Handling .....	1-5
Changes to Tape Device Behavior .....	1-5
Autoswap and Wrap-Around Modes .....	1-5
Query Frequencies for Each Tape Drive .....	1-6
Bulk Import and Export Library Commands .....	1-6
Multiple Devices Not Supported on obtar Command Line .....	1-6
<b>Overview of the Migration from Reliaty Backup to Oracle Secure Backup .....</b>	<b>1-6</b>
Overview of the Migration Steps .....	1-7
<b>Preparing for the Migration from Reliaty Backup to Oracle Secure Backup .....</b>	<b>1-8</b>
<b>Installing Oracle Secure Backup on the Administrative Server .....</b>	<b>1-9</b>
<b>Stopping Oracle Secure Backup and Reliaty Backup Daemons on Linux and UNIX .....</b>	<b>1-13</b>
<b>Installing Oracle Secure Backup on Media Servers .....</b>	<b>1-14</b>
Installing Oracle Secure Backup on Linux and UNIX Media Servers .....	1-15
Installing Oracle Secure Backup on Windows Media Servers .....	1-15
<b>Installing Oracle Secure Backup on Clients .....</b>	<b>1-16</b>

Installing Oracle Secure Backup on Linux and UNIX Clients .....	1-16
Uninstalling Reliety Backup and Installing Oracle Secure Backup on Windows Clients ....	1-17
<b>Performing Post-Installation Review and Configuration .....</b>	<b>1-18</b>
Reviewing Oracle Secure Backup Settings .....	1-18
Configuring Additional Oracle Secure Backup Settings .....	1-20
Configuring Backup Schedules .....	1-21
<b>Uninstalling Reliety Backup from Linux and UNIX.....</b>	<b>1-21</b>
<b>Finding SCSI Device Information on Linux and UNIX .....</b>	<b>1-22</b>

## 2 Migrating from Legato to Oracle Secure Backup

<b>Overview of the Migration from Legato.....</b>	<b>2-2</b>
Legato and Oracle Secure Backup .....	2-2
Overview of the Migration Procedure .....	2-2
<b>Checking Compatibility.....</b>	<b>2-3</b>
<b>Planning the Oracle Secure Backup Domain.....</b>	<b>2-3</b>
Media Management Architecture.....	2-3
Multiple-Domain Architecture .....	2-3
Single-Domain Architecture.....	2-4
Backup Procedures and Scripts.....	2-5
Database Backups .....	2-6
File System Backups .....	2-6
<b>Managing Legato Backups When Migrating to Oracle Secure Backup.....</b>	<b>2-6</b>
Discarding Legato Backups .....	2-7
Retaining Legato Backups.....	2-8
Copying Legato Backups to Oracle Secure Backup .....	2-9
About migrate2osb .....	2-9
Copying Legato Backups in One Stage.....	2-10
Copying Legato Backups in Two Stages .....	2-11

## Index

---

# Preface

This preface contains the following topics:

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

## Audience

The *Oracle Secure Backup Migration Guide* is intended for system administrators and database administrators who need to perform either of the following tasks:

- Migrate from Reliaty Backup to Oracle Secure Backup
- Migrate from Legato Storage Manager (LSM) or Legato Single Server Version (LSSV) to Oracle Secure Backup

To use this document, you need to be familiar with the operating system environment on which you plan to use Oracle Secure Backup.

## 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 Documents

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

- *Oracle Secure Backup Installation Guide*  
This manual explains how to install Oracle Secure Backup.
- *Oracle Secure Backup Administrator's Guide*  
This manual explains how to administer an Oracle Secure Backup domain.
- *Oracle Secure Backup Reference*

This manual contains information about the command-line interfaces for Oracle Secure Backup.

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 for users who choose not to use RMAN.

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/>

The Legato Single Server Version documentation is located at the following URL:

<http://www.legato.com/products/networker/lssv/index.htm>

The Legato Storage Manager documentation for Oracle9i Database is accessible through the following URL:

<http://www.oracle.com/pls/db901/db901.homepage/>

The Reliaty Backup version 3.1.3 documentation is located at the following URL:

<http://www.oracle.com/technology/deploy/availability/reliaty/htdocs/products/>

## Conventions

The following text conventions are used in this document:

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





---

# Migrating from Reliaty Backup to Oracle Secure Backup

This chapter explains how to migrate from Reliaty Backup to Oracle Secure Backup. This chapter contains the following topics:

- [Introduction to Oracle Secure Backup for Reliaty Backup Users](#)
- [Overview of the Migration from Reliaty Backup to Oracle Secure Backup](#)
- [Preparing for the Migration from Reliaty Backup to Oracle Secure Backup](#)
- [Installing Oracle Secure Backup on the Administrative Server](#)
- [Stopping Oracle Secure Backup and Reliaty Backup Daemons on Linux and UNIX](#)
- [Installing Oracle Secure Backup on Media Servers](#)
- [Installing Oracle Secure Backup on Clients](#)
- [Performing Post-Installation Review and Configuration](#)
- [Uninstalling Reliaty Backup from Linux and UNIX](#)
- [Finding SCSI Device Information on Linux and UNIX](#)

## Introduction to Oracle Secure Backup for Reliably Backup Users

*Oracle Secure Backup Administrator's Guide* provides a comprehensive introduction to Oracle Secure Backup. This section describes only the features of Oracle Secure Backup most relevant to Reliably Backup users who are migrating to Oracle Secure Backup. The most important points are as follows:

- Oracle Secure Backup retains the ability to back up and restore UNIX, Linux, Windows, and NAS file systems in a manner completely compatible with its predecessor, Reliably Backup.
- Oracle Secure Backup adds support for the SBT API 2.0, thereby enabling Recovery Manager (RMAN) to use the Oracle Secure Backup SBT interface for media management operations (see *Oracle Secure Backup Administrator's Guide* to learn more about the SBT interface).

Thus, Oracle Secure Backup performs two separate functions: the backup and restore of Oracle databases and the backup and restore of other file system objects.

---

---

**Note:** What was referred to as recovering data in Reliably Backup is referred to as restoring data in Oracle Secure Backup. The term "recovery" refers exclusively to database recovery, which is the process of rolling forward a database backup.

---

---

Whether you use Oracle Secure Backup to back up the database or the file system, you must first establish an administrative domain and define hosts, users, devices, and so forth just as you did with Reliably Backup.

This section contains the following topics:

- [Support for Oracle Database](#)
- [Terminology Changes](#)
- [Changes to Directory and File Names](#)
- [Changes to Users and Classes](#)
- [Changes to Tape Device Behavior](#)

**See Also:** *Oracle Secure Backup Licensing Information* for Oracle Secure Backup licensing terms

### Support for Oracle Database

To support the backup of Oracle databases, Oracle Secure Backup includes additional object types and policies. This section describes these new features.

---

---

**Note:** Oracle Secure Backup does not support BMC SQL-BackTrack or Microsoft's Exchange and SQL databases.

---

---

#### Database Backup Storage Selectors

When backing up an Oracle database, you can use a configuration object called a database backup storage selector to manage aspects of the backup. For example, you can configure device restrictions, the media family, and resource wait time for a backup. The Web tool and `obtool` support a new set of commands for managing storage selectors: `mkssel`, `chssel`, `lsssel`, and `renssel`.

**See Also:** *Oracle Secure Backup Reference* to learn about the database backup storage selector commands

### Oracle Database File Exclusion

When performing a non-database backup, you can skip files that would be included in a database backup. Examples of such files include Oracle datafiles, control files, archived redo logs, flashback logs, and so forth. To exclude these files, specify the `exclude oracle database files` directive in your dataset. The corresponding entry for a backup description file (BDF) is `~files`.

**See Also:** *Oracle Secure Backup Reference* to learn about the dataset syntax

### Backup Pieces and Sections

An RMAN backup of an Oracle database results in a backup set, which is a logical container for one or more backup pieces. Each backup piece is a separate backup image.

Through the Web tool and `obtool` you can list backup pieces (`lspiece`) and remove them (`rmpiece`). The `lssection`, `rmsection`, and `unrmsection` commands give you control over the individual sections of a backup piece.

**See Also:**

- *Oracle Secure Backup Reference* to learn about the backup piece commands
- *Oracle Secure Backup Reference* to learn about section commands

### Content-Managed Expiration Policies

Reliably Backup recycled volumes based on an expiration time determined when the volume set was created. The expiration time was based on the write window and volume retention time defined in the media family for the volume. Oracle Secure Backup uses the same type of time-managed expiration policy. You can make file system backups or RMAN backups to volumes that use a time-managed policy.

You can also make RMAN backups, but not file system backups, to volumes that use a new content-managed expiration policy. When you create a media family you specify which type of expiration policy should be used. A content-managed volume expires when all backup pieces on the volume have been marked as deleted. You use the `DELETE` command in RMAN to mark tape backups as deleted.

When you install Oracle Secure Backup, the software includes a default content-managed media family named `RMAN-DEFAULT`. Oracle Secure Backup users are not permitted to delete, change, or rename this media family.

**See Also:** *Oracle Secure Backup Reference* for a description of the media family commands

### Delayed Start Time for RMAN Restore Operations

The `rmanrestorestartdelay` operations policy controls how long Oracle Secure Backup waits before beginning an RMAN-initiated restore operation. The default is 10 seconds. This delay enables the Oracle Secure Backup scheduler to optimize tape position operations when confronted with multiple restore requests.

## Terminology Changes

In some cases, terminology used in the Reliety Backup documentation has changed in the Oracle Secure Backup documentation. [Table 1–1](#) describes some of the more significant changes.

**Table 1–1** Terminology Changes

Old Term	New Term
Administrative host	Administrative server
Archive	Backup image
Archive section	Backup section
Backup database (maintained by Reliety Backup on administrative host)	Backup catalog (maintained by Oracle Secure Backup on administrative server)
Recover	Restore

**See Also:** *Oracle Secure Backup Administrator's Guide* for a glossary of Oracle Secure Backup terms

## Changes to Directory and File Names

The Reliety Backup root directory is now called the Oracle Secure Backup home directory. This directory and the files contained within it are named differently in Oracle Secure Backup.

**Table 1–2** Name Changes for Reliety Backup Files and Directories

Old Name	New Name
/usr/local/reliety/backup	/usr/local/oracle/backup
C:\Program Files\Reliety\Backup	C:\Program Files\Oracle\Backup
/usr/etc/rb	/usr/etc/ob
rbcleanup	obcleanup
rbcopy	obcopy
rbcv	osbcv
rbexec	obexec
rbxd	obxd
rbndmpd	obndmpd
rbnotify	obnotify
rbrotd	obrotd
rbscheduled	obscheduled
rb serviced	observed
rbt	obt
rbtar	obtar
rbtool	obtool

**See Also:** *Oracle Secure Backup Installation Guide* for a description of Oracle Secure Backup files and directories

## Changes to Users and Classes

This section describes changes to the way users and classes are handled.

### Oracle Class Rights

To control user access to Oracle database backups, Oracle Secure Backup includes new class rights. The `access Oracle backups` right determines which database backups an Oracle Secure Backup user can access. The `perform Oracle backups` and `restores` right enables class members to back up and restore Oracle databases.

### Oracle Class of Users

When Oracle Secure Backup is installed, a new class of users called `oracle` is defined. Users in this class can perform RMAN backup and restore operations and have owner rights to Oracle database backups. The `admin` class also has all Oracle rights.

### User Preauthorization

You can preauthorize an operating system user name for either RMAN or command-line access to Oracle Secure Backup when logged into a given host. This technique enables use of Oracle Secure Backup without going through the normal Oracle Secure Backup login requirements. When installing Oracle Secure Backup, you have the option of defining an operating system user named `oracle` who is preauthorized to execute RMAN operations.

### Login Token Handling

The following changes have been made to the handling of login tokens:

- Your login token, which Reliaty Backup used to retain, is no longer stored in your home directory. Oracle Secure Backup maintains login tokens on the administrative server (formerly called the administrative host).
- In Reliaty Backup, the login token was stamped with an expiration time based on the `security/loginduration` policy. If the administrator subsequently changed the `loginduration` policy, it would not affect the login token. In Oracle Secure Backup, the login token is tagged with the time of the login and its expiration time is dynamically recalculated on every login attempt.

#### See Also:

- *Oracle Secure Backup Reference* to learn about class rights
- *Oracle Secure Backup Reference* to learn about user commands
- *Oracle Secure Backup Reference* to learn about class commands

## Changes to Tape Device Behavior

This section describes changes to how Oracle Secure Backup handles tape libraries and tape drives.

### Autoswap and Wrap-Around Modes

Oracle Secure Backup discontinues the autoswap and wrap-around modes of library operation that were part of the automount logic in Reliaty Backup. The only change to the user interface is the disappearance of the corresponding options to the `mkdev` and `chdev` commands in `obtool` (and their Web tool equivalents).

### Query Frequencies for Each Tape Drive

Tape drives vary considerably in the degree to which the position query frequency in use affects tape throughput. For this reason, you can establish the position query frequency for each tape drive by specifying the `--queryfreq` option to `mkdev` and `chdev` for tape drives. These values take effect only if the `operations/positionqueryfrequency` policy is set to the default value.

### Bulk Import and Export Library Commands

The `importvol` and `exportvol` library commands are available in `obtool` and the Web tool. These commands move tapes into and out of a tape library through the import/export mechanism.

### Multiple Devices Not Supported on `obtar` Command Line

In Reliaty Backup, you could specify `-f` and `-fX` multiple times on the `rbtar` command line. For example, the following command specifies that `rbtar` should write to device `tape1` after `tape0` is full:

```
rbtar -g home_bdf -f tape0 -f tape1
```

Oracle Secure Backup does not support multiple specifications of `-f` or `-fX` on the `obtar` command line.

#### See Also:

- *Oracle Secure Backup Reference* for a description of the device commands
- *Oracle Secure Backup Reference* for a description of the library commands

## Overview of the Migration from Reliaty Backup to Oracle Secure Backup

This chapter explains how to migrate a Reliaty Backup administrative domain to an Oracle Secure Backup administrative domain. The migration procedure is usable for any version of Reliaty Backup.

This chapter assumes that you want to replace your Reliaty Backup administrative domain with an Oracle Secure Backup administrative domain. More specifically, the instructions make the following assumptions:

- The set of hosts in the Oracle Secure Backup domain is the same set of hosts as in the Reliaty Backup domain.
- Every host in the new Oracle Secure Backup administrative domain will retain its old Reliaty Backup role of administrative server, media server, or client.
- The Oracle Secure Backup domain will include the same tape devices that existed in the Reliaty Backup domain.

If you want to add, modify, or remove hosts or devices from the new Oracle Secure Backup domain, then you can perform this configuration after you have installed Oracle Secure Backup on the hosts in the domain.

Note that you cannot create a mixed domain that includes hosts running Reliaty Backup and hosts running Oracle Secure Backup. The software architecture and network messages of the two backup applications differ substantially. Also, you cannot run both Reliaty Backup and Oracle Secure Backup on the same host simultaneously because it results in contention for communication ports.

## Overview of the Migration Steps

This section describes the basic steps of the migration. Each step includes a link to a section in this chapter that explains the task in detail.

To migrate Reliety Backup to Oracle Secure Backup:

1. Identify all hosts and devices in the administrative domain and then back up the Reliety Backup files on the administrative server.

This task is described in ["Preparing for the Migration from Reliety Backup to Oracle Secure Backup"](#) on page 1-8.

2. Install Oracle Secure Backup on the administrative server.

During the installation, the install script detects the Reliety Backup installation and asks whether you wish to run a conversion routine called `osbcvt`. This utility automatically converts the pertinent Reliety Backup administrative files into the proper formats and locations within Oracle Secure Backup.

This task is described in ["Installing Oracle Secure Backup on the Administrative Server"](#) on page 1-9.

3. From the administrative server, use `stoprb` to stop the Reliety Backup daemons running on all Linux and Solaris clients and media servers in the administrative domain.

---

**Note:** You cannot stop Reliety Backup services on a Windows host from a remote location. Thus, you must stop them locally. This procedure is explained in ["Installing Oracle Secure Backup on Windows Media Servers"](#) on page 1-15 and ["Uninstalling Reliety Backup and Installing Oracle Secure Backup on Windows Clients"](#) on page 1-17.

---

This task is described in ["Stopping Oracle Secure Backup and Reliety Backup Daemons on Linux and UNIX"](#) on page 1-13.

4. Install Oracle Secure Backup on the media servers in the administrative domain.

After you have migrated the administrative server you are ready to migrate your remote media servers (if any). The procedure is essentially the same as for installing Oracle Secure Backup on the administrative server.

This task is described in ["Installing Oracle Secure Backup on Media Servers"](#) on page 1-14.

5. Install Oracle Secure Backup on the clients in the administrative domain.

After you have migrated the administrative server and media servers you are ready to migrate your clients. You can use your administrative server's client update feature to bring the Linux and UNIX clients into the domain. You must log on to each Windows client locally.

This task is described in ["Installing Oracle Secure Backup on Clients"](#) on page 1-16.

6. Perform post-installation review and configuration of the administrative domain.

This task is described in ["Performing Post-Installation Review and Configuration"](#) on page 1-18.

7. Uninstall Reliety Backup from all Linux and UNIX hosts in the administrative domain.

This task is described in ["Uninstalling Reliatty Backup from Linux and UNIX"](#) on page 1-21.

**See Also:** *Oracle Secure Backup Reference* for a description of the `osbcvt` utility

## Preparing for the Migration from Reliatty Backup to Oracle Secure Backup

Your first task is to prepare for the migration. You should make backups of important files, cancel active and scheduled backup jobs, and stop Reliatty Backup daemons on the administrative server.

Note that these instructions refer to the administrative server, which was known as the administrative host in Reliatty Backup. Reliatty Backup did not support the use of a Windows host for an administrative server.

The Reliatty Backup home is the directory in which Reliatty Backup is installed. By default, this home directory is `/usr/local/reliatty/backup` on Linux and UNIX and `C:\Program Files\Reliatty\Backup` on Windows (see [Table 1-2](#)).

Follow these steps to prepare for the migration:

1. Log in to the Reliatty Backup Web tool and display all hosts and devices in the administrative domain. Copy this information to a convenient location.
2. Log on to the administrative server and back up the following Reliatty Backup files and directories, making sure to use a backup tool *other than* Reliatty Backup:

- The `/etc/rbconfig` file

In this file you can locate the paths to other files that you want to back up. The following sample file shows typical directories:

```
local db dir:      /usr/etc/rb
temp dir:         /usr/tmp
rb dir:           /usr/local/reliatty/backup
admin dir:        /usr/local/reliatty/backup/admin
```

Note that `rb dir` indicates the Reliatty Backup home.

- The `admin` directory in the Reliatty Backup home (as specified in `rbconfig`)
- The local database directory (as specified in `rbconfig`)
- The `install/rbparameters` file in the Reliatty Backup home

Another backup method is to copy the `rbconfig` file, local database directory, and device files into the parent directory of your Reliatty Backup home. Afterwards, use `tar` to create an archive of this directory.

Assuming the paths shown in the preceding example of `/etc/rbconfig`, you would create the archive as follows:

```
cd /usr/local/reliatty # navigate to parent directory of Reliatty Backup home
cp -r /etc/rbconfig /usr/etc/rb . # copy rbconfig and local db
cd .. # navigate to superdirectory
tar -cvf reliatty.tar reliatty # create TAR file
```

---

**Note:** This backup can be quite large because it includes all of the Reliatty Backup catalog data for all backups on all hosts. Ensure that you have sufficient disk space for the backup.

---



You could then use `ftp` to transfer the TAR file to another host on your network and remove the original TAR from your local administrative server. Other alternatives include a native `tar` backup to a local tape drive or writing the files and directories to removable media.

3. Change into the Reliety Backup home and run the `install/probedev` utility. The command generates `probedev.out` in `/tmp`.

As shown in Step 7 of "[Installing Oracle Secure Backup on the Administrative Server](#)" on page 1-9, you can use `probedev.out` as a reference for configuring the SCSI devices attached to your media servers.

4. Copy the `install/rbparameters` file in your Reliety Backup home to a convenient location.

You will compare `rbparameters` to your new `obparameters` file to make sure that your installation locations are consistent.

5. Make sure that no active backups are running.

Check for active backups by using an `lsjob` command in `rbtool` or by checking jobs status in the Reliety Backup Web tool. If active jobs exist, then wait for them to finish or cancel them with the `canceljob` command. If jobs are pending for today, then cancel them as well. You can cancel all pending and active jobs as follows:

```
rbtool lsjob -s | xargs rbtool canceljob
```

6. Stop all Reliety Backup processes on the administrative server.

If you are using a Linux or UNIX system, then you can use the following command to list the processes:

```
/bin/ps -ef | grep rb
```

Use a `kill -9` command on all the Reliety Backup processes.

7. If your domain includes remote media servers, then gather the device information for these servers. Follow these steps:
  - a. Log on to each remote media server.
  - b. Change into the Reliety Backup home and run the `install/probedev` utility.
  - c. Rename the `probedev.out` file for each media server so that the host of origin is included in the name: `probedev_brhost2.out`, `probedev_brhost3.out`, and so forth.
  - d. Transfer the renamed `probedev.out` files for all media servers into the same directory that contains the `probedev.out` file on the administrative server.

After you have completed the tasks in this section, you are ready to install Oracle Secure Backup on the administrative server.

## Installing Oracle Secure Backup on the Administrative Server

The instructions for installing Oracle Secure Backup on the administrative server are essentially the same as the instructions in "Loading and Installing the Oracle Secure Backup Software on Linux or UNIX" in *Oracle Secure Backup Installation Guide*. The setup and most of the installation is identical.

The migration diverges from a standard installation if the `installob` script detects that Reliaty Backup is installed on your system. In this case, the script prompts you to migrate Reliaty Backup to Oracle Secure Backup. The script runs a migration utility called `osbcvt`.

The procedure in this section makes the following assumptions:

- Your local host runs Linux or UNIX. Reliaty Backup does not support Windows as the administrative server.
- Your local host was configured as an administrative server in Reliaty Backup.
- You have convenient access to a copy of *Oracle Secure Backup Installation Guide*. Rather than duplicating information, some steps in this section refer to instructions in the installation manual.

The sample output in this section is for an installation on a Solaris host called `sun_host` with an attached tape drive and tape library. The instructions are equally applicable to Linux and UNIX.

To install Oracle Secure Backup on an administrative server:

1. Use the Linux or UNIX `script` utility (or another method of your choosing) to generate a transcript of the migration. This transcript may be useful if you need assistance from Oracle Support.
2. Stage the installation software as described in "Accessing Oracle Secure Backup Installation Software" in *Oracle Secure Backup Installation Guide*.
3. Follow Steps 1 through 7 in "Loading and Installing the Oracle Secure Backup Software on Linux or UNIX" in *Oracle Secure Backup Installation Guide*. Make the following choices:
  - a. When prompted to load packages, load all the packages that will be used by hosts in the administrative domain.
  - b. Enter `yes` to start `installob`.
  - c. When prompted to review the `obparameters` file, compare the `obparameters` file to the old `rbparameters` file that you saved to a safe place in "[Preparing for the Migration from Reliaty Backup to Oracle Secure Backup](#)" on page 1-8.

Typically, `obparameters` has the following settings:

```
customized obparameters: yes
start daemons at boot: yes
start daemons at install: yes
```

Sometimes you need to customize the paths to the installation directories. Refer to *Oracle Secure Backup Installation Guide* to learn how to configure the parameters in this file. When you are satisfied with the `obparameters` file contents, enter `yes` at the `installob` prompt.

- d. Choose the interactive mode of installation.
4. When prompted to select a role for your host, select the option for the administrative server.

When the `installob` script detects the Reliaty Backup installation, the script displays output similar to the following, which varies among operating systems:

```
An installation of Reliaty Backup has been detected on this host.
If you have not already backed up your Reliaty Backup installation,
Oracle recommends that you do so now. As a part of the migration the Oracle
```

Secure Backup installer will disable any startup scripts used by Reliaty Backup.

This is required to prevent the contention for port 400 by the Reliaty Backup and Oracle Secure Backup service daemons.

Do you wish to proceed? [yes]

**5. Enter yes to proceed.**

The `installob` script asks you to confirm the migration:

Would you like to migrate the admin directory from Reliaty Backup to Oracle Secure Backup? [yes]

**6. Enter yes to confirm the migration of the admin directory.**

At this point the `installob` script launches the `osbcvt` utility and starts migrating the data. The script installs the Oracle Secure Backup device driver automatically. The script displays output similar to the following:

```
Starting data migration from Reliaty Backup to Oracle Secure Backup.
The Reliaty Backup admin data will be moved to /space/oracle/backup.051011
```

```
Data migration from Reliaty Backup is complete.
```

```
Beginning the installation. This will take just a minute and will produce
several lines of informational output.
```

```
Installing Oracle Secure Backup on sun_host (solaris version 5.7)
generating links for admin installation with Web server
checking Oracle Secure Backup's configuration file (/etc/obconfig)
setting Oracle Secure Backup directory to /space/oracle/backup.051011 in
/etc/obconfig
setting local database directory to /usr/etc/ob in /etc/obconfig
setting temp directory to /usr/tmp in /etc/obconfig
setting administrative directory to /space/oracle/backup.051011/admin in
/etc/obconfig
protecting the Oracle Secure Backup directory
installing /etc/init.d/OracleBackup for observed start/kill ops at
operating system run-level transition
installing start-script (link) /etc/rc2.d/S92OracleBackup
installing kill-script (link) /etc/rc1.d/K01OracleBackup
installing kill-script (link) /etc/rc0.d/K01OracleBackup
initializing the administrative domain
```

```
NOTE: installing Oracle Secure Backup driver in order to identify SCSI
busses...
```

```
NOTE: /space/oracle/backup.051011/.drv.solaris/ob copied to /usr/kernel/drv/ob
```

```
NOTE: /space/oracle/backup.051011/.drv.solaris/ob.conf copied to
/usr/kernel/drv/ob.conf
```

```
NOTE: /space/oracle/backup.051011/.drv.solaris/ob64 copied to
/usr/kernel/drv/sparcv9/ob
```

```
NOTE: The Oracle Secure Backup device driver has been successfully installed.
```

```
Is sun_host connected to any tape libraries that you'd like to use with
Oracle Secure Backup [no]?
```

If the local host is not a media server, then answer no to the next three questions to complete the administrative server installation; you can skip ahead to ["Stopping Oracle Secure Backup and Reliaty Backup Daemons on Linux and UNIX"](#) on page 1-13. Otherwise, proceed to the next step to configure tape devices.

7. If you have tape libraries or tape drives attached to this host that you used with Reliarty Backup, then obtain the SCSI target ID and SCSI LUN for each device attached to your system.

["Finding SCSI Device Information on Linux and UNIX"](#) on page 1-22 explains how to obtain SCSI device information for these operating systems.

8. Create the device special files as explained in the section "Creating Device Special Files with installob" in *Oracle Secure Backup Installation Guide*. For each device attached to your system, supply the SCSI target ID and SCSI LUN obtained in the preceding step.

---

**Note:** The sample output shown in this step is provided as an illustration, not as data for you to enter in your own installation.

---

The following sample output shows how to configure the tape library and tape drive from the previous step:

```
Is sun_host connected to any tape libraries that you'd like to use with
Oracle Secure Backup [no]? yes

How many Oracle Secure Backup tape libraries are attached to sun_host [1]?

Please describe each tape library by answering the following questions.

    Logical unit number [0]:
    SCSI bus name-instance [pci1000,f0]:
    SCSI target ID [3]: 1
    SCSI lun 0-7 [0]:

Is the information you entered correct [yes]?

Is sun_host 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 sun_host [1]?

Please describe each tape drive by answering the following questions.

    Logical unit number [0]:
    SCSI bus name-instance [pci1000,f0]:
    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=pci1000,f0      obt0
Could not read symbolic link /dev/bd.off
/dev/obt0 created
NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=1,0;minor=pci1000,f0      obl0
Could not read symbolic link /dev/bd.off
/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]?
```

```
Enter the name of a host onto which you'd like to install Oracle Secure Backup:
- - - - -
```

```
Would you like to install Oracle Secure Backup on any other machine [yes]?
```

9. Answer no when asked whether to install the software on other machines.

The following sample output shows the summary of the installation:

```
Would you like to install Oracle Secure Backup on any other machine [yes]? no
Installation summary:
```

Installation Mode	Host Name	OS Name	Driver Installed?	OS Move Required?	Reboot Required?
admin	sun_host	solaris	no	no	no

Oracle Secure Backup is now ready for your use.

At this stage of the migration, you are now to stop the daemons in preparation for the installation on the remaining hosts in the domain.

## Stopping Oracle Secure Backup and Reliaty Backup Daemons on Linux and UNIX

The Reliaty Backup and Oracle Secure Backup service daemons both use the same ports. If you have `rb serviced` running on a client or media server, then you will not be able to start `observed` on the same host. Thus, you should stop the Reliaty Backup processes on the clients and media servers. You should also stop the Oracle Secure Backup processes running on the administrative server.

To stop Oracle Secure Backup and Reliaty Backup daemons:

1. Log on the administrative server (if you are not already logged on).
2. Stop all Oracle Secure Backup processes running on the administrative server.

You can use the following command to list the processes:

```
/bin/ps -ef | grep ob
```

Use a `kill -9` command on all of the Oracle Secure Backup processes.

---

**Note:** If Oracle Secure Backup daemons are running on hosts in the domain other than the administrative server, perhaps because of test installations on these machines, then stop these daemons as well.

---

3. You can stop the Reliaty Backup daemons on Linux and UNIX media servers and clients by running the `install/stoprb` utility on the administrative server. You already stopped the Reliaty Backup daemons on the administrative server in ["Preparing for the Migration from Reliaty Backup to Oracle Secure Backup"](#) on page 1-8, so you do not need to stop the daemons on this host.

---

**Note:** To stop the Reliaty Backup service on Windows hosts you must log on locally to each Windows host. This procedure is explained in "Installing Oracle Secure Backup on Windows Media Servers" on page 1-15 and "Uninstalling Reliaty Backup and Installing Oracle Secure Backup on Windows Clients" on page 1-17.

---

The procedure varies depending on whether you have remote shell (`rsh`) as `root` to the hosts on which the Reliaty Backup daemons are running:

- If you have `rsh` enabled, then navigate to the Oracle Secure Backup home and use the `install/stoprb` utility on the administrative server.

You can use this utility to stop Reliaty Backup daemons on multiple hosts by specifying a space-separated list after the `stoprb` command. For example, the following command stops Reliaty Backup daemons on `brhost1`, `brhost2`, and `brhost3`:

```
# install/stoprb brhost1 brhost2 brhost3
```

- If `rsh` is not enabled, then log on to each Linux and UNIX host in the domain and stop the processes.

You can use the following command to show the processes:

```
/bin/ps -ef | grep rb
```

Use the `kill -9` command on the associated process IDs.

At this stage of the migration, only the administrative server has Oracle Secure Backup installed. You have stopped all Oracle Secure Backup and Reliaty Backup daemons running on Linux and UNIX hosts in the administrative domain.

You are now ready to install Oracle Secure Backup on the media servers and clients in the domain. If any of these hosts run the Windows operating system, then you will stop the Reliaty Backup services on these hosts, uninstall Reliaty Backup, and then install Oracle Secure Backup.

## Installing Oracle Secure Backup on Media Servers

If your administrative domain uses media servers other than the administrative server, then install Oracle Secure Backup on each media server. Otherwise, skip to "[Installing Oracle Secure Backup on Clients](#)" on page 1-16.

The installation instructions vary depending on the operating system of the media server. This section assumes that you have convenient access to a copy of *Oracle Secure Backup Installation Guide*. Rather than duplicating information, some steps in this section refer to instructions in the installation manual.

---

**Note:** In this phase of the migration, you configure only the device special files and drivers for the media servers. The Reliaty Backup device names and other device configuration data is migrated to Oracle Secure Backup automatically. You can make changes to this data in "[Performing Post-Installation Review and Configuration](#)" on page 1-18.

---

## Installing Oracle Secure Backup on Linux and UNIX Media Servers

The instructions for installing Oracle Secure Backup on media servers are basically the same as "[Installing Oracle Secure Backup on the Administrative Server](#)" on page 1-9. You must log on to each host, access the installation software by mounting the distribution media or downloading a TAR file, and then run `setup` and `installob`. The differences are as follows:

- You choose `media server` rather than `administrative server` when `installob` prompts for the role used by the host.
- You do not need to migrate the `admin` directory because the host is not configured as the administrative server.

## Installing Oracle Secure Backup on Windows Media Servers

The instructions in this section apply to Windows media servers only. The instructions are written to be as generic as possible, so the names of the GUI elements may vary slightly among the various Windows platforms.

Before installing Oracle Secure Backup on a Windows host, you must stop the Reliety Backup services and uninstall Reliety Backup. Unlike in the case of Linux and UNIX, you cannot run a batch program to stop the Reliety Backup daemons on Windows hosts remotely from the administrative server.

To uninstall Reliety Backup and install Oracle Secure Backup on a Windows media server:

1. Log on to the Windows host as an administrator.
2. Stop the Reliety Backup service as follows:
  - a. Open the Control Panel.
  - b. Double-click **Administrative Tools**.
  - c. Double-click **Services**.
  - d. Right-click **Reliety Backup** and select **Stop** from the shortcut menu.
3. Uninstall the Reliety Backup software as follows:
  - a. Open the Control Panel.
  - b. Double-click **Add or Remove Programs**.
  - c. Select **Reliety Backup**.
  - d. Click **Remove**.
  - e. Click **Yes** to remove Reliety Backup.
4. Remove the Reliety Backup device driver as follows:
  - a. Open the Control Panel.
  - b. Double-click **System**.
  - c. Click the **Hardware** tab.
  - d. Click **Device Manager**.
  - e. Right-click the `rbt` driver and select **Uninstall** from the shortcut menu.
  - f. Click **OK**.
5. Restart the system.

6. Install Oracle Secure Backup on this host and configure it as a media server. This task is explained in *Oracle Secure Backup Installation Guide*.

When Oracle Secure Backup is installed on all media servers in your administrative domain, you are ready to install Oracle Secure Backup on the clients.

## Installing Oracle Secure Backup on Clients

This section assumes that you have convenient access to a copy of *Oracle Secure Backup Installation Guide*. Rather than duplicating information, some steps in this section refer to instructions in the installation manual.

The installation instructions for a client vary depending on the host operating system. You can install on either UNIX/Linux or Windows clients first, but it is recommended that you install the software on the set of clients running a particular operating system. For example, install Oracle Secure Backup on all UNIX/Linux clients and then install Oracle Secure Backup on all Windows clients.

### Installing Oracle Secure Backup on Linux and UNIX Clients

The instructions in this section apply to Linux and UNIX only. These instructions assume that you run the `installob` script in batch mode, although you can adapt the instructions to install the software interactively. The interactive mode is recommended only if the administrative domain includes a small number of clients.

To install Oracle Secure Backup on Linux and UNIX clients:

1. Determine whether you have remote shell access to remote clients. You have the following options:
  - If you have remote shell (`rsh`) as `root` to Linux and UNIX clients, then you can run `installob` in batch mode on the administrative server. A batch installation is the most convenient and reliable means to perform the migration.  
  
Refer to the man pages for your particular operating system on how to set up the permissions for `rsh` access. Note that `rsh` access is no longer required after the software running on the client.
  - If you do not have remote shell (`rsh`) as `root` to Linux and UNIX clients, then you must install the Oracle Secure Backup software individually on each client. Use the CD-ROM, mounted locally or through NFS, or by another means.
2. Create a network description file that you can use for a batch installation.

Create a plain text file that identifies the name of each Linux or UNIX client within your existing Reliety Backup administrative domain along with the software components that need to be installed on each client. The template is called `obndf` and is located in the `admin` subdirectory of the Oracle Secure Backup home.

The following example shows the format of the network description file:

```
# Install Oracle Secure Backup on four clients:
# brclient1, brclient2, brclient3, brclient4
client      brclient1
client      brclient2
client      brclient3
client      brclient4
```



3. Edit the `obparameters` file if necessary, comparing it to the old `rbparameters` file that you saved to a safe place in ["Preparing for the Migration from Reliety Backup to Oracle Secure Backup"](#) on page 1-8.

Typically, `obparameters` has the following settings:

```
customized obparameters: yes
start daemons at boot: yes
start daemons at install: yes
```

Sometimes you need to customize the paths to the installation directories. Review the `obparameters` file and make sure that you are happy with its contents. Refer to *Oracle Secure Backup Installation Guide* to learn how to configure the parameters in this file.

4. Change to your Oracle Secure Backup home directory and run `installlob`.

If you have installed Oracle Secure Backup in the default location, then you run the installation program as follows:

```
cd /usr/local/oracle/backup
install/installlob
```

5. When prompted, choose the option for batch installation. Enter the name of the network description file that you created in Step 2.

## Uninstalling Reliety Backup and Installing Oracle Secure Backup on Windows Clients

The instructions in this section apply to Windows clients only. The instructions are written to be as generic as possible, so the names of the GUI elements may vary slightly among the various Windows platforms.

Before installing Oracle Secure Backup on a Windows host, you must stop the Reliety Backup services and uninstall Reliety Backup. Unlike in the case of UNIX and Linux, you cannot run a batch program to stop the Reliety Backup daemons on Windows hosts remotely from the administrative server.

To uninstall Reliety Backup and install Oracle Secure Backup on a Windows client:

1. Log on to the Windows client as an administrator.
2. Stop the Reliety Backup service as follows:
  - a. Open the Control Panel.
  - b. Double-click **Administrative Tools**.
  - c. Double-click **Services** (you may have to double-click **Computer Management** and then **Services**).
  - d. Right-click **Reliety Backup** and select **Stop** from the shortcut menu.
3. Uninstall the Reliety Backup software as follows:
  - a. Open the Control Panel.
  - b. Double-click **Add or Remove Programs**.
  - c. Select **Reliety Backup**.
  - d. Click **Remove**.
  - e. Click **Yes** to remove Reliety Backup.
4. Restart the system.

5. Install Oracle Secure Backup on this host and configure it as a client. This task is explained in *Oracle Secure Backup Installation Guide*.

When Oracle Secure Backup is installed on all hosts in your administrative domain, you are ready to review the domain configuration and make any changes.

## Performing Post-Installation Review and Configuration

This section describes the following tasks:

- [Reviewing Oracle Secure Backup Settings](#)
- [Configuring Additional Oracle Secure Backup Settings](#)
- [Configuring Backup Schedules](#)

### Reviewing Oracle Secure Backup Settings

Inspect the configuration data for the administrative domain to ensure that it migrated correctly from Reliety Backup. This section explains how to perform administrative tasks by means of the Oracle Secure Backup Web tool.

This section assumes that you are acquainted with the Web tool and have convenient access to *Oracle Secure Backup Administrator's Guide*. It also assumes that you have stopped the Oracle Secure Backup processes on the administrative server as described in Step 2 in "[Stopping Oracle Secure Backup and Reliety Backup Daemons on Linux and UNIX](#)" on page 1-13.

To review Oracle Secure Backup settings:

1. Log on to the administrative server and start the Oracle Secure Backup service daemon, which automatically starts the Apache Web server. For example:

```
/etc/observed
```

2. Start the Web tool as explained in "Using the Web Tool" in *Oracle Secure Backup Administrator's Guide*. For example, if the administrative server is named `sun_server`, then enter the following URL in your browser:

```
https://sun_server
```

3. Log in to the Oracle Secure Backup administrative domain as `admin`.

The `admin` password for Oracle Secure Backup is the same password used for Reliety Backup. As explained in *Oracle Secure Backup Administrator's Guide*, you can change the password for this user by clicking the **Configure** tab, **Users**, and then **Change Password**.

4. If you are backing up Windows clients and have Windows Domains, then check the `admin` user settings to be sure that they are correct. Otherwise, skip this step and proceed to the next step.

Follow these steps to configure Windows domain settings:

- a. Click the **Configure** tab and then click **Users**.
- b. Select the `admin` user and click **Edit**.
- c. Click **Windows Domains**.
- d. Enter the Windows Domain Name, Administrative User, and password for each of the Windows Domains for Windows clients that you plan to back up with Oracle Secure Backup.

When defining an user for a Windows Domain, choose the Administrator or a user configured by the Administrator. This user must belong to the Backup Operators group, must not be required to change password at login, must have a non-expiring password, and must have the right to back up files and directories, restore files and directories, log in as a service, act as part of the operating system, increase quotas, and replace a process level token.

5. Review the configuration data for the hosts in your administrative domain.

*Oracle Secure Backup Administrator's Guide* explains how to review information for hosts and perform configuration tasks. Follow these steps:

- a. From the home page, click the **Configure** tab and then **Hosts**.

Use the Hosts page as a base for the tasks in this step.

- b. Optionally, select a host and click **Rename** to rename to change the name of a host within the administrative domain.
- c. Select each host and click **Ping** to make sure that each host is resolvable to an IP address.

You can use `nslookup` or the `/etc/hosts` file on the administrative server to resolve IP address issues. Alternatively, click **Edit** to edit the properties of the host and define one or more resolvable names in **IP interface name(s)**.

- d. Ensure that the roles assigned to each host are correct. For example, ensure that the hosts with the media server role really are media servers.
- e. Select any obsolete hosts and click **Remove** to delete the hosts from the domain.
- f. Select each host and click **Edit** to confirm that the properties are set correctly. If a host is no longer in your network but has backups in the catalog for legacy reasons, then check **Suppress communication with host** and then **Apply**.
- g. In the Hosts page, select each host name and click **Update** to inform Oracle Secure Backup that this host is in the administrative domain managed by this administrative server.

6. Review the information for the tape devices in your administrative domain.

*Oracle Secure Backup Administrator's Guide* explains how to configure devices. Follow these steps:

- a. Click the **Configure** tab and then click **Devices**.

Use the Devices page as a base for the tasks in this step.

- b. Optionally, select a device name and click **Rename** to rename any devices that you would like to identify by a different name.

Note that your backup schedules have been imported from Reliaty Backup with the former device names. If you change the device names, then remember to update the backup schedules to use these new names.

- c. Select each device and click **Show Properties** to review the properties to confirm that the settings are correct.
- d. For each device, click **Edit** and then **Attachments**. Attachments identify the host and internal name by which Oracle Secure Backup accesses the device.

The new device special files will be named `hostname: /dev/obtOSB_LUN` for tape drives and `hostname: /dev/oblOSB_LUN` for libraries, where `OSB_LUN` is a placeholder for the Oracle Secure Backup logical unit number.

To remove the existing attachment for a Reliaty Backup device (*hostname: /dev/rb\**) and replace it with the Oracle Secure Backup attachments, select the media server in **Host** and enter the raw device name. Typically, if you are replacing *hostname: /dev/rbt0*, then your new device will be *hostname: /dev/obt0*.

Click **Apply** to save your attachments settings and return to the Devices page.

- e. Optionally, click **Add** to add any devices attached to Windows media servers that were not migrated from Reliaty Backup.
  - f. Click **Ping** for each device to make sure that it is accessible.
7. Inspect the remaining configuration data for datasets, media families, backup schedules, and so forth to make sure that it migrated properly.

At this stage of the migration, you have reviewed the settings in the administrative domain and confirmed that they are correct. You can take this opportunity to configure additional Oracle Secure Backup settings.

## Configuring Additional Oracle Secure Backup Settings

In this section, you have an opportunity to modify your administrative domain configuration. For example, you can create new users. This section assumes that you have convenient access to *Oracle Secure Backup Administrator's Guide*, which provides detailed configuration instructions.

To configure additional domain settings:

1. Optionally, add classes that define different rights other than those found in the default classes installed by Oracle Secure Backup.

The section "Configuring Classes" in *Oracle Secure Backup Administrator's Guide* explains how to perform this task.

2. Add other Oracle Secure Backup users as needed. You may want to create users who can log in with limited rights.

The section "Configuring Users" in *Oracle Secure Backup Administrator's Guide* explains how to perform this task.

3. Edit your defaults and policies settings to custom configure them to your site.

The section "Configuring Defaults and Policies" in *Oracle Secure Backup Administrator's Guide* explains how to perform this task.

4. Configure a job summary schedule so that you can have backup status summaries produced and mailed at user-defined intervals.

The section "Configuring Job Summary Schedules" in *Oracle Secure Backup Administrator's Guide* explains how to perform this task.

5. Configure preauthorizations, database backup storage selectors, and media families needed for RMAN backups.

The section "Configuring RMAN and Oracle Secure Backup" in *Oracle Secure Backup Administrator's Guide* explains how to perform this task.

At this stage of the migration, the Oracle Secure Backup administrative domain is configured. You are now ready to begin creating backups schedules in preparation for normal backup operations.

## Configuring Backup Schedules

Before resuming normal backup operations, ensure that your backup settings are configured correctly and the tape devices are prepared.

This section refers to administrative tasks that you can perform with the Oracle Secure Backup Web tool. If you need additional information about how to perform these tasks, refer to *Oracle Secure Backup Administrator's Guide*.

1. Check your media servers to confirm that their inventory status is current.

Log in to the Web tool as the `admin` user and perform the following steps:

- a. In the home page, Click **Manage** and then **Libraries**.
- b. In the Libraries page, select each library name and then select **Inventory** from **Library Commands**. Click **Apply**.
- c. Check **Force** to force an inventory and then click **OK**.
- d. In the Libraries page, select each library and click **List Volumes**.

2. Check that your backup schedules have the right host and device names specified to reflect any changes made to your configuration.

*Oracle Secure Backup Administrator's Guide* explains how to configure backup schedules. Follow these steps:

- a. From the home page, click **Backup** and then **Schedules**.
- b. Select each schedule and click **Edit** to display the properties and modify them if necessary.
- c. Click **Triggers** to display the trigger information and modify it if necessary.

3. Restart the schedule daemon.

*Oracle Secure Backup Administrator's Guide* explains how to manage daemons. Follow these steps:

- a. Click the **Manage** tab and then click **Daemons**.
- b. In the **Type** list, select **obscheduled**.
- c. In the **Host** list, select the administrative server.
- d. Click **Suspend** and then **Resume**.

4. From the home page, Click **Manage** and then **Jobs** to make sure that backups scheduled for today are displayed.

5. From the home page, click **Backup** and then **Backup Now** to create a test backup job. For example, create a subdirectory called `testbkup` in your `/tmp` directory, copy a few small files to this directory, and then back up `/tmp/testbkup`.

6. From the home page, click **Restore** and then **Backup Catalog**. To test a restore operation, restore the backup that you created in the previous step.

You are now ready to resume normal backups operations with Oracle Secure Backup.

## Uninstalling Reliaty Backup from Linux and UNIX

At this point the migration from Reliaty Backup to Oracle Secure Backup is almost complete. You can now uninstall Reliaty Backup from your Linux and UNIX hosts.

---

**Note:** You do not need to uninstall Reliaty Backup from Windows hosts because you perform this task in ["Uninstalling Reliaty Backup and Installing Oracle Secure Backup on Windows Clients"](#) on page 1-17.

---

To uninstall Reliaty Backup from the Linux and UNIX hosts in your domain:

1. Log on as `root` to the host that was the administrative server for your Reliaty Backup domain.
2. Change into the Reliaty Backup root directory:  

```
cd /usr/local/reliaty/backup
```
3. Run the `uninstallrb` utility:  

```
install/uninstallrb
```
4. Answer the questions asked by `uninstallrb` to remove Reliaty Backup from each Linux and UNIX host in your administrative domain. Be sure to start with your clients and uninstall your administrative server last.

## Finding SCSI Device Information on Linux and UNIX

*Oracle Secure Backup Installation Guide* provides a general description of how to obtain device information on Linux and UNIX when installing Oracle Secure Backup. You can find the information for your Reliaty Backup devices by examining the `probedev.out` file that you generated in Step 3 of ["Preparing for the Migration from Reliaty Backup to Oracle Secure Backup"](#) on page 1-8.

On Solaris, search the file for the string `/var/adm/messages` and look for a line that includes a target and LUN for the SCSI device. [Example 1-1](#) shows an example of the relevant section on a Solaris system.

### **Example 1-1** *probedev Output for Solaris*

```
/var/adm/messages...
Oct 13 09:52:25 sun_host unix: rb0: <EXABYTE EXB-85058SQANXR1>
Oct 13 09:52:25 sun_host unix: rb0 at glm0:
Oct 13 09:52:25 sun_host unix: target 0 lun 0
Oct 13 09:52:25 sun_host unix: rb0 is /pci@1f,0/pci@1/scsi@1/rb@0,0
Oct 13 09:52:25 sun_host unix: rb2: <EXABYTE EXB-10i>
Oct 13 09:52:25 sun_host unix: rb2 at glm0:
Oct 13 09:52:25 sun_host unix: target 1 lun 0
Oct 13 09:52:25 sun_host unix: rb2 is /pci@1f,0/pci@1/scsi@1/rb@1,0
```

In [Example 1-1](#), the EXB-8505 tape drive uses SCSI target ID 0 and SCSI lun 0. The EXABYTE EXB-10i tape library uses SCSI target ID 1 and SCSI lun 0.

On Linux, search the file for the string `/proc/scsi/scsi` and look for a line that includes a target and LUN for the SCSI device. [Example 1-2](#) shows an example of the relevant section on a Linux system.

### **Example 1-2** *probedev Output for Linux*

```
/proc/scsi/scsi...
Attached devices:
Host: scsi0 Channel: 00 Id: 03 Lun: 00
Vendor: ADIC      Model: FastStor DLT      Rev: 0115
```

```
Type:      Medium Changer                ANSI SCSI revision: 02
Host: scsi0 Channel: 00 Id: 04 Lun: 00
Vendor: Quantum  Model: DLT4000          Rev: D98C
Type:      Sequential-Access             ANSI SCSI revision: 02
```

In [Example 1–2](#), the FastStor DLT Library is using SCSI target ID 03 and SCSI lun 0. The DLT4000 tape drive uses SCSI target ID 04 and SCSI lun 0.

In addition to specifying SCSI device information, you must also assign an Oracle Secure Backup logical unit number during the configuration process. This number, which is between 0 and 31, is used to generate unique device special file names during device configuration. Sample device special file names are `/dev/obt0` and `/dev/obt1`.

Typically, Oracle Secure Backup logical unit numbers start at 0 and increment for each additional device of a given type, whether library or drive. Do not confuse the Oracle Secure Backup logical unit number with the SCSI LUN. The SCSI LUN is part of the hardware address of the device, whereas the Oracle Secure Backup logical unit number is part of the device special file name. The Oracle Secure Backup logical unit number is the first number queried for each device during the configuration process.





---

# Migrating from Legato to Oracle Secure Backup

This chapter explains how to migrate from Legato Storage Manager (LSM) or Legato Single Server Version (LSSV) to Oracle Secure Backup. This chapter contains the following topics:

- [Overview of the Migration from Legato](#)
- [Checking Compatibility](#)
- [Planning the Oracle Secure Backup Domain](#)
- [Managing Legato Backups When Migrating to Oracle Secure Backup](#)

## Overview of the Migration from Legato

This section offers an overview of the migration from a Legato environment to an Oracle Secure Backup environment. This section contains the following topics:

- [Legato and Oracle Secure Backup](#)
- [Overview of the Migration Procedure](#)

### Legato and Oracle Secure Backup

In previous database releases, Legato Storage Manager and Legato Single Server Version were bundled with Oracle Database. Legato Single Server Version included a single-server version of the EMC Legato NetWorker and the NetWorker Module for Oracle that together enabled administrators to back up Oracle databases to tape.

---

---

**Note:** Legato Storage Manager and Legato Single Server Version are referred to collectively as Legato in this chapter. The instructions in this chapter apply only to the versions of Legato previously bundled with Oracle Database.

---

---

Oracle now provides Oracle Secure Backup and Oracle Secure Backup Express as its media management solution. Oracle Secure Backup Express is recommended as the best replacement for previously bundled versions of Legato. The instructions in this chapter refer to Oracle Secure Backup, but apply equally to either Oracle Secure Backup or Oracle Secure Backup Express.

The Oracle Secure Backup media management software enables you to back up files on your file system to tape and is also fully integrated with RMAN to provide data protection services for one or more Oracle databases in a networked environment.

This chapter describes best practices for migrating from a Legato environment to an Oracle Secure Backup environment. This chapter does not explain how to install or configure Oracle Secure Backup. These tasks are explained in *Oracle Secure Backup Installation Guide* and *Oracle Secure Backup Administrator's Guide*.

Although the focus of this chapter is on migrating from Legato to Oracle Secure Backup, many of the practices and recommendations described in this chapter are applicable to migration from other media management products.

**Tip:** *Oracle Secure Backup Licensing Information*

### Overview of the Migration Procedure

The basic stages of the migration from Legato to Oracle Secure Backup are as follows:

1. Verify that the components of your Legato infrastructure work with Oracle Secure Backup.

["Checking Compatibility"](#) on page 2-3 explains this stage.

2. Plan the Oracle Secure Backup administrative domain. In this stage, you must consider the environment where Legato is currently used and how you will deploy Oracle Secure Backup there.

["Planning the Oracle Secure Backup Domain"](#) on page 2-3 explains this stage.

3. Install Oracle Secure Backup and either discard, maintain, or copy your legacy Legato backups.

"Managing Legato Backups When Migrating to Oracle Secure Backup" on page 2-6 explains this stage.

## Checking Compatibility

Verify that the components of your Legato infrastructure are certified to work with Oracle Secure Backup. Gather the following information:

- Hardware type and operating system version of the hosts on which you plan to install Oracle Secure Backup
- Type and firmware version of your tape drives and libraries

You can find a list of supported platforms and devices at the following Web site:

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

## Planning the Oracle Secure Backup Domain

Before migrating from Legato to Oracle Secure Backup, decide where you will install Oracle Secure Backup and how you will use the software to make backups. As explained in "Managing Legato Backups When Migrating to Oracle Secure Backup" on page 2-6, you should also decide whether to migrate or discard legacy Legato backups.

This section contains the following topics:

- [Media Management Architecture](#)
- [Backup Procedures and Scripts](#)

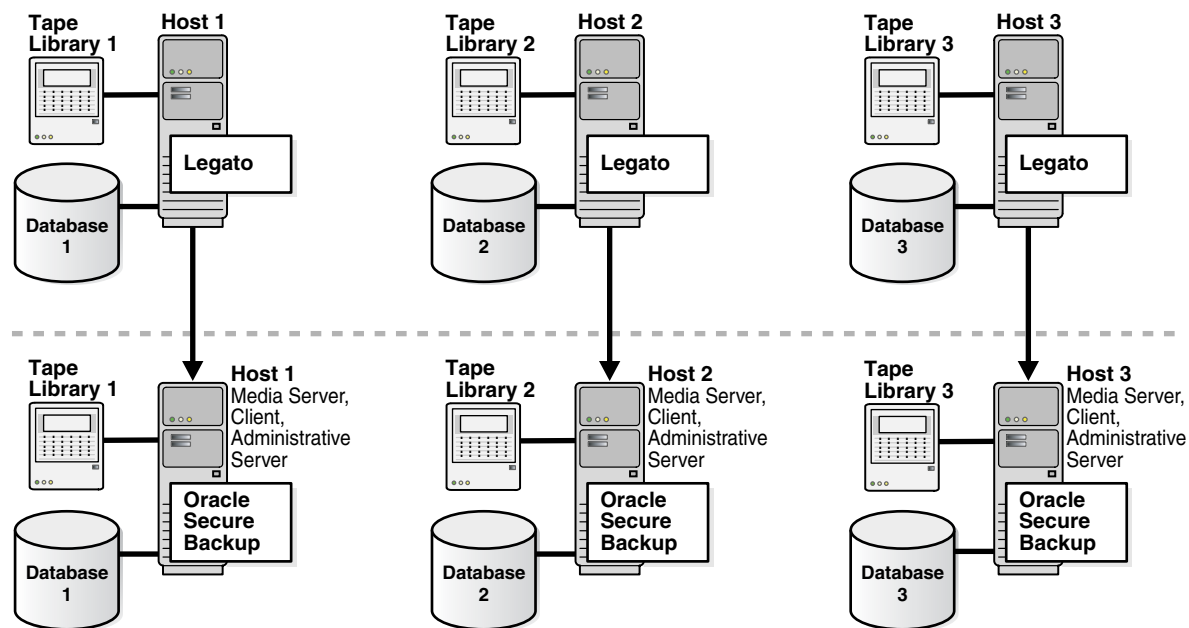
### Media Management Architecture

Typically, Legato environments include a small to medium number of hosts, each of which backs up data to a small number of locally attached tape devices. You can use the same model with Oracle Secure Backup and configure each host to use locally attached devices. Alternatively, you can consolidate your backup environment so that backups are sent to centralized media servers within a single administrative domain. This section describes both approaches.

#### Multiple-Domain Architecture

A multiple-domain architecture most closely corresponds to your existing Legato architecture. In this architecture, you install Oracle Secure Backup on every host on which you previously installed Legato and leave the tape devices as they are. Each host functions as administrative server, media server, and client.

[Figure 2-1](#) illustrates a sample network of three hosts, each of which runs Legato in conjunction with an Oracle database and has a locally attached tape device. During migration, you install Oracle Secure Backup on each host and assign it the roles of client, media server, and administrative server.

**Figure 2–1 Multiple-Domain Architecture**

To implement this architecture, follow these instructions:

1. Install Oracle Secure Backup on every Oracle database host.
2. Assign each host the role of administrative server, media server, and client.

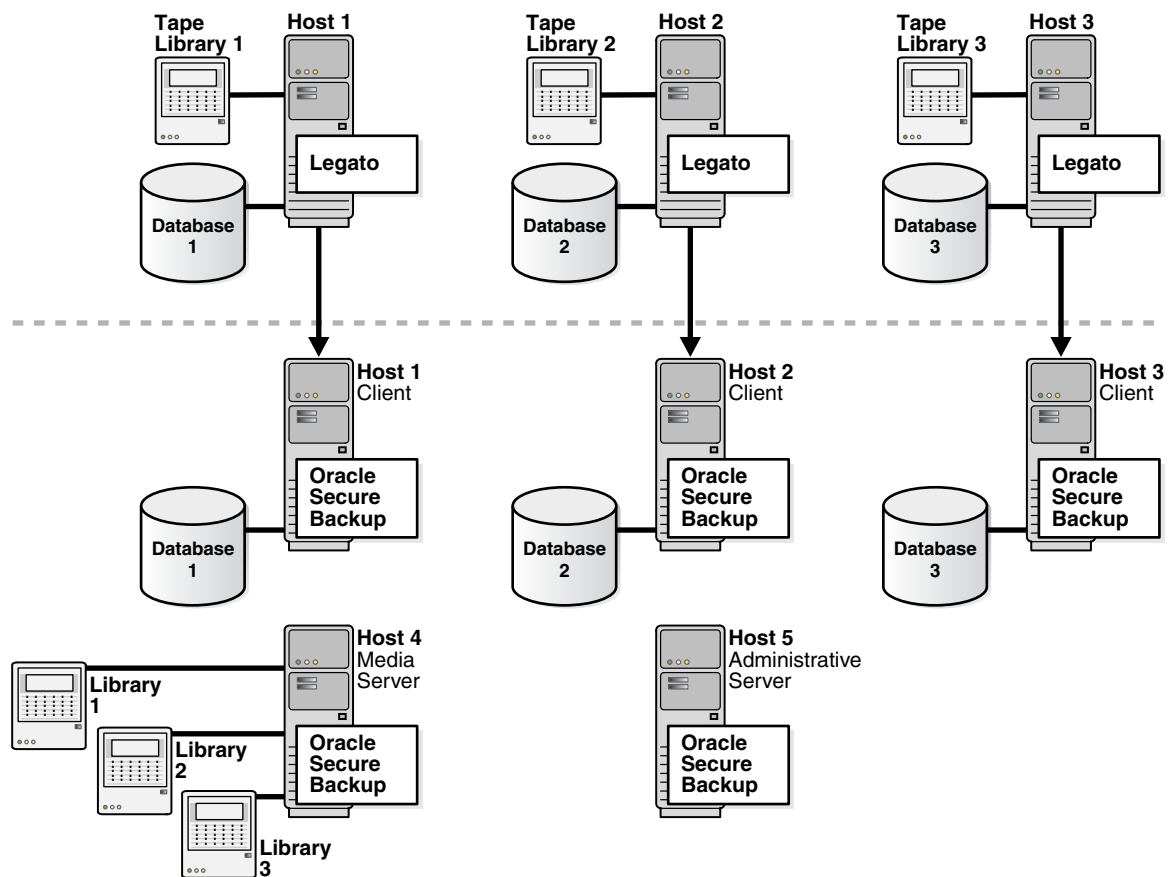
Make sure to answer **yes** when prompted to configure your Oracle homes to use the Oracle Secure Backup SBT interface for database backups.

3. Configure the tape devices attached to each host.

**See Also:** *Oracle Secure Backup Installation Guide* to learn how to install and configure Oracle Secure Backup

### Single-Domain Architecture

This architecture offers the benefits of centralized media and backup catalog management. [Figure 2–2](#) illustrates the same Legato network depicted in [Figure 2–1](#). During migration, you install Oracle Secure Backup on each of the three hosts and assign it the role of client. The tape devices are centralized on a fourth host, which is the media server. A fifth host is a dedicated administrative server, which manages the administrative domain.

**Figure 2–2 Single-Domain Architecture**

To implement this architecture, follow these instructions:

1. Identify the host that will be the administrative server and install Oracle Secure Backup on this host.  
You can configure a new host to assume this role, as shown in [Figure 2–2](#), or use an existing host. If you use an existing host, and if one of the hosts contains a centralized RMAN recovery catalog, then this host is a good candidate for the administrative server
2. Identify the hosts that will manage the tape devices and install Oracle Secure Backup on these hosts. Assign these hosts the role of media server.
3. Configure the tape devices attached to the media servers.
4. Install Oracle Secure Backup on the database hosts and assign them the client role.

Make sure to answer yes when prompted to configure your Oracle homes to use the Oracle Secure Backup SBT interface for database backups.

**See Also:** *Oracle Secure Backup Installation Guide* to learn how to install and configure Oracle Secure Backup

## Backup Procedures and Scripts

Oracle Secure Backup supports both file system and database backups. Depending on how you implement your Oracle Secure Backup environment, you may need to modify your backup procedures and scripts.

## Database Backups

After configuring RMAN to make backups through the Oracle Secure Backup SBT interface, you may need to make the following additional changes:

- Change RMAN tape parallelism if the number of tape drives used for database backups changes during the migration. You can perform this task with the `CONFIGURE DEVICE TYPE SBT PARALLELISM` command.
- Remove `PARMS` parameters that provide the name of the SBT module or vendor-specific environment variables. Oracle Secure Backup does not require these `PARMS` settings.

---

**Note:** Because you may need to retain your existing media manager configuration for a period of time during the migration, only remove the `PARMS` settings when they are no longer needed.

---

- Create database backup storage selectors within Oracle Secure Backup. Simple installations probably do not need storage selectors. You should create them only if you need to direct backups to different types or classes of media.
- Create one or more Oracle Secure Backup preauthorizations. Oracle Secure Backup can grant preauthorized access to the operating system user under which an RMAN backup is performed.

### See Also:

- *Oracle Database Backup and Recovery Advanced User's Guide* to learn how to configure RMAN for use with a media manager
- *Oracle Database Backup and Recovery Reference* to learn about the `CONFIGURE` command
- *Oracle Secure Backup Administrator's Guide* to learn how to use Oracle Secure Backup with a database

## File System Backups

Because Legato supports only database backups, you probably use a different tool to back up the non-database contents of the systems that host your databases. When migrating to Oracle Secure Backup, decide whether to use Oracle Secure Backup to protect the file system data as well as the databases on those systems.

**See Also:** *Oracle Secure Backup Administrator's Guide* to learn how to perform file system backups.

# Managing Legato Backups When Migrating to Oracle Secure Backup

After planning your administrative domain, you can install Oracle Secure Backup and configure the domain. The procedure varies depending on what you do with your legacy Legato backups. You have the following options:

- Discard your Legato tape backups.

In this case, you cannot restore Legato backups after migrating your environment to Oracle Secure Backup, but you do not have the overhead of maintaining or copying the Legato backups.

This technique is described in ["Discarding Legato Backups"](#) on page 2-7.

- Retain your Legato tape backups but do not copy them to tapes managed by Oracle Secure Backup.

In this case, you must manage the Oracle Secure Backup environment as well as a Legato installation capable of restoring the Legato backups.

This technique is described in ["Retaining Legato Backups"](#) on page 2-8.

- Copy some or all of your Legato tape backups to tapes managed by Oracle Secure Backup.

In this case, you do not need to maintain a Legato installation after migration, yet some or all of the data previously stored in Legato is restorable by Oracle Secure Backup. This solution necessitates the overhead of copying your old Legato backups to tapes managed by Oracle Secure Backup.

This technique is described in ["Copying Legato Backups to Oracle Secure Backup"](#) on page 2-9.

Your backup retention policies dictate which option is best for your environment.

## Discarding Legato Backups

In this option, you uninstall Legato from a database host, install Oracle Secure Backup, and reuse or discard the old Legato tapes. This option requires no overhead and is suitable for databases that meet either of the following criteria:

- Databases with no historical retention requirements
- Databases whose primary backups are located on disk rather than on tape

Only discard your legacy tape backups if you are able to take a new full backup immediately after installing Oracle Secure Backup.

To migrate to Oracle Secure Backup and discard legacy tape backups:

1. Identify the databases to be backed up to the Oracle Secure Backup SBT interface.
2. Perform a consistent shutdown of the databases identified in the previous step.

Note that you do not have to shut down the databases if your configuration meets both of the following criteria:

- You are backing up to disk as well as to tape.
- You have sufficient backups on disk to recover if a failure occurs during the migration.

If your configuration does not meet the preceding criteria, then you risk losing data if a failure occurs before you make a new backup with Oracle Secure Backup.

If you cannot shut down the database during the Oracle Secure Backup migration, and if you have no disk backups, then make a temporary disk backup. This backup protects you from failures during the migration. You can discard the temporary backup after making a backup with Oracle Secure Backup.

3. For each database, run the RMAN command `DELETE BACKUP DEVICE TYPE sbt` to remove its Legato backups.
4. Uninstall Legato from all hosts where it is no longer needed.
5. Install and configure Oracle Secure Backup on each host in your administrative domain according to the architecture that you chose in ["Media Management Architecture"](#) on page 2-3.

*Oracle Secure Backup Installation Guide* explains how to install and configure Oracle Secure Backup.

6. Modify your RMAN scripts to work with Oracle Secure Backup.

As explained in "[Database Backups](#)" on page 2-6, you may need to change the PARMS settings used by RMAN when backing up through the Legato interface. *Oracle Database Backup and Recovery Advanced User's Guide* to learn how to configure RMAN for use with a media manager.

7. Back up each database to tape.

If you are not using disk backups, then back up the databases to tape *before* opening the database. If you use disk backups, then these backups protect you from failure until your scheduled backup time. *Oracle Secure Backup Administrator's Guide* explains how to back up a database with Oracle Secure Backup.

8. Verify that the new Oracle Secure Backup backups can be restored by using the RMAN RESTORE VALIDATE command.
9. Open the databases and make them available to users.

## Retaining Legato Backups

In this option, you maintain dual Legato and Oracle Secure Backup installations on a host for as long as you need to restore backups from Legato. You must maintain the legacy Legato tapes along with the Oracle Secure Backup tapes.

This option may be suitable for databases that meet any of the following criteria:

- Databases with long retention requirements
- Databases where it is not desirable or feasible to copy older backups into Oracle Secure Backup
- Databases that cannot be shut down or left unprotected during migration

To migrate to Oracle Secure Backup and retain legacy backups in Legato:

1. Identify the databases to be backed up to the Oracle Secure Backup SBT interface.
2. Install and configure Oracle Secure Backup on each host in your administrative domain according to the architecture that you chose in "[Media Management Architecture](#)" on page 2-3.

*Oracle Secure Backup Installation Guide* explains how to install Oracle Secure Backup.

---

**Note:** Because this strategy requires that Legato and Oracle Secure Backup co-exist for some time, consider how to allocate tape resources. Legato and Oracle Secure Backup cannot share tape resources.

---

3. Modify your RMAN scripts to work with Oracle Secure Backup.

As explained in "[Database Backups](#)" on page 2-6, you may need to change the PARMS settings used by RMAN when backing up through the Legato interface. See *Oracle Secure Backup Administrator's Guide* to learn how to configure RMAN for use with Oracle Secure Backup.

4. Create RMAN scripts to restore backups from Legato.



There will be a period of time during which you may need to restore backups from either Legato or Oracle Secure Backup. During this time, you need RMAN scripts to restore from Legato. These scripts should use manually allocated channels that specify the Legato shared library.

Optionally, you can write restore scripts that reference both Legato and Oracle Secure Backup shared libraries, thereby enabling RMAN to restore backups from either Legato or Oracle Secure Backup. [Example 2–1](#) shows a sample script of this type. When you run this script, RMAN automatically uses the correct channel to restore the required backups.

#### **Example 2–1 Specifying Legato and Oracle Secure Backup Libraries**

```
RUN
{
  ALLOCATE CHANNEL c1 TYPE sbt
    PARMS 'SBT_LIBRARY=oracle_secure_backup_library';
  ALLOCATE CHANNEL c2 TYPE sbt
    PARMS 'SBT_LIBRARY=legato_library';
  RESTORE DATABASE;
  RECOVER DATABASE;
}
```

5. Verify that you can back up files in the new Oracle Secure Backup environment.

A small backup of the control file, a few datafiles, and a few archived redo logs is sufficient to test that you can back up.

6. Verify that you can restore files from both Legato and Oracle Secure Backup by using the RMAN `RESTORE VALIDATE` command.
7. When your Legato backups are no longer needed, perform the following tasks:
  - Uninstall Legato.
  - Discard the special restore scripts that you created to restore from Legato.
  - Reuse the Legato tape resources.

## **Copying Legato Backups to Oracle Secure Backup**

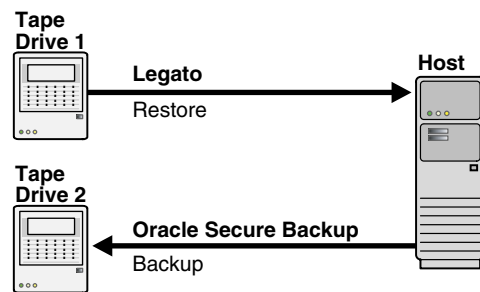
Assume that you require continued access to historical backup data that is stored in Legato, but you choose not to maintain a separate Legato environment. In this case, you can migrate all or some of your Legato backups into Oracle Secure Backup. The `migrate2osb` utility facilitates the migration.

### **About migrate2osb**

You can use the `migrate2osb` utility to migrate all or selected backups from Legato to Oracle Secure Backup. You can also use `migrate2osb` to perform any of the following independent tasks:

- Display backup pieces backed up by Legato
- Restore Legato backups to disk
- Restore and back up the backup pieces in one step

[Figure 2–3](#) illustrates the basic process of migration.

**Figure 2–3 Migrating Backups from Legato to Oracle Secure Backup**

When copying backups from Legato to Oracle Secure Backup, the procedure varies depending on the following:

- Whether you can run Legato and Oracle Secure Backup simultaneously during the copying process
- Whether you have enough disk space to restore all Legato backup pieces at the same time or must restore to disk in stages

Use [Table 2–1](#) to determine which procedure to follow.

**Table 2–1 Choosing a Copy Procedure**

Can Stage All Files at the Same Time	Can Run Legato and Oracle Secure Backup Simultaneously	Recommended Procedure
Yes or No	Yes	<a href="#">"Copying Legato Backups in One Stage"</a> on page 2-10
Yes	No	<a href="#">"Copying Legato Backups in Two Stages"</a> on page 2-11

### Copying Legato Backups in One Stage

In this scenario, `migrate2osb` stages Legato backups to disk, backs them up again with Oracle Secure Backup, and continues the process until all files have been staged and backed up. This scenario assumes the following:

- You can operate both Legato and Oracle Secure Backup at the same time.
- You have local disk space that you can use as a staging area. The total size of the files in the Legato tapes can be greater than the specified size of the staging directory. If any individual file exceeds the specified size, then `migrate2osb` displays a message and does not restore this file. If each individual file is larger than the specified directory size, then `migrate2osb` displays an error and exits.

The copying procedure is a variation of the procedure described in ["Retaining Legato Backups"](#) on page 2-8.

To copy Legato backups to Oracle Secure Backup:

1. Follow Steps 1 through 6 in ["Retaining Legato Backups"](#) on page 2-8. Make sure that the environment variables required for `migrate2osb` to identify the database (`ORACLE_HOME`, `ORACLE_SID`, and `PATH`) are set.
2. Use the `migrate2osb` utility to copy all Legato backups to Oracle Secure Backup. The script automatically stages all Legato backup pieces to a directory, backs up the staged backup pieces to tape, and repeats until all backup pieces are copied.

In [Example 2–2](#), the `--mmparms` option specifies media management parameters needed to restore backups from Legato, while `--osbparms` specifies parameters

for Oracle Secure Backup. The `--size` attribute indicates that Legato backup pieces will be restored in batches of 5 GB. The `--directory` attribute identifies `/stage` as the staging directory.

### Example 2-2 Restoring and Backing Up with One Command

```
migrate2osb --restore all
--mmparms 'SBT_LIBRARY=/opt/nsr/legato.so'
--directory /stage --size 5G
--backup --osbpars 'SBT_LIBRARY=/usr/local/oracle/backup/lib/libobk.so'
```

3. Verify that you can restore the migrated backup pieces by running the RMAN `RESTORE VALIDATE` command with Oracle Secure Backup.
4. When your Legato backups are no longer needed, perform the following tasks:
  - Uninstall Legato.
  - Discard the special restore scripts that you created to restore from Legato.
  - Reuse the Legato tape resources.

**See Also:** *Oracle Secure Backup Reference* to learn about the `migrate2osb` utility

### Copying Legato Backups in Two Stages

This scenario uses `migrate2osb` to stage all Legato backups to a single directory. After you restore all of the backup pieces, you uninstall Legato and install Oracle Secure Backup. You then use `migrate2osb` to back up the staged files to tape by means of Oracle Secure Backup. This scenario assumes the following:

- You either cannot or do not want to operate Legato and Oracle Secure Backup at the same time during the migration.
- You have sufficient space on local disk to stage all Legato backups at the same time.

The recommended procedure in this scenario uses the `migrate2osb` utility. You first use the utility to stage the files to disk with Legato. After you uninstall Legato and install Oracle Secure Backup, you use the utility to back up the staged files to tape with Oracle Secure Backup.

The recommended procedure in this scenario modifies the procedure described in ["Discarding Legato Backups"](#) on page 2-7.

To copy Legato backups to Oracle Secure Backup:

1. Identify the Oracle databases to be backed up to the Oracle Secure Backup SBT interface.
2. Perform a consistent shutdown of the databases identified in the previous step.
3. Use `migrate2osb` to restore all Legato backup pieces to a single staging directory. [Example 2-3](#) restores files to the `/stage` directory.

### Example 2-3 Restoring Backup Pieces from Legato to a Temporary Directory

```
migrate2osb --restore all
--mmparms 'SBT_LIBRARY=/opt/nsr/libnwora.so'
--directory /stage
```

In [Example 2-3](#), the `--restore` option specifies media management parameters needed to restore backups from Legato. The `--mmparms` parameters must be the same as those in the `RMAN ALLOCATE CHANNEL` commands used with Legato. Note that because `--size` is not specified, the tool calculates the size available.

4. Uninstall Legato from all hosts where it is no longer needed.
5. Follow Steps 5 through 9 in "[Discarding Legato Backups](#)" on page 2-7.
6. Back up the staged backup pieces through the Oracle Secure Backup interface by means of the `migrate2osb` utility. [Example 2-4](#) shows a sample backup to tape.

**Example 2-4 Backing Up Staged Backup Pieces to Tape**

```
migrate2osb
--backup --osbparms 'SBT_LIBRARY=/usr/local/oracle/backup/lib/libobk.so'
--directory /stage
```

In [Example 2-4](#), the `--backup` option specifies media management parameters needed by Oracle Secure Backup. The `--osbparms` parameters must be the same used in the `RMAN ALLOCATE CHANNEL` commands used with Oracle Secure Backup.

**See Also:** *Oracle Secure Backup Reference* to learn about the `migrate2osb` utility

---

---

# Index

## A

---

access Oracle backups right, 1-5  
admin class, 1-5  
admin directory, migrating, 1-11, 1-15  
administrative hosts, 1-4  
administrative servers, 1-4  
    installing Oracle Secure Backup on, 1-9, 1-10  
    unsupported on Windows in Reliaty Backup, 1-8  
ALLOCATE CHANNEL command, 2-12  
Apache Web server, 1-18  
archive sections, 1-4  
archives, 1-4

## B

---

backup description files, 1-3  
backup images, 1-3, 1-4  
backup pieces, 1-3, 2-9, 2-10  
backup retention policies, 2-7  
backup schedules, configuring, 1-21  
backup sections, 1-4  
backup sets, 1-3  
BDF  
    *See* backup description files  
best practices for Legato migration, 2-2  
BMC SQL-BackTrack, 1-2

## C

---

canceljob command, 1-9  
catalog, Oracle Secure Backup, 1-4  
chdev command, 1-5, 1-6  
chssel command, 1-2  
classes, Oracle Secure Backup, 1-5, 1-20  
    admin, 1-5  
    oracle, 1-5  
clients, installing Oracle Secure Backup on, 1-16  
CONFIGURE command, 2-6  
content-managed expiration policies, 1-3

## D

---

database backup storage selectors, 1-2, 1-20, 2-6  
database backups, 1-2, 1-3, 1-5, 1-20, 2-4, 2-6  
database files, excluding from backups, 1-3  
DELETE command, 2-7

device drivers, Oracle Secure Backup, 1-11  
device special files, configuring, 1-12, 1-14, 1-23  
--directory option, migrate2osb program, 2-11

## E

---

EMC Legato NetWorker, 2-2  
EMC NetWorker Module for Oracle, 2-2  
expiration policies  
    content-managed, 1-3  
    time-managed, 1-3  
exportvol command, 1-6

## F

---

file system backups, 1-2, 1-3, 2-2, 2-6

## I

---

importvol command, 1-6  
installing Oracle Secure Backup, 1-9, 1-10, 1-14, 1-16,  
    2-7, 2-11  
    batch mode, 1-16, 1-17  
    remote shell access, 1-16  
    Windows, 1-15, 1-17  
installob program, 1-10, 1-11, 1-15, 1-16, 1-17

## J

---

job summary schedules, 1-20

## L

---

Legato Single Server Version, 2-2  
Legato Storage Manager, 2-2  
Legato tape backups  
    copying, 2-9  
    copying in one stage, 2-10  
    copying in two stages, 2-11  
    discarding, 2-7, 2-9  
    retaining, 2-8  
Legato, uninstalling, 2-7, 2-9, 2-11, 2-12  
licensing terms, Oracle Secure Backup, 1-2  
Linux operating system, 1-2, 1-7, 1-8, 1-9, 1-10, 1-13,  
    1-14, 1-15, 1-16, 1-21, 1-22  
login tokens, 1-5

loginduration policy, 1-5  
lsjob command, 1-9  
lspiece command, 1-3  
lssection command, 1-3  
lsssel command, 1-2

## M

---

media families, 1-2, 1-20  
    RMAN-DEFAULT, 1-3  
media servers, 1-9  
    installing Oracle Secure Backup on, 1-14  
Microsoft Exchange, 1-2  
migrate2osb program, 2-9, 2-10, 2-11  
    --directory option, 2-11  
    --mmparms option, 2-10, 2-12  
    --osbparms option, 2-10, 2-12  
    --restore option, 2-12  
    --size option, 2-10  
migration from Legato  
    best practices, 2-2  
    checking compatibility, 2-3  
    modifying backup scripts, 2-5  
    multiple-domain architecture, 2-3  
    overview, 2-2  
    planning the domain, 2-3  
    single-domain architecture, 2-4  
migration from Reliety Backup  
    installing Oracle Secure Backup, 1-9  
    migrating the admin directory, 1-11  
    overview, 1-6  
    preparations, 1-8  
mkdev command, 1-5, 1-6  
mkssel command, 1-2  
--mmparms option, migrate2osb program, 2-10, 2-12

## N

---

NAS file systems, 1-2  
network description files, 1-16, 1-17  
NFS, 1-16

## O

---

obcleanup program, 1-4  
obcopy program, 1-4  
obexec program, 1-4  
obixd program, 1-4  
obndf file, 1-16  
obndmpd program, 1-4  
obnotify program, 1-4  
obparameters file, 1-9, 1-10, 1-17  
obrobotd program, 1-4  
obscheduled daemon, 1-4  
observed daemon, 1-13, 1-18  
observed program, 1-4  
obt program, 1-4  
obtar program, 1-4, 1-6  
obtool commands  
    chdev, 1-5, 1-6  
    chssel, 1-2

exportvol, 1-6  
importvol, 1-6  
lspiece, 1-3  
lssection, 1-3  
lsssel, 1-2  
mkdev, 1-5, 1-6  
mkssel, 1-2  
renssel, 1-2  
rmpiece, 1-3  
rmsection, 1-3  
unrmsection, 1-3  
obtool program, 1-2, 1-4  
operating systems  
    Linux, 1-2, 1-7, 1-8, 1-9, 1-10, 1-13, 1-14, 1-15, 1-16,  
        1-21, 1-22  
    UNIX, 1-2, 1-7, 1-8, 1-9, 1-10, 1-13, 1-14, 1-15, 1-16,  
        1-21, 1-22  
    Windows, 1-2, 1-7, 1-8, 1-10, 1-14, 1-15, 1-16, 1-17,  
        1-18, 1-20, 1-22  
oracle class, 1-5  
Oracle database home, 2-10  
Oracle Secure Backup  
    installing, 2-7, 2-11  
    introduction to, 1-2  
Oracle Secure Backup catalog, 1-4  
Oracle Secure Backup daemons, 1-13  
    observed, 1-13, 1-18  
    stopping, 1-13  
Oracle Secure Backup files  
    obndf, 1-16  
    obparameters, 1-9, 1-10, 1-17  
Oracle Secure Backup home, 1-4, 1-16, 1-17  
Oracle Secure Backup licensing terms, 1-2  
Oracle Secure Backup logical unit number, 1-23  
Oracle Secure Backup policies  
    loginduration, 1-5  
    positionqueryfrequency, 1-6  
Oracle Secure Backup programs, 1-10  
    installob, 1-10, 1-11, 1-15, 1-16, 1-17  
    migrate2osb, 2-9, 2-10, 2-11  
    obcleanup, 1-4  
    obcopy, 1-4  
    obexec, 1-4  
    obixd, 1-4  
    obndmpd, 1-4  
    obnotify, 1-4  
    obrobotd, 1-4  
    obscheduled, 1-4  
    observed, 1-4  
    obt, 1-4  
    obtar, 1-4, 1-6  
    obtool, 1-2, 1-4  
    osbcvt, 1-7, 1-10, 1-11  
    probedev, 1-9, 1-22  
    stoprb, 1-7  
Oracle Secure Backup settings, configuring, 1-18,  
    1-20  
Oracle Secure Backup Web tool, 1-2, 1-18  
osbcvt program, 1-7, 1-10, 1-11  
--osbparms option, migrate2osb program, 2-10, 2-12

## P

---

PARMS parameter, 2-6, 2-8  
perform Oracle backups and restores right, 1-5  
ports, contention in mixed domains, 1-6  
positionqueryfrequency policy, 1-6  
preauthorizations, RMAN, 1-5, 1-20  
probedev program, 1-9, 1-22

## R

---

rbcleanup program, 1-4  
rbconfig file, 1-8  
rbcopy program, 1-4  
rbcv program, 1-4  
rbexec program, 1-4  
rbixd program, 1-4  
rbndmp program, 1-4  
rbnotify program, 1-4  
rbparameters file, 1-9, 1-10, 1-17  
rbrobotd program, 1-4  
rbscheduled program, 1-4  
rbserviced daemon, 1-13  
rbserviced program, 1-4  
rbt program, 1-4  
rbtar command, 1-6  
rbtar program, 1-4, 1-6  
rbtool commands  
    canceljob, 1-9  
    lsjob, 1-9  
rbtool program, 1-4, 1-9  
recovery catalog, 2-5  
Recovery Manager  
    *See* RMAN  
recovery, and restore, 1-2  
recovery, database, 1-2  
Reliety Backup daemons, stopping, 1-8, 1-13, 1-14, 1-15, 1-17  
Reliety Backup device driver, removing, 1-15  
Reliety Backup files  
    rbconfig, 1-8  
    rbparameters, 1-9, 1-10, 1-17  
Reliety Backup home, 1-8, 1-9  
Reliety Backup home directory, 1-4  
Reliety Backup processes, stopping, 1-9, 1-13  
Reliety Backup programs, 1-4  
    probedev, 1-9  
    rbcleanup, 1-4  
    rbcopy, 1-4  
    rbcv, 1-4  
    rbexec, 1-4  
    rbixd, 1-4  
    rbndmp, 1-4  
    rbnotify, 1-4  
    rbrobotd, 1-4  
    rbscheduled, 1-4  
    rbserviced, 1-4  
    rbt, 1-4  
    rbtar, 1-4, 1-6  
    rbtool, 1-9  
    stoprb, 1-14

    uninstallrb, 1-22  
Reliety Backup services, stopping on  
    Windows, 1-14, 1-15, 1-17  
Reliety Backup Web tool, 1-8, 1-9  
Reliety Backup, migrating from  
    overview, 1-6  
    preparations, 1-8  
Reliety Backup, uninstalling, 1-15, 1-17, 1-21, 1-22  
remote shell access, 1-14, 1-16  
removing Reliety Backup device driver, 1-15  
renssel command, 1-2  
--restore option, migrate2osb program, 2-12  
RESTORE VALIDATE command, 2-8, 2-9, 2-11  
restore, and recovery, 1-2  
RMAN  
    preauthorized access, 1-5, 2-6  
    tape parallelism, 2-6  
RMAN commands  
    ALLOCATE CHANNEL, 2-12  
    CONFIGURE, 2-6  
    DELETE, 2-7  
    RESTORE VALIDATE, 2-8, 2-9, 2-11  
RMAN scripts, 2-8  
rm piece command, 1-3  
rmsection command, 1-3  
rsh program, 1-14, 1-16

## S

---

SBT API, 1-2, 2-4, 2-5, 2-6, 2-8  
SCSI device information, obtaining, 1-12, 1-22  
SCSI devices, 1-9  
SCSI LUN, 1-12, 1-22, 1-23  
SCSI target ID, 1-12, 1-22  
--size option, migrate2osb program, 2-10  
stopping Reliety Backup processes, 1-9  
stoprb program, 1-7, 1-13, 1-14

## T

---

tape devices, 2-3, 2-5  
    centralized on media server, 2-4  
    configuring, 1-12, 2-4  
    supported by Oracle Secure Backup, 2-3  
tape drives, 1-5, 1-12, 2-3  
    position query frequency, 1-6  
tape libraries, 1-12, 1-22, 2-3  
    autoswap mode, 1-5  
    import/export mechanism, 1-6  
    wrap-around mode, 1-5  
TAR files, 1-15  
terminology, changes in, 1-4  
time-managed expiration policies, 1-3

## U

---

uninstalling Legato, 2-7, 2-9, 2-11, 2-12  
uninstalling Reliety Backup, 1-15, 1-17, 1-21, 1-22  
uninstallrb program, 1-22  
UNIX operating system, 1-2, 1-7, 1-8, 1-9, 1-10, 1-13, 1-14, 1-15, 1-16, 1-21, 1-22

unrmsection command, 1-3  
users, Oracle Secure Backup, 1-5

## **W**

---

Windows operating system, 1-2, 1-7, 1-8, 1-10, 1-15,  
1-16, 1-17, 1-18, 1-20, 1-22  
installing Oracle Secure Backup on, 1-15, 1-17  
stopping Reliaty Backup services, 1-14, 1-17