

Oracle® Secure Backup

Installation Guide

Release 10.1

B14235-05

October 2006

A guide to acquiring, installing, and uninstalling Oracle Secure Backup, as well as performing initial device configuration.

Oracle Secure Backup Installation Guide, Release 10.1

B14235-05

Copyright © 2006, Oracle. All rights reserved.

Primary Authors: Antonio Romero, Lance Ashdown

Contributing Authors: Rhonda Day, Randy Urbano

Contributors: Michael Chamberlain, Tony Dziedzic, Judy Ferstenberg, Ashok Joshi, Cris Pedregal-Martin, Janet Stern, Radhika Vullikanti, Joe Wadleigh, and Vinisha Dharamshi

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 USA, Inc., 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, PeopleSoft, and Siebel 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

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	viii
Conventions	viii
1 Introduction to Oracle Secure Backup	
What Is Oracle Secure Backup?	1-1
Oracle Secure Backup Interfaces	1-1
Oracle Secure Backup Administrative Domains and Host Roles	1-2
Planning Your Administrative Domain	1-4
Determining System Requirements for Oracle Secure Backup	1-4
Platforms and Operating Systems Supported by Oracle Secure Backup	1-4
Planning Disk Space Requirements for Oracle Secure Backup	1-4
Other System Requirements for Oracle Secure Backup	1-6
Linux Media Server System Requirement: SCSI Generic Driver	1-7
Choosing Roles for Hosts in Your Administrative Domain	1-8
Collecting Device Parameters for UNIX and Linux Tape Devices	1-8
Assigning Oracle Secure Backup Logical Unit Numbers to Devices	1-9
Overview of Oracle Secure Backup Installation	1-9
Overview of Installation of Oracle Secure Backup on Linux and UNIX	1-12
Acquiring Oracle Secure Backup Installation Software	1-14
Methods of Accessing the Oracle Secure Backup Installation Software	1-14
Installing Oracle Secure Backup from CD-ROM	1-15
Extracting Oracle Secure Backup from OTN Download on Linux or Solaris	1-15
Extracting Oracle Secure Backup from OTN Download on Windows	1-16
2 Installing Oracle Secure Backup on Windows	
Before You Begin	2-1
Preparing Windows Media Servers for Oracle Secure Backup Installation	2-1
Disabling Drivers on Windows-Based Media Servers	2-2
Disabling Removable Storage Service on Windows Media Servers	2-3
Do Not use STORport Miniport Drivers	2-3
Running the Oracle Secure Backup Windows Installer setup.exe	2-3
Configuring Firewalls for Oracle Secure Backup on Windows	2-13

3	Configuring a Domain and Devices on Windows	
	Configuring Libraries and Tape Drives on Windows: Overview	3-1
	About Oracle Secure Backup Logical Unit Numbers	3-2
	About Fibre Channel Shared Devices	3-2
	Configuring an Administrative Domain on Windows: Overview	3-2
	Configuring NAS Filers.....	3-3
	Assigning Oracle Secure Backup Device Names on Windows	3-4
	Taking Inventory of Tape Devices on Windows	3-6
	Configuring NAS Libraries and Tape Drives on Windows	3-6
	Making NAS Device Names Accessible to Oracle Secure Backup	3-7
4	Installing Oracle Secure Backup on Linux or UNIX	
	Preparing to Install Oracle Secure Backup on Linux and UNIX.....	4-1
	Creating the Oracle Secure Backup Home	4-2
	Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script.....	4-3
	Optional: Configuring Installation Parameters in the obparameters File	4-5
	Installing Oracle Secure Backup on Linux or UNIX with installob.....	4-6
	Running installob Again for Device Configuration or Push Installs.....	4-15
5	Configuring a Domain and Devices on Linux and UNIX	
	Determining SCSI Device Parameters on Linux and UNIX	5-1
	Determining SCSI Device Parameters on Linux.....	5-2
	Determining SCSI Device Parameters on Solaris	5-3
	Probing SCSI Target ID and LUN for Media Devices From Solaris Open Boot PROM...	5-3
	Viewing SCSI Bus Name-Instance Parameter Values in Solaris	5-4
	Configuring an Administrative Domain on Linux and UNIX with obtool	5-6
	Configuring Administrative Domain NAS Filers Using obtool.....	5-7
	Creating Device Special Files on Solaris and Linux.....	5-8
	Creating Device Special Files with makedev	5-8
	Creating Device Special Files with installob	5-10
	Configuring SCSI Devices on Solaris with installob.....	5-10
	Configuring SCSI Devices on Linux with installob	5-14
	Configuring Devices on Linux and UNIX with obtool.....	5-18
	Taking Inventory of Devices on Linux and UNIX	5-19
	Configuring NAS Libraries and Tape Drives on Linux and UNIX	5-20
	Making NAS Device Names Accessible to Oracle Secure Backup	5-20
6	Uninstalling Oracle Secure Backup	
	Uninstalling Oracle Secure Backup on Windows.....	6-1
	Uninstalling Oracle Secure Backup on Linux or UNIX.....	6-1
A	Oracle Secure Backup Directories and Files	
	Oracle Secure Backup Home Directory	A-1
	Oracle Secure Backup Configuration File.....	A-1
	Administrative Server Directories and Files.....	A-2

Media Server Directories and Files.....	A-4
Client Host Directories and Files	A-5

B Oracle Secure Backup obparameters Installation Parameters

customized obparameters	B-1
start daemons at boot	B-2
create pre-authorized oracle user	B-2
default UNIX user	B-2
default UNIX group	B-2
identity certificate key size.....	B-3
<os-name> ob dir.....	B-3
<os-name> db dir	B-4
<os-name> temp dir.....	B-4
<os-name> links	B-4
ask about ob dir	B-5
default protection	B-5
run obopenssl.....	B-6

C Manually Configuring UNIX Drivers

Installing the Oracle Secure Backup Device Driver Manually	C-1
Installing the Driver on Solaris 2.8 and Later	C-2
Uninstalling the Oracle Secure Backup Device Driver Manually.....	C-2
Manually Uninstalling the Oracle Secure Backup Driver on Solaris.....	C-3

Index

Preface

This Preface contains these topics:

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

Audience

The *Oracle Secure Backup Installation Guide* is intended for system administrators and database administrators who install the Oracle Secure Backup software. These administrators might also perform backup and restore operations. To use this document, you need to be familiar with the operating system environment on which you plan to use Oracle Secure Backup. To perform Oracle database backup and restore operations, you should also be familiar with Oracle Secure Backup and Recovery and Recovery Manager concepts.

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 backing up and restoring file systems with Oracle Secure Backup, see the following Oracle resources:

- *Oracle Secure Backup Migration Guide*
This book explains how to migrate from Reliaty Backup to Oracle Secure Backup.
- *Oracle Secure Backup Administrator's Guide*
This book contains information about configuring and running the Oracle Secure Backup Web tool.
- *Oracle Secure Backup Reference*
This manual contains information about the command-line interface for Oracle Secure Backup.
- *Oracle Secure Backup Administrator's Guide*
This book describes how to use Oracle Secure Backup to perform backup and restore operations. The book is oriented to the Oracle Secure Backup Web tool, which is a Web-based GUI interface.

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/secure-backup>

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

<http://www.oracle.com/technology/software>

Conventions

The following text conventions are used in this document:

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

Introduction to Oracle Secure Backup

This chapter provides an introduction to Oracle Secure Backup and includes advice on planning and configuring your administrative domain.

This chapter includes the following sections:

- [What Is Oracle Secure Backup?](#)
- [Planning Your Administrative Domain](#)
- [Overview of Oracle Secure Backup Installation](#)
- [Acquiring Oracle Secure Backup Installation Software](#)

See Also: *Oracle Secure Backup Administrator's Guide* for conceptual information about Oracle Secure Backup

What Is Oracle Secure Backup?

Oracle Secure Backup enables reliable data protection through file system backup to tape. It supports the major tape drives and libraries in SAN, Gigabit Ethernet, and SCSI environments using standard tape formats.

As part of the Oracle storage solution, it reduces complexity and minimizes the need to purchase additional software. Oracle Secure Backup provides scalable distributed backup and recovery capabilities, and it lowers software cost by:

- Integrating with the Oracle stack for maximum ease of use in a single Oracle solution to protect your data from disk to tape
- Employing single vendor technical support for database and file system backup and recovery to tape
- Utilizing existing or new hardware with Oracle Secure Backup's broad tape device support in SCSI, GbE, and SAN environments with dynamic drive sharing for maximum drive utilization

Oracle Secure Backup also eliminates integration challenges with ready-to-use tape management software that provides single vendor support. When using Oracle Secure Backup in conjunction with Recovery Manager (RMAN) to back up and recover databases and files to and from tape, no other tape management software is required. Centralized administration, heterogeneous network support, and flexible scheduling simplify and automate the protection of the Oracle environment.

Oracle Secure Backup Interfaces

You can interact with Oracle Secure Backup by means of the following tools:

- Oracle Secure Backup Web tool
The Oracle Secure Backup Web tool is an online graphical user interface that enables you to configure administrative domains, manage operations, browse the backup catalog, and back up and restore data.
- Oracle Secure Backup command-line interface
Oracle Secure Backup provides you with a command-line interface as an alternative to the Web tool. You can take advantage of an extensive online help system for determining command options.
- Oracle Enterprise Manager
Oracle Enterprise Manager is a set of systems management tools for managing the Oracle environment. Enterprise Manager provides a graphical interface to Oracle Secure Backup that can be used to perform database backup and restore operations in conjunction with RMAN.

See Also: *Oracle Enterprise Manager Administrator's Guide* and the online help to learn how to use Enterprise Manager

Oracle Secure Backup Administrative Domains and Host Roles

To oversee data protection activities among diverse hosts, devices, and databases, Oracle Secure Backup defines an administrative domain. An administrative domain is a collection of hosts under the direction of an administrative server.

Each host can play one or more of the following roles in an administrative domain:

- Administrative server
Each administrative domain must have exactly one administrative server. This server stores data pertinent to the operation of the administrative domain in a set of configuration files. Metadata relating to backup and restore operations is also stored on the administrative server in a backup catalog.
The administrative server runs the scheduler, which starts and monitors jobs within the administrative domain.
The disk storage required by Oracle Secure Backup on the administrative server depends on how much data you back up as well as your backup schedules.
See Also: "[Planning Disk Space Requirements for Oracle Secure Backup](#)" on page 1-4 for more information about disk storage requirements
- Media server
A media server has one or more secondary storage devices, such as a library and tape drives, connected to it. At a minimum, a media server must have one standalone tape drive. Many media servers utilize robotic tape libraries.
A media server transfers data to or from volumes loaded on these devices. During installation, you can configure multiple secondary storage devices on media servers.
- Client
A client host is a host that has locally-accessed data that is backed up or restored by Oracle Secure Backup. Any host where Oracle Secure Backup is installed, or that contains data that Oracle Secure Backup accesses through Network Data

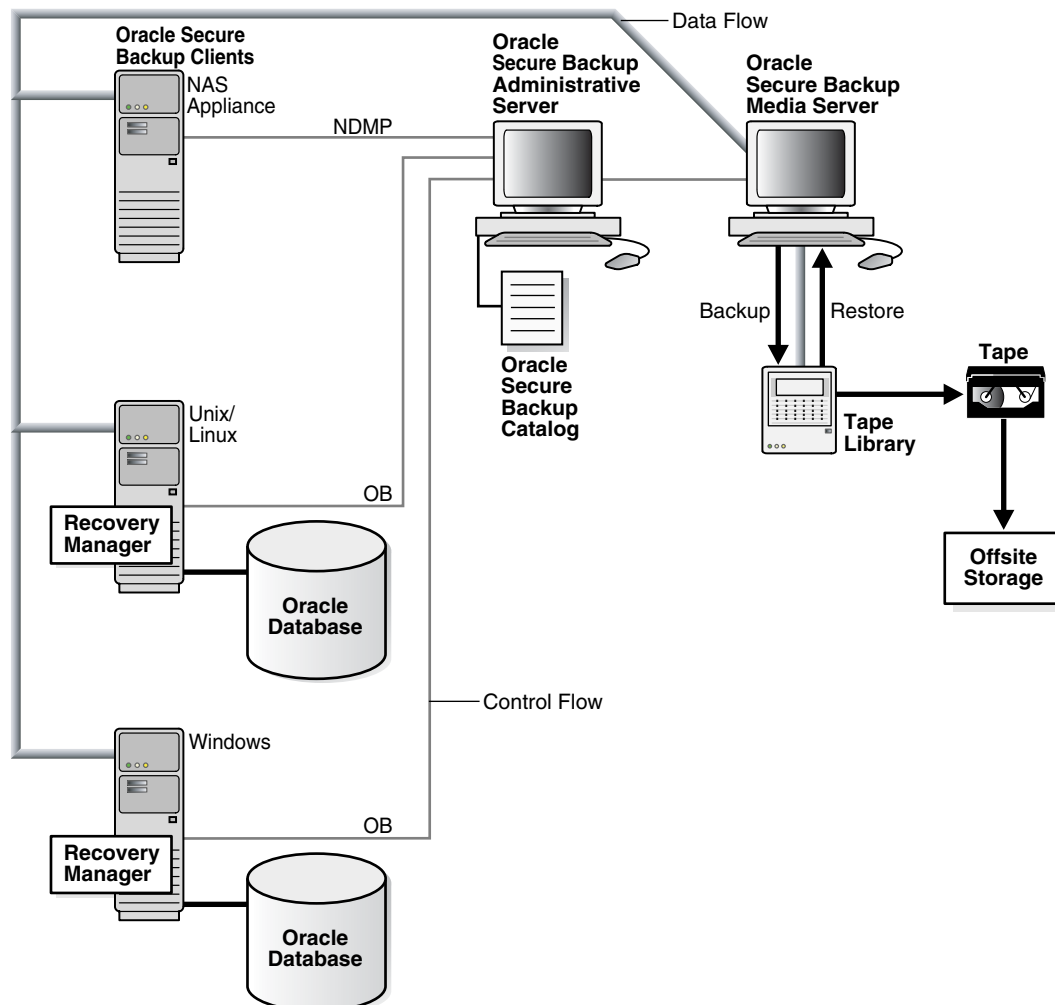
Management Protocol (NDMP), can act as a client. Each client host is associated with one administrative server.

Most hosts defined within the administrative domain are clients. Client hosts typically store data in an Oracle database or in local file systems.

You must install Oracle Secure Backup on your administrative server and on each of the media servers and client hosts in your administrative domain. During installation, the installation software asks you to specify the roles played by the different hosts. Typically, an administrative domain includes an administrative server, one or more media servers, and one or more client hosts.

Figure 1-1 shows a possible Oracle Secure Backup administrative domain that includes three client hosts, one administrative server, and one media server. RMAN can back up database files to tape through the Oracle Secure Backup SBT interface; Oracle Secure Backup can back up files on the file system to tape.

Figure 1-1 Oracle Secure Backup Administrative Domain



See Also: *Oracle Secure Backup Administrator's Guide* for a comprehensive conceptual overview of Oracle Secure Backup

Planning Your Administrative Domain

Before installing Oracle Secure Backup and configuring your domain, you must perform the planning tasks described in this section:

- [Determining System Requirements for Oracle Secure Backup](#)
- [Choosing Roles for Hosts in Your Administrative Domain](#)
- [Collecting Device Parameters for UNIX and Linux Tape Devices](#)

Determining System Requirements for Oracle Secure Backup

This section contains the following topics:

- [Platforms and Operating Systems Supported by Oracle Secure Backup](#)
- [Planning Disk Space Requirements for Oracle Secure Backup](#)
- [Other System Requirements for Oracle Secure Backup](#)

Platforms and Operating Systems Supported by Oracle Secure Backup

For the list of supported operating systems, web browsers and NAS for Oracle Secure Backup, see Certify on Metalink, at the following URL:

<http://metalink.oracle.com/>

Tape device matrixes are available at the following URL:

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

Planning Disk Space Requirements for Oracle Secure Backup

To help you manage your installation, hardware and software capacity planning values are provided for Oracle Secure Backup on the Windows, UNIX, and Linux operating systems. In addition to considering the space you need for Oracle Secure Backup, evaluate the size requirements of your network as a whole. Factors such as the number of hosts on the network and the volume of backups and restores you plan to perform significantly affect resource requirements.

Although no strict rules exist for determining the exact amount of disk space required for any particular network, consider the following general guidelines:

- One backup catalog exists for each client host.
- No appreciable backup catalog data are recorded for database backups.
- The size of the backup catalog of any client is a direct function of the following:
 - Number of files and directories backed up
 - Frequency of backups and ratio of full to incremental backups
 - Length of file names
 - Depth of directory trees
 - Frequency at which position data is sampled
 - Frequency at which statistical data for a file changes, irrespective of whether that file is backed up in full or incremental mode
 - Maximum retention period of backup catalog data, if configured
 - Rate at which backup media are recycled

- Number of backups retained in the catalog for the clients

On any operating system, when an administrative server is installed, the files for a media server and client are included automatically, even if they are not installed.

The following sections provide approximate disk space requirements for the Oracle Secure Backup software on the Windows, UNIX, and Linux operating systems. The values specified are approximations only and may vary by installation. Also, the disk space requirements do not include the required space for backup catalogs and for log files that are generated by Oracle Secure Backup. Backup catalogs and log files can require considerable additional disk space.

Disk Space Requirements for Oracle Secure Backup on Windows Table 1–1 describes the disk space required for an installation of Oracle Secure Backup on Windows with and without the administrative server.

Table 1–1 Disk Space Requirements for Oracle Secure Backup on Windows

Oracle Secure Backup Installation	Disk Space
Administrative server (can include the media server or client, or both)	50 MB
Media server or client, or both (no administrative server)	40 MB

Disk Space Requirements for Oracle Secure Backup on Linux and UNIX When you install Oracle Secure Backup on Linux or UNIX, you load an install package for a particular operating system and perform the installation with the install package. You also have the option of loading Oracle Secure Backup install packages for multiple operating systems. These packages enable you to initiate the installation of Oracle Secure Backup to other hosts in the network. Typically, install packages that will be used for network installations are loaded onto an administrative server.

Table 1–2 describes the disk space requirements for installing an administrative server, media server, and client on Linux and UNIX. This table also describes the disk space requirements for loading install packages that will be used for network installations to other hosts.

Table 1–2 Disk Space Requirements for Oracle Secure Backup on Linux and UNIX

Oracle Secure Backup Installation and Packages	Disk Space
Administrative server for UNIX installation (can include the media server or client, or both)	60 MB
Administrative server for Linux x86 installation (can include the media server or client, or both)	40 MB
Administrative server for Linux x86-64 and Linux Itanium installation (can include the media server or client, or both)	120 MB
Administrative server for HP-UX PA-RISC (64-Bit) installation (can include the media server or client, or both)	670 MB
Common administrative server files for all operating systems	10 MB
Each copy of an install package loaded for network installations to other hosts running UNIX operating systems	60 MB
Package files loaded for network installations to other hosts running the Linux operating system	40 MB
Media server or client, or both	50 MB

To calculate the amount of disk space required for a host that will function as both an administrative server and as a server for network installations to other hosts, add the following disk space requirements to determine the total disk space required:

- The amount of disk space required to install the administrative server locally
- The amount of disk space required for install packages for other operating systems
- 10 MB for common administrative server files that are used for all operating systems

The following examples describe the disk space requirements for various installations of Oracle Secure Backup on Linux or UNIX:

- Install the administrative server for the Solaris 64 operating system, and load the install packages for the Linux operating system for network installations to other hosts:

```
60 MB (administrative server installation for Solaris 64)
40 MB (install package for Linux x86)
10 MB (common administrative server files)
110 MB total disk space required
```

- Install the administrative server, media server, and client for the Linux operating system without loading install packages for other operating systems:

```
40 MB (administrative server, media server, and client for Linux x86)
10 MB (common administrative server files)
50 MB total disk space required
```

- Network install of a media server and client on the Solaris 64 operating system:

```
200 MB total disk space required
```

- Network install of a client on the Linux x86 operating system:

```
50 MB total disk space required
```

Note: The restartable backups feature, supported by some backup devices such as those from Network Appliance, generate bulkfiles in /tmp on a Linux or UNIX administrative server that can require considerable extra space. If you are using this feature, you should maintain at least 1GB of free disk space on the file system that contains /tmp.

Other System Requirements for Oracle Secure Backup

The following requirements also apply for Oracle Secure Backup installations:

- Each host that participates in a Oracle Secure Backup administrative domain must run TCP/IP. Oracle Secure Backup uses this protocol for all inter- and intra-machine communication between its own and other system components.
- Each appliance that employs a closed operating system, such as Network Attached Storage (NAS) and tape servers, must run NDMP. This protocol enables Oracle Secure Backup to access primary and secondary storage controlled by the appliance. Oracle Secure Backup supports NDMP versions 2, 3, and 4, and various extensions to version 4. It automatically negotiates with other, non-Oracle NDMP components to select a mutually agreeable protocol version. Between its own components, Oracle Secure Backup uses NDMP version 4.

- Each host that participates in an Oracle Secure Backup administrative domain must also have some preconfigured way to resolve a host name to an IP address. Most systems use one of the name resolution mechanisms (DNS, NIS, WINS, or a local "hosts" file) to do this. Oracle Secure Backup does not require a specific mechanism. Oracle Secure Backup only requires that, upon presenting the underlying system software with an IP address you have configured, it obtains an IP address corresponding to that name.

Note:

- You can configure Oracle Secure Backup to use WINS, the Microsoft Windows name resolution protocol, from UNIX hosts. Although this configuration is atypical, WINS name resolution from UNIX hosts can be a practical solution.
 - The use of DHCP to assign IP addresses is not supported for hosts that participate in an Oracle Secure Backup administrative domain. Static IP addresses should be assigned to all hosts. If you cannot use static IP addresses, you must ensure that the DHCP server guarantees that a given host is always assigned the same IP address.
 - On OSB network installations, it is important that there be no duplicate host names. Index catalog data is stored in a directory based on the name of the client host. Duplicate host names would result in information related to backups from multiple clients being combined in a manner that could prevent successful restores from backup.
-
-

See Also: *Oracle Secure Backup Administrator's Guide* for information about using WINS name resolution from UNIX hosts with Oracle Secure Backup

Linux Media Server System Requirement: SCSI Generic Driver

Configuring a Linux host for the Oracle Secure Backup media server role requires that the SCSI Generic driver be installed on that host. This driver is required for Oracle Secure Backup to interact with media devices. The host must also be configured to automatically reload the driver after a reboot.

Kernel modules are usually loaded directly by the facility that requires them, if the correct settings are present in the `/etc/modprobe.conf` file. However, it is sometimes necessary to explicitly force the loading of a module at boot time.

For example, on RedHat Enterprise Linux, the module for the SCSI Generic driver is named `sg`. Red Hat Enterprise Linux checks for the existence of the `/etc/rc.modules` file at boot time, which contains various commands to load modules.

Note: The `rc.modules` should be used, and not `rc.local`, because `rc.modules` is executed earlier in the boot process.

The following commands can be used to add the `sg` module to the list of modules configured to load as `root` at boot time:

```
# echo modprobe sg >> /etc/rc.modules
```

```
# chmod +x /etc/rc.modules
```

Choosing Roles for Hosts in Your Administrative Domain

When planning your administrative domain, you must designate the specific role or roles for each host. You should ask the following questions:

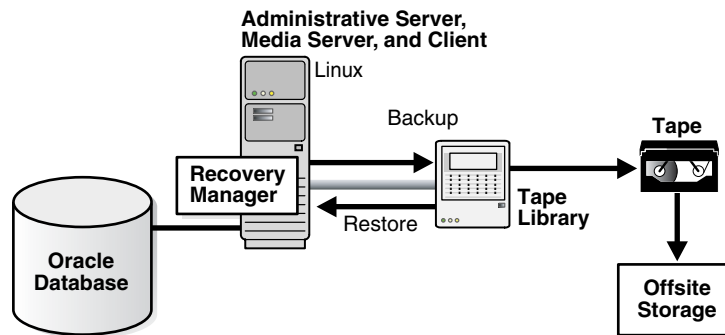
- Which host will you use to initiate and manage backup and restore jobs? Assign this host the role of administrative server.
- Which hosts have tape or other secondary storage devices attached to them? Assign these hosts the role of media server.
- Which hosts in your network have data that needs to be backed up? Assign these hosts the role of client.

Note that a single host can serve several roles. For example, if you want to use a host to administer your backups that also contains data to be backed up, assign that host the roles of administrative server and client. If a host to be backed up has attached devices, then assign the host the roles of client and media server.

Note: All hosts possessing data to be backed up must be assigned the client role, regardless of other roles assigned to that host.

As shown in [Figure 1-2](#), a domain can consist of a single host which is administrative server, media server, and client.

Figure 1-2 Administrative Domain with One Host



Collect a list of each host in your administrative domain and which roles are assigned to each one. Then verify that each host meets the system requirements for Oracle Secure Backup for that role. Oracle Secure Backup must be installed on each host in your domain except NDMP-enabled hosts such as NAS filers.

Collecting Device Parameters for UNIX and Linux Tape Devices

Installing and configuring Oracle Secure Backup on Linux media servers with attached media devices requires the SCSI configuration parameters for all attached tape drives or libraries, as well as the creation of device special files for each device.

Obtain SCSI bus instance names, target IDs, and SCSI logical unit numbers (LUNs) by using operating system-specific utilities for media servers running Oracle Secure Backup on Linux and UNIX operating systems.

Note: It is not necessary to collect SCSI parameter information for devices attached to Windows media servers. Windows correctly determines SCSI parameters for the tape drives and tape libraries automatically.

See Also: ["Determining SCSI Device Parameters on Linux and UNIX"](#) on page 5-1 for details on collecting SCSI parameters under Linux or UNIX

Assigning Oracle Secure Backup Logical Unit Numbers to Devices

In addition to obtaining SCSI device information, tape drives and libraries must be assigned an Oracle Secure Backup logical unit number during the configuration process. This number is used to generate unique device names during device configuration.

For UNIX or Linux media servers, you must select Oracle Secure Backup logical unit numbers for each device as part of planning your administrative domain.

Note: It is not necessary to assign Oracle Secure Backup logical unit numbers for devices attached to Windows media servers. On Windows, Oracle Secure Backup logical unit numbers are assigned as needed automatically.

While there is no required order for assigning Oracle Secure Backup logical unit numbers, they are typically assigned sequentially, starting at 0, for each device of a given type, whether library or drive. That is, libraries are typically numbered 0, 1, 2 and so on, and tape drives are also numbered 0, 1, 2 and so on. The maximum value for an Oracle Secure Backup logical unit number is 31.

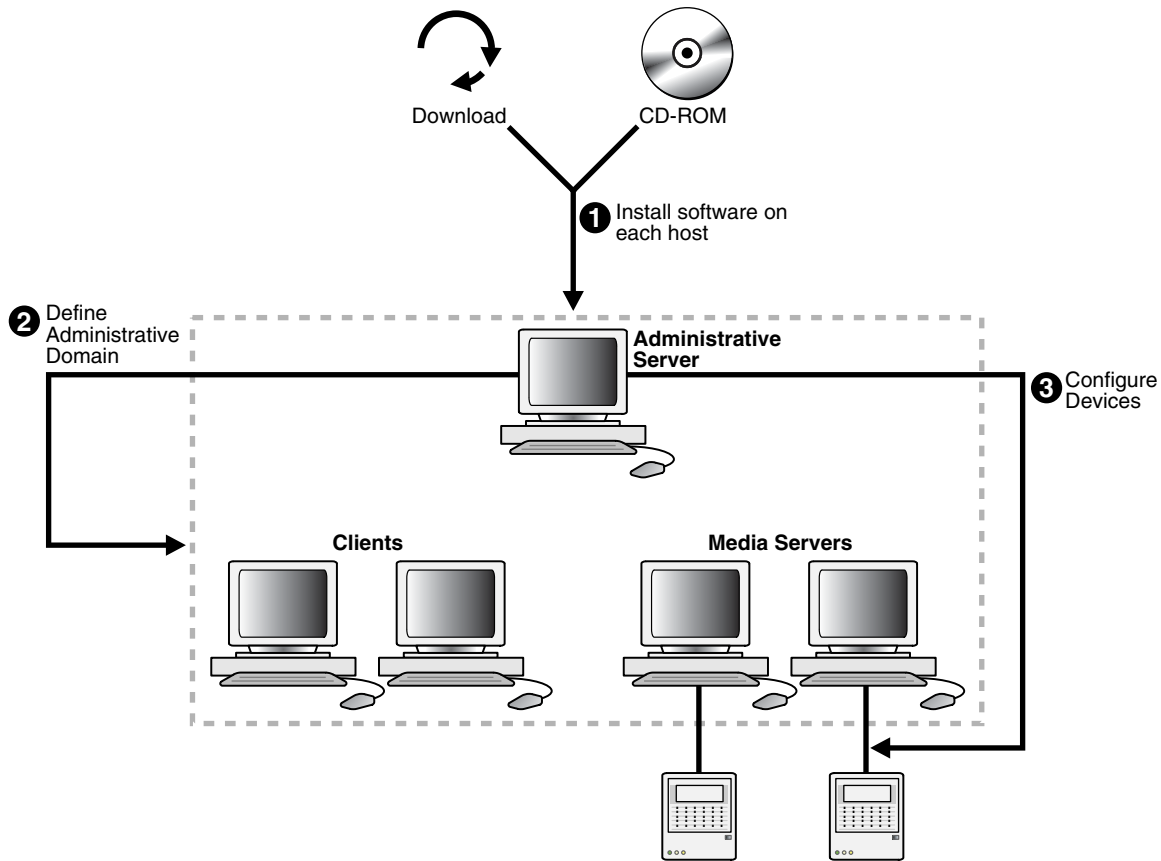
On Linux or Solaris, the resulting device special file names for tape libraries are `/dev/ob11`, `/dev/ob12`, `/dev/ob13` and so on, and the names for tape drives are `/dev/obt1`, `/dev/obt2`, `/dev/obt3` and so on through `/dev/obtn`, where *n* in each case is the Oracle Secure Backup logical unit number you assigned the device. On Windows, the resulting tape library names are `ob11`, `ob12`, `ob13` and so on, and the names for tape drives are `obt1`, `obt2`, `obt3` and so on, where these names are assigned automatically during the installation of Oracle Secure Backup on Windows. (Note that the 1 character in the name of each tape drive is a lower-case L, not a numeral 1.)

Note: The Oracle Secure Backup logical unit number should not be confused with the SCSI logical unit number (SCSI LUN). The SCSI LUN is part of the hardware address of the device, while the Oracle Secure Backup logical unit number is part of the device special file name.

Overview of Oracle Secure Backup Installation

After you have completed the tasks in ["Planning Your Administrative Domain"](#) on page 1-4, you are ready to install the software and configure your administrative domain. [Figure 1-3](#) illustrates the basic process, which can be used on any combination of Linux, UNIX and Windows hosts.

Figure 1-3 Installing Oracle Secure Backup



You can perform the installation and configuration in the following steps:

1. Plan your administrative domain, including:
 - Determine which hosts are assigned each role
 - For Linux-based media servers, collect device information such as SCSI parameters for tape libraries and drives
2. Install the Oracle Secure Backup software on each Windows, UNIX or Linux host in your administrative domain, *except* for any hosts which will run NDMP daemons from other vendors, such as NDMP-enabled NAS filers.

Note:

- During installation on each host, specify the roles you assigned in Step 1 when prompted.
 - Before installation on Windows media servers, disable existing device drivers for tape drives and libraries so that the Oracle Secure Backup device driver can manage these devices. This enables Oracle Secure Backup for Windows to determine SCSI device parameters automatically during installation.
 - For Linux or UNIX installation on media servers, you can enter SCSI device parameters for your tape drives and libraries during installation, or as a separate task performed immediately after installation.
 - During installation on a host designated as administrative server, an administrative domain is created on that host. At this point it contains no information about hosts other than the administrative server.
-
-

See Also: [Chapter 2, "Installing Oracle Secure Backup on Windows"](#) and [Chapter 4, "Installing Oracle Secure Backup on Linux or UNIX"](#) for installation and device configuration instructions specific to each platform

3. Log in to the administrative server and add media server hosts and clients to the administrative domain.

["Configuring an Administrative Domain on Windows: Overview"](#) on page 3-2 and ["Configuring an Administrative Domain on Linux and UNIX with obtool"](#) on page 5-6 explain how to perform this task.

4. Configure the administrative domain with information about media devices on each media server added in Step 3.

Configure the SCSI and Fibre Channel libraries and tape drives directly attached to each Oracle Secure Backup media server in your administrative domain, and discover the libraries and tape drives attached to NAS filers so that they are included in the domain.

Note: Oracle Secure Backup takes advantage of pass-through device drivers on most operating systems. For operating systems with special requirements, you can install Oracle Secure Backup device drivers.

See Also: [Chapter 3, "Configuring a Domain and Devices on Windows"](#) and [Chapter 5, "Configuring a Domain and Devices on Linux and UNIX"](#) for details on configuring your administrative domain to recognize your media devices.

5. Once the administrative server and media servers are configured successfully, install Oracle Secure Backup on the hosts that play only the client role if you have not already done so, and add them to the administrative domain.

Overview of Installation of Oracle Secure Backup on Linux and UNIX

Oracle Secure Backup on Linux or UNIX is performed in three phases:

- **Loading** (performed by a script called `setup`), in which files required for installing Oracle Secure Backup on one or more different Linux or UNIX platforms are staged on the administrative server, in a directory called the **Oracle Secure Backup home**.
- **Installing** (performed by a script called `installob`), in which Oracle Secure Backup executables are deployed on individual Linux or UNIX hosts.

Note: On media servers, `installob` also performs some device configuration tasks, including installation of a required device driver on Solaris, and, optionally, creation of device special files required for Oracle Secure Backup to access the media devices.

- Optionally, **SCSI device configuration** on media servers, which involves creation of device special files on media servers to allow the Oracle Secure Backup device driver to access the media devices. You need the SCSI device information collected in "[Collecting Device Parameters for UNIX and Linux Tape Devices](#)" on page 1-8 to perform this task.

Note: This is properly speaking a configuration task, but as a convenience the `installob` script can prompt for the necessary information and perform the configuration process during initial Linux or UNIX installation or in a later session. Until this task is performed, Oracle Secure Backup cannot access media devices.

Remote or Push Installation of Oracle Secure Backup on Linux and UNIX

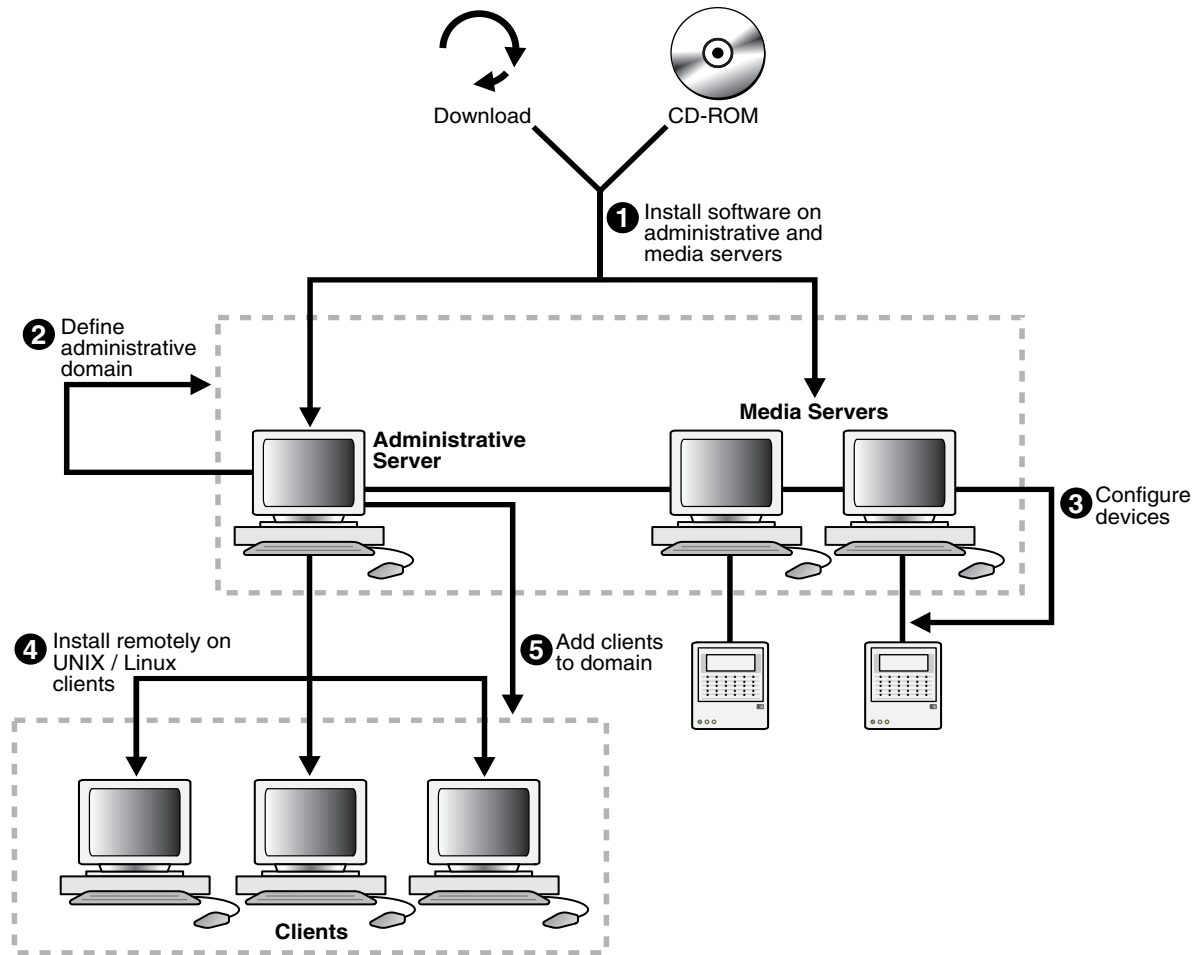
After installing on a Linux or UNIX administrative server, the `installob` script can be used to **push** software across the network directly from the administrative server to Linux or UNIX clients or media servers in what is called a **remote installation** or **push installation**. In a remote installation `installob` copies the installation files required for the destination platform across the network, then uses `rsh` to send commands to the destination host that perform the installation and configuration.

Note: This distribution method requires that administrators be able to issue the `rsh` command as `root` without a password on the destination host. Configuring your Linux and UNIX clients to permit this form of access presents security issues.

Also, if support for `rsh` as `root` without a password is not part of your normal host configuration, you must configure each host to accept commands this way before the push installation, and then disable this capability when installation is complete.

Figure 1–4 illustrates local installation on the administrative server and media servers in an administrative domain, and push installation onto hosts that play the client role only.

Figure 1–4 Installing Oracle Secure Backup on Linux and UNIX



In this scenario the steps in the installation process are as follows:

1. Load and install the Oracle Secure Backup software only on the administrative server and media servers.

When running `setup` on the administrative server host, load the installation packages for all UNIX or Linux operating systems used in your administrative domain onto the server. Also, when running `installob` on the media servers, install and configure the Oracle Secure Backup device drivers and create device special files on each host.

2. Log in to the administrative server, and add the media servers to the administrative domain.

Perform this task directly on the administrative server, which is automatically defined during the software installation in the preceding step.

3. Make the administrative server aware of tape devices in your domain.

This step involves media servers only. Configure the SCSI and Fibre Channel libraries and tape drives directly attached to an Oracle Secure Backup host in your administrative domain, if you have not already done so, and configure the administrative domain with information about the tape devices attached to each media server. Also, discover the libraries and tape drives attached to a NAS filer so that the filer can communicate with Oracle Secure Backup.

4. Perform the push installation process from the administrative server to the Linux or UNIX clients. Run `installob` on the UNIX or Linux administrative server again, and follow the prompts to install Oracle Secure Backup on other hosts.
5. Log in to the administrative server and configure the administrative domain with information about the clients.

Acquiring Oracle Secure Backup Installation Software

This section explains how to acquire installation media for Oracle Secure Backup from a Web download or on CD-ROM.

Note: The contents of the CD-ROM and download archive are identical. Each one contains the complete set of files required for installation on all supported operating systems.

This section contains the following topics:

- [Methods of Accessing the Oracle Secure Backup Installation Software](#)
- [Extracting Oracle Secure Backup from OTN Download on Linux or Solaris](#)
- [Extracting Oracle Secure Backup from OTN Download on Windows](#)

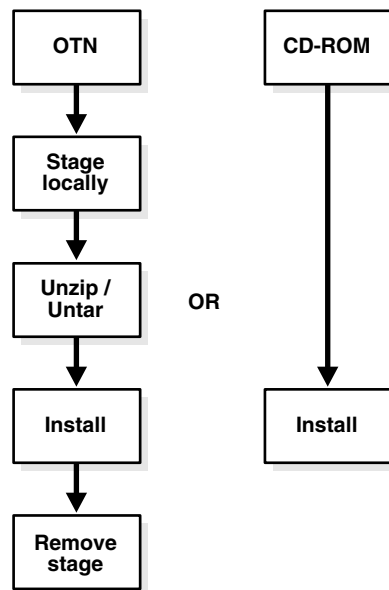
Methods of Accessing the Oracle Secure Backup Installation Software

Oracle Secure Backup can be installed from CD-ROM, or from an installation archive downloaded from the Oracle Technology Network (OTN) Web site for Oracle Secure Backup:

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

If you download the software from OTN, then you must store the downloaded file in a temporary directory, then extract the contents of the installation file, as described in the following sections.

[Figure 1–5](#) illustrates the two methods for accessing Oracle Secure Backup software in preparation for installation.

Figure 1-5 Accessing the Oracle Secure Backup Software

Note: If you use a remote installation on Linux or UNIX, as described in "[Remote or Push Installation of Oracle Secure Backup on Linux and UNIX](#)" on page 1-12, then you do not need to make installation media available on hosts that are the destination for remote installation.

Installing Oracle Secure Backup from CD-ROM

If you have Oracle Secure Backup installation media as a CD-ROM, then insert the CD-ROM into your CD drive and if necessary, mount the CD on UNIX or Linux. Then, depending upon your platform, proceed to [Chapter 2, "Installing Oracle Secure Backup on Windows"](#) or [Chapter 4, "Installing Oracle Secure Backup on Linux or UNIX"](#) for installation instructions.

Extracting Oracle Secure Backup from OTN Download on Linux or Solaris

To download and extract the Oracle Secure Backup installation software:

1. Log on to your host as a user with `root` privileges.
2. Create a temporary directory called `osbdownload` on a file system with enough free space to hold the downloaded installation file. For example, enter the following command:

```
mkdir /tmp/osbdownload
```

3. Open a Web browser and navigate to the Oracle Secure Backup web site on Oracle Technology Network (OTN):

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

4. Find the download link for Oracle Secure Backup, and follow the download instructions to download the Zip file to your temporary directory.

For this example, assume that the downloaded file is named `osb_10_1cdrom.zip`.

5. Extract the contents of the Zip file in the temporary directory. For example:

```
$ cd /tmp/osbdownload
$ unzip osb_10_1cdrom.zip
```

By default, the Zip file contents are extracted to a directory whose name is identical to the name of the Zip file, except without the `.zip` extension. For this example, assume that the contents are extracted into a subdirectory `/tmp/osbdownload/osb_10_1cdrom`.

The contents of this directory are the same as the top-level directory contents on physical installation media such as a CD. You can list these files with the `ls` command. For example:

On Linux x86, Windows, Solaris Operating System (SPARC 64-Bit)

```
$ ls /tmp/osbdownload/osb_10_1cdrom
autorun.inf  doc.tar  obreadme.pdf  setup.exe  winx86
cdtools     install.tar  osb.10.1.060420.rel  solaris64
doc         linux32  setup         welcome.html
```

Note: Installation files for Linux x86, Windows, Solaris Operating System (SPARC 64-Bit) are in a single bundle. Therefore, even on Linux x86 or Solaris Operating System (SPARC 64-Bit) platforms, you will see installation files for Windows platforms, such as `autorun.inf` and `setup.exe`.

On Linux x86-64

```
$ ls /tmp/osbdownload/osb_10_1cdrom
cdtools  install.tar  linuxx64060419.rel  setup
doc      linux86_64  obreadme.pdf        welcome.html
```

On Linux Itanium

```
$ ls /tmp/osbdownload/osb_10_1cdrom
cdtools  install.tar  linuxia64060419.rel  setup
doc      linuxia64   obreadme.pdf        welcome.html
```

On HP-UX PA-RISC (64-Bit)

```
$ ls /tmp/osbdownload/osb_10_1cdrom
cdtools  install.tar  hp64pa060419.rel  setup
doc      hp64pa     obreadme.pdf      welcome.html
```

You are now ready to install the software. See [Chapter 4, "Installing Oracle Secure Backup on Linux or UNIX"](#) for details.

Extracting Oracle Secure Backup from OTN Download on Windows

To download and extract the Oracle Secure Backup installation software on Windows

1. Log on to your host as a user with Administrator privileges.
2. In Windows Explorer, create a temporary folder called `osbdownload` on a file system with enough free space to hold the downloaded installation file.
3. Open a Web browser and navigate to the Oracle Secure Backup web site on Oracle Technology Network (OTN):

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

4. Find the download link for Oracle Secure Backup, and follow the download instructions to download the Zip file to your temporary directory.

For this example, assume that the downloaded file is named `osb_10_1cdrom.zip`.

5. Extract the contents of the Zip file into a subdirectory with the same name as the Zip file, with the `.zip` extension removed.

Note: Windows XP and Windows Server 2003 contain integrated support for exploring and extracting compressed Zip files. Windows 2000, however, requires a third party utility to extract Zip file contents. WinZip is one frequently used commercial product. There are also freeware and open source alternatives available. When extracting the Zip file contents, be sure to preserve the directory structure of files within the Zip file.

On Windows XP or Windows Server 2003, perform the following steps:

1. Right-click the file, choose **Open With**, then choose **Compressed (zipped) Folders**.
2. In Folder Tasks, click **Extract All Files** to start the Compressed (zipped) Folders Extraction Wizard.
3. Click **Browse**, and select the folder where the Zip file was downloaded as the destination for the extracted files.
4. Click **Next** to extract the files.

When the extraction is complete, the temporary folder contains a new subfolder named `osb_10_1cdrom`. The contents of the new subfolder are the same as the top-level directory contents on a physical installation CD. You can use Windows Explorer to view the contents of the folder.

Note: Installation files for all platforms are included in the download. Thus, even on Windows platforms, you will see installation files for Solaris and Linux platforms.

You are now ready to install the software. [Chapter 2, "Installing Oracle Secure Backup on Windows"](#) explains how to perform this task.

Installing Oracle Secure Backup on Windows

This chapter explains how to install Oracle Secure Backup on hosts that run the Windows operating system.

This chapter covers the following topics:

- [Before You Begin](#)
- [Preparing Windows Media Servers for Oracle Secure Backup Installation](#)
- [Running the Oracle Secure Backup Windows Installer setup.exe](#)
- [Configuring Firewalls for Oracle Secure Backup on Windows](#)

Before You Begin

Perform the following actions before you begin:

- Decide which roles to assign the hosts in your network, as described in "[Planning Your Administrative Domain](#)" on page 1-4.
- Ensure that each host has a network connection and runs TCP/IP.
- If you are installing Oracle Secure Backup on a media server, physically attach the libraries and drives (if any) that you intend to make available for use by Oracle Secure Backup. Reboot the media server if required.
- For hosts that are to be used in the media server role, follow the procedures in "[Preparing Windows Media Servers for Oracle Secure Backup Installation](#)" on page 2-1 to prevent conflicts between Oracle Secure Backup and other software on your system.
- Log on to your host as either the Administrator user or as a user that is a member of the Administrators group.

Note: If you are installing Oracle Secure Backup in an Oracle Real Application Clusters (RAC) environment, then you must install Oracle Secure Backup on each node in the cluster.

Preparing Windows Media Servers for Oracle Secure Backup Installation

Preparing Windows hosts for Oracle Secure Backup installation requires the following steps:

- [Disabling Drivers on Windows-Based Media Servers](#)
- [Disabling Removable Storage Service on Windows Media Servers](#)

Note: These steps are only required for hosts that are configured for the media server role.

Disabling Drivers on Windows-Based Media Servers

Before installing Oracle Secure Backup on hosts configured for the media server role, you must disable any existing drivers for tape drives and libraries that you intend to use with Oracle Secure Backup. These drivers conflict with the Oracle Secure Backup device driver used to support these devices.

To disable tape drive and library device drivers on Windows platforms:

1. From the Control Panel, click **System**.
2. Click the **Hardware** tab.
3. Click **Device Manager** to launch the Device Manager window.

If no tape libraries are attached to your system, skip to Step 8.

If a tape library is attached to your system, continue to Step 4.

4. Select **Medium Changers** from the navigation tree.

Note: Medium Changer devices are only displayed in the Device Manager window if a library is attached to the system.

5. Select the icon that represents your library and right-click with your mouse. A menu appears.
6. Disable the medium changer driver.
On Windows 32-bit, select **Disable**.
On Windows Itanium and Windows x64, select **Uninstall**.
7. Repeat steps 5 and 6 for each medium changer that appears in the expanded list.
8. Select **Tape Drives** from the navigation tree to display installed drivers for tape drives.

Note: If **Tape Drives** is not in the navigation tree, then your tape drive may be listed in the navigation tree under **Other Devices** instead.

9. Select the icon that represents your tape drive and right-click with your mouse. A menu appears.
10. Disable the tape drive driver.
On Windows 32-bit, select **Disable**.
On Windows Itanium and Windows x64, select **Uninstall**.
11. Repeat steps 9 and 10 for each tape drive.
12. Reboot your host.

Note for Windows Itanium and Windows x64:

If a new tape library is connected to the system after the installation of Oracle Secure Backup software, then perform the following steps:

1. Uninstall any existing driver for the newly connected medium changers and tape drives.
2. Run the following commands for installing Oracle Secure Backup driver for tape drives and medium changer devices:

```
obdrvctl -add ob -device SCSI\Sequential
obdrvctl -add ob -device SCSI\Changer
```

Disabling Removable Storage Service on Windows Media Servers

The Removable Storage service is used to manage removable media, drives, and libraries. On Windows hosts configured for the media server role, this service must be disabled for the Oracle Secure Backup device driver to correctly control media devices.

To disable the Removable Storage service:

1. From the Windows Control Panel, click **Administrative Tools**.
2. Click **Services** to view the list of services on your host.
3. Right-click the **Removable Storage** service and choose **Properties**.
4. In the Properties window, if the service is running, then click **Stop** to stop the service. Set the Startup Type field to **Disabled**.
5. Click **OK**.

Do Not use STORport Miniport Drivers

When you try to use Removable Storage or a third-party program to manage a media changer device, the device may not work correctly. Also, you may experience one or more of the following symptoms:

- You receive an error message.
- The device does not come online.

Oracle Secure Backup's device driver is unable to bind to tape drive and library devices when the host bus adapter (HBA) used to connect them to the host is using a STORport Miniport Driver. This problem occurs if you install a Storport-based miniport driver for the fibre channel HBA that you connect the device to. This problem does not occur if you use a SCSIPort-based miniport driver for the HBA device.

Running the Oracle Secure Backup Windows Installer setup.exe

Complete the following steps to install Oracle Secure Backup as a client, media server, administrative server or any combination of these roles.

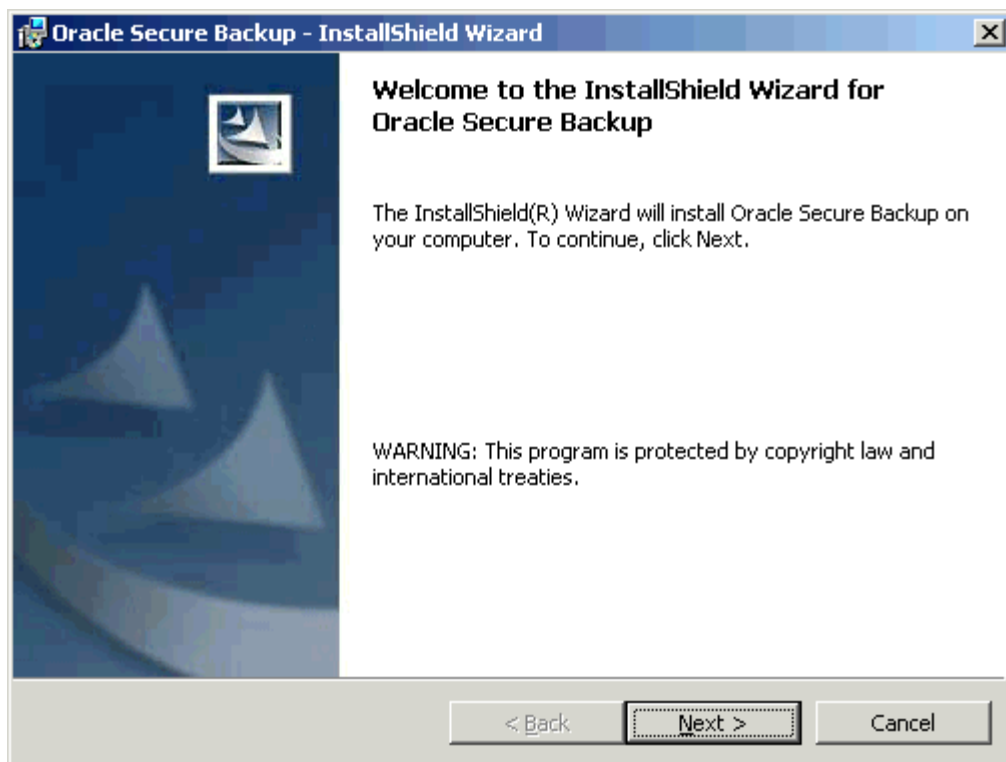
During the installation process, the Oracle Secure Backup Setup Wizard copies all Oracle Secure Backup files to the local host and generates Windows Registry entries.

Note: If you are installing Oracle Secure Backup in an Oracle Real Application Clusters (RAC) environment, then you must install Oracle Secure Backup on each node in the cluster.

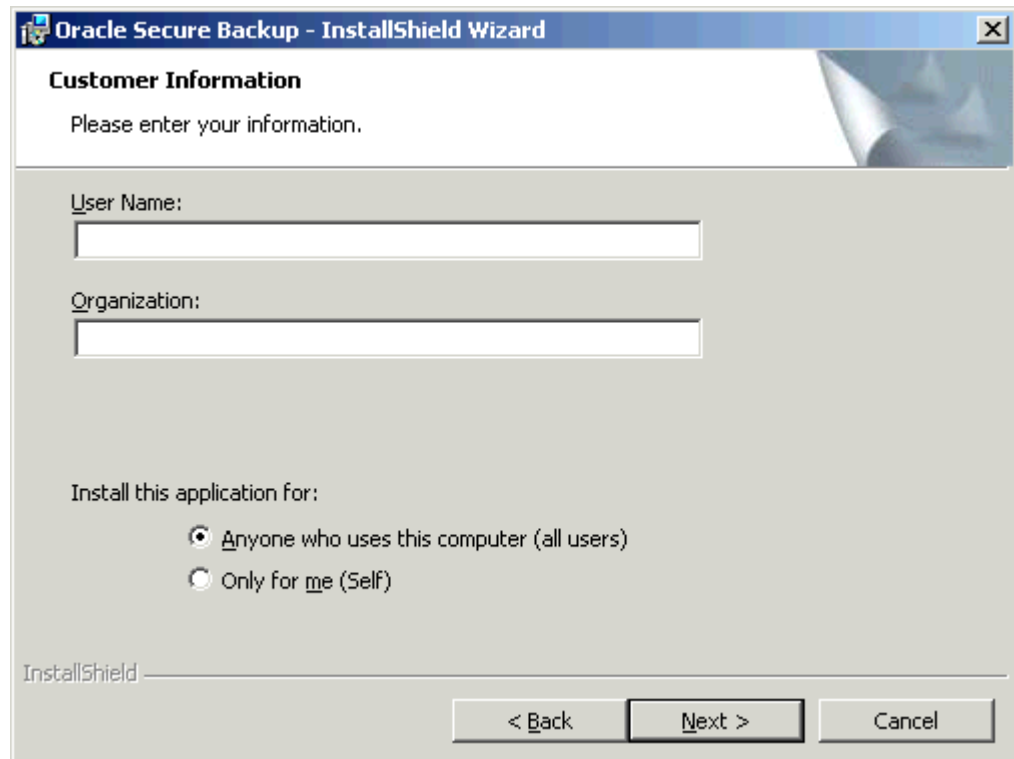
1. Select one of the following install options:
 - If you are installing Oracle Secure Backup from a CD-ROM, insert the CD-ROM. If AutoPlay is enabled, then the `setup.exe` program starts automatically and opens the Oracle Secure Backup Setup Wizard.
-
- Note:** If Windows AutoPlay is not enabled, then open the drive containing the installation CD-ROM using Windows Explorer and run the `setup.exe` program.
-
- If you are installing Oracle Secure Backup from an Oracle Technology Network (OTN) download, then run the `setup.exe` program from the folder into which the download TAR file contents were extracted, as explained in "[Extracting Oracle Secure Backup from OTN Download on Linux or Solaris](#)" on page 1-15.

The Oracle Secure Backup Setup Wizard starts and the Welcome dialog box appears.

Figure 2–1 Welcome Dialog Box



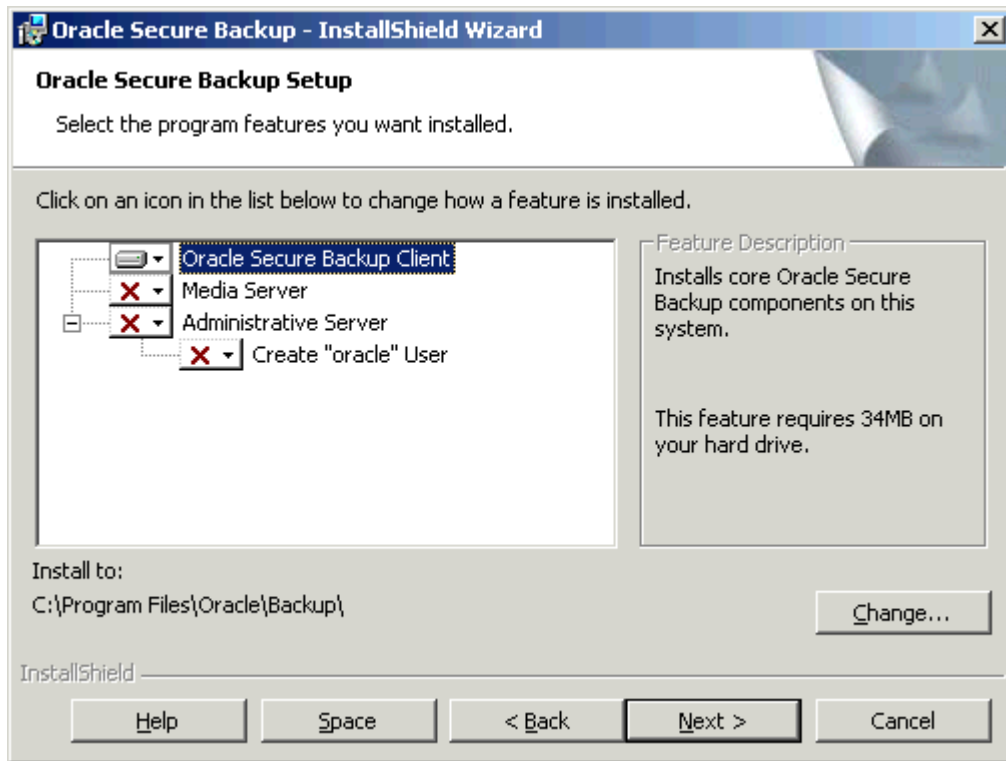
2. Click **Next** to continue.
The Readme Information dialog box displays.
3. Click **Next** to continue.
The Customer Information dialog box displays.

Figure 2–2 Customer Information Dialog Box

The screenshot shows a Windows dialog box titled "Oracle Secure Backup - InstallShield Wizard". The dialog has a blue header bar with the title and a close button (X). Below the header, the text "Customer Information" is displayed in bold, followed by the instruction "Please enter your information." There are two text input fields: "User Name:" and "Organization:". Below these fields, the text "Install this application for:" is followed by two radio button options: "Anyone who uses this computer (all users)" (which is selected) and "Only for me (Self)". At the bottom left, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter your customer information as follows:
 - a. Enter your name in the **User Name** box and the name of your company in the **Organization** box.
 - b. Select a target user for the application: **Anyone who uses this computer** (all users) or **Only for me** (current user).
5. Click **Next** to continue.

The Oracle Secure Backup Setup dialog box appears. (See [Figure 2–3](#).)

Figure 2-3 Setup Dialog Box

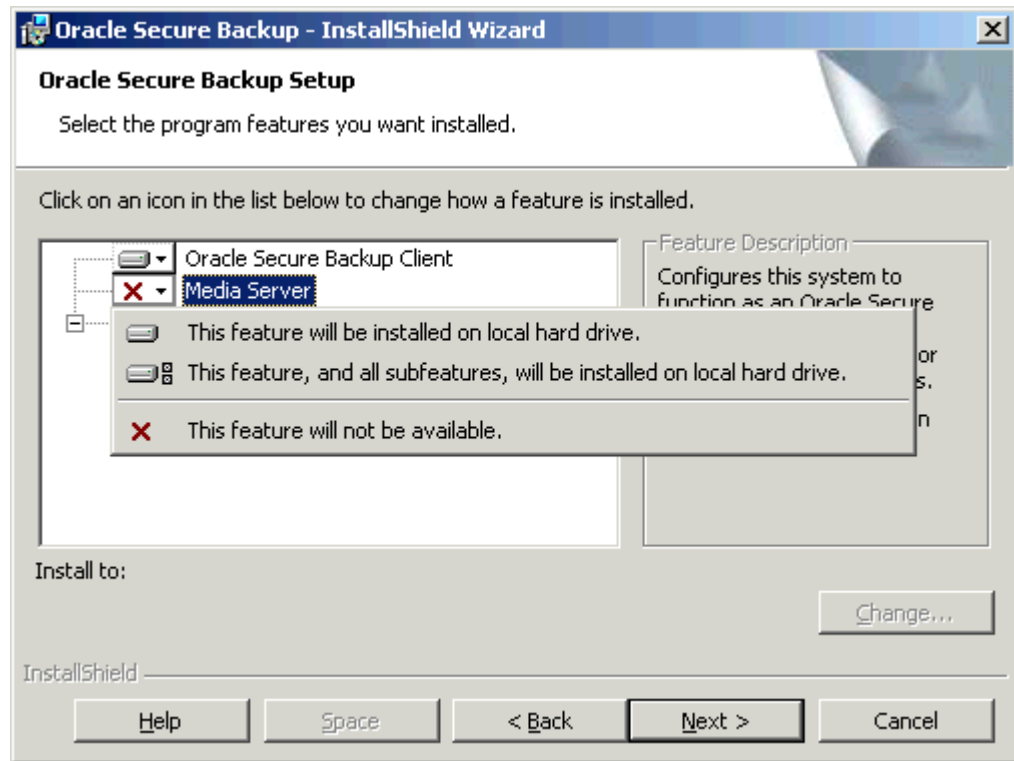
"Choosing Roles for Hosts in Your Administrative Domain" on page 1-8 explains that a single host can assume multiple roles. Roles in Oracle Secure Backup are additive rather than exclusive. You have the following options when choosing roles:

- To install the Windows host as client only, skip to Step 9.

Note: Every installation of Oracle Secure Backup on Windows includes a client installation.

- To install the Windows host as a media server, proceed to Step 6.
 - To install the Windows host as an administrative server but **not** as a media server, skip to Step 7.
6. To install the Windows host as a media server, click the menu of the Media Server icon. [Figure 2-4](#) shows the menu options.

Figure 2-4 Setup Dialog Box: Media Server Menu



Select **This feature will be installed on local hard drive**. Selecting this option removes the X from the Media Server icon and includes the Media Server in the installation.

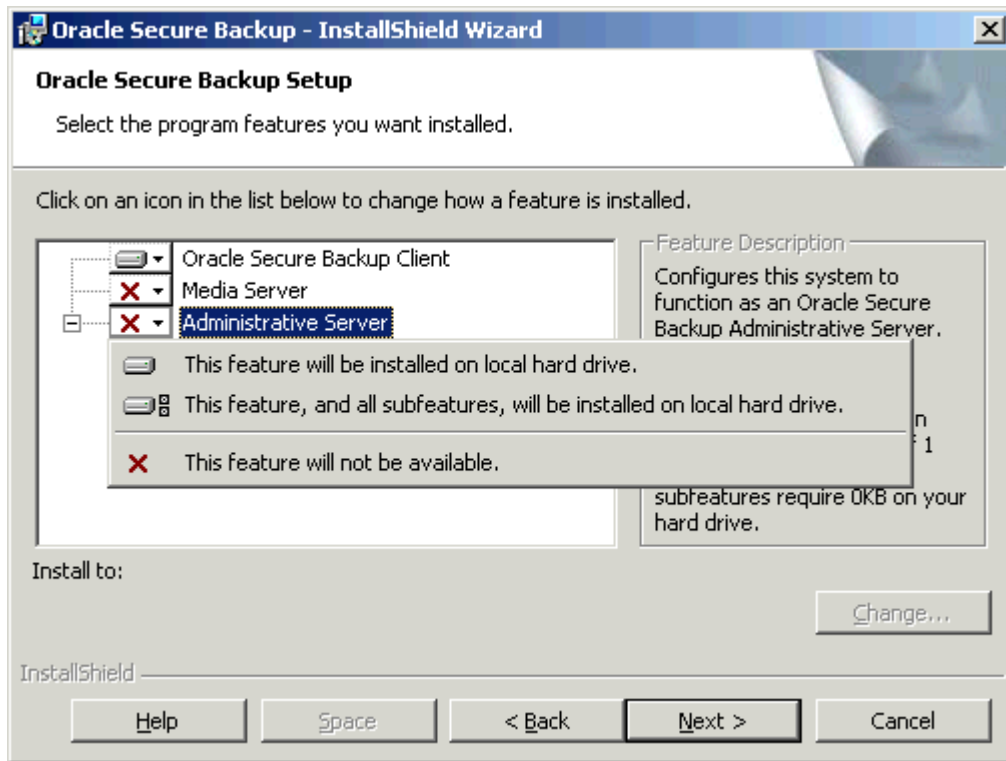
Caution: When there are no media devices attached to a Windows 2000 host, do not install the Windows host as a media server.

If you configure the media server role on a Windows 2000 host with no attached media devices, then the operating system will continuously try to load the Oracle Secure Backup driver. Continuously trying to load the driver uses most of the available CPU cycles on that system, and renders the system unusable.

To configure the Windows host to also be an administrative server, proceed to Step 7. Otherwise, skip to Step 9.

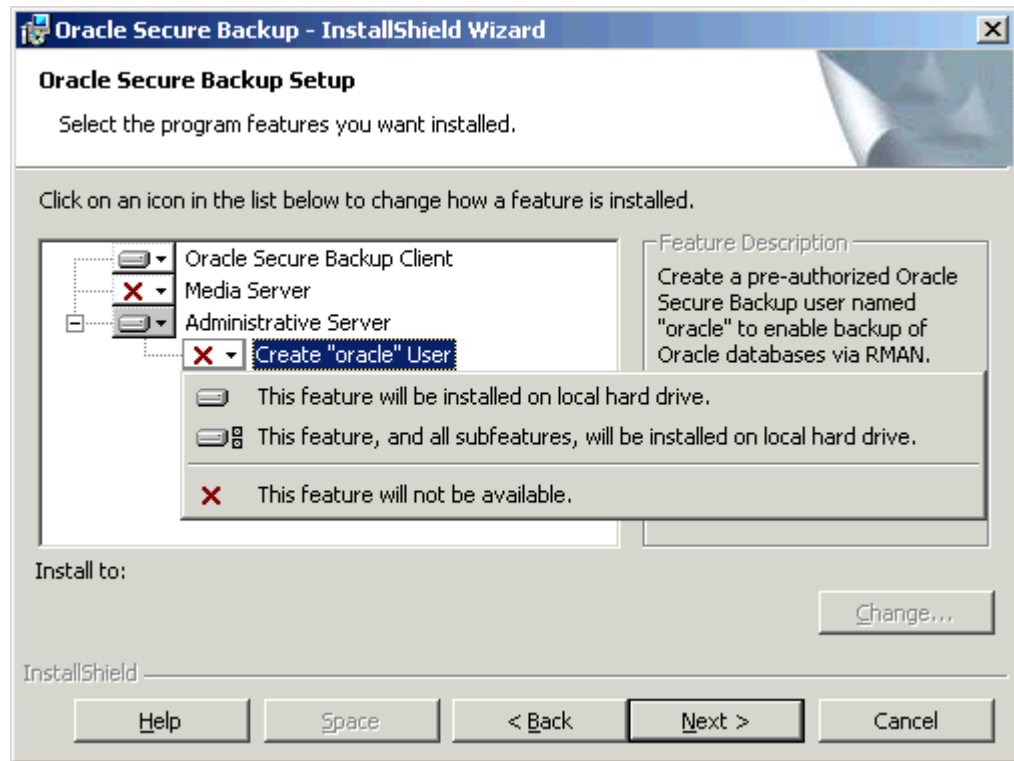
7. To install the Windows host as an administrative server, click the menu of the administrative server icon. [Figure 2-5](#) shows the menu options.

Figure 2-5 Setup Dialog Box: Administrative Server Menu



Select **This feature will be installed on local hard drive**. Selecting this option removes the X from the administrative server icon and includes the administrative server in the installation.

If you plan to perform Oracle database backups and restores with RMAN, then enable the action for **Create "oracle" user** in the submenu attached to the administrative server icon.

Figure 2-6 Setup Dialog Box: Create "Oracle" User Menu

If this choice is enabled, the installer creates an Oracle Secure Backup user called `oracle` (with the rights of the `oracle` class) whose purpose is to facilitate backup and restore of Oracle databases with Recovery Manager. If the X is removed from **Create "oracle" user**, then the `oracle` user is created.

Note:

- You only need to create the `oracle` user if you plan to use Oracle Secure Backup with RMAN.
 - If you intend to use Oracle Secure Backup to perform one-time, RMAN-initiated, or unprivileged backups on Windows clients, then you must modify the Oracle Secure Backup `admin` and `oracle` users to assign them Windows credentials (a domain, username and password) that are valid at the client with required privileges after you complete the Oracle Secure Backup installation. Otherwise, Oracle Secure Backup is unable to perform the backup operation. This requirement applies regardless of the platform that acts as the administrative server.
 - Before electing to create an Oracle Secure Backup `oracle` user, be aware that this choice involves a trade-off between convenience and security.
-
-

See Also: *Oracle Secure Backup Reference* for more information about the `oracle` class

If you do not plan to use Oracle Secure Backup to back up your Oracle databases, then leave the **Create "oracle" user** option unselected. This is the default.

In addition to the options described in steps 6 and 7, you can perform the following actions in the Oracle Secure Backup Setup dialog box:

- Click **Help** for detailed descriptions of the installation options.
 - Click **Change** to change the destination folder for the installation.
 - Click **Space** to display the disk space required for the installation.
8. Click **Next** to continue.

If you are configuring this host to act as an administrative server, the Oracle Secure Backup Admin User Password dialog box appears. (See [Figure 2–7](#).)

Figure 2–7 Admin User Password Dialog Box

Choose a password for the Oracle Secure Backup administrative user, and enter it in both fields, for confirmation. The maximum password length is 16 characters.

Note: Oracle suggests that you choose an administrative user password of at least eight characters in length, containing a mixture of alphabetic and numeric characters. The maximum length is 16 characters.

9. Click **Next** to continue.

The Ready to Install the Program dialog box displays.

10. Click **Install** to start copying files.

A progress bar appears. When the files are copied the InstallShield Completed dialog box displays.

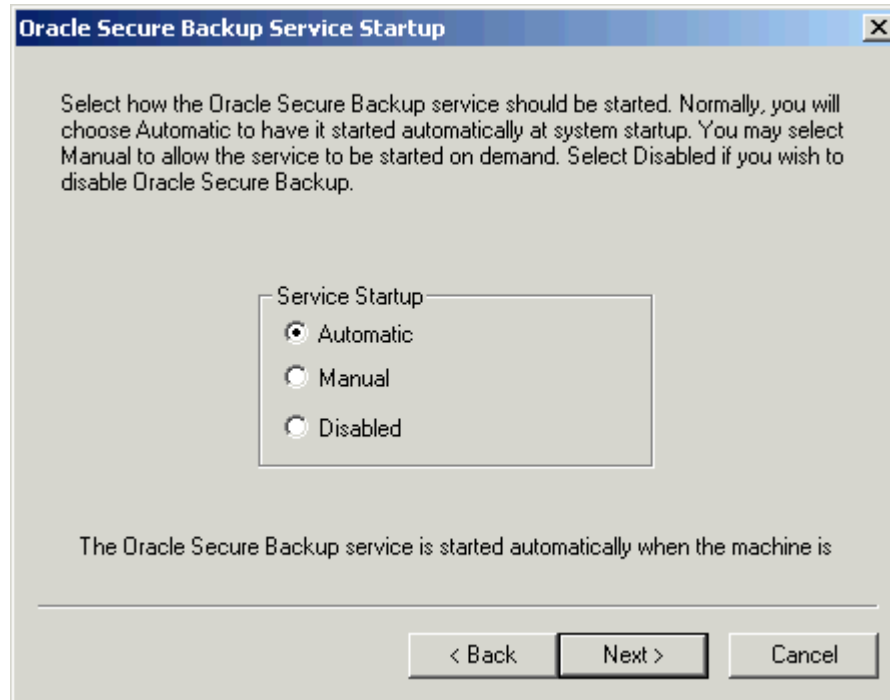
11. Click **Finish** to continue.

The Oracle Secure Backup Configuration dialog box displays.

12. Click **Next** to continue.

The Oracle Secure Backup Service Startup dialog box displays.

Figure 2–8 Oracle Secure Backup Service Startup



13. Click one of the possible modes in which to start the Oracle Secure Backup service. Your choices are:

- **Automatic**

The Oracle Secure Backup service starts automatically when you reboot your host.

- **Manual**

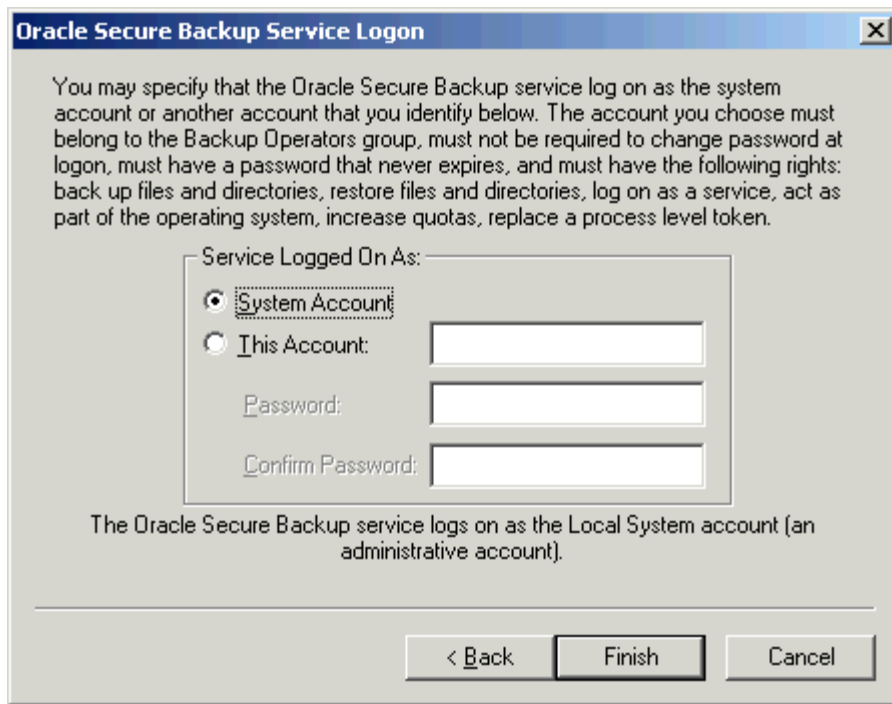
The Oracle Secure Backup service must be started manually by a user who is a member of the Administrators group.

- **Disabled**

The Oracle Secure Backup service is disabled.

14. Click **Next** to continue.

The Oracle Secure Backup Service Login dialog box appears.

Figure 2–9 Service Logon Dialog Box

15. Select one of the following options:

Note: By default, the Oracle Secure Backup service logs on as the Local System account, which is an administrative account. You can select the **This Account** option to specify a different account for the Oracle Secure Backup Service.

- Select **System Account** if you plan to run the Oracle Secure Backup service daemon (and associated subordinate daemons) with full privileges.
- Select **This Account** if you plan to run the Oracle Secure Backup service daemon (and associated subordinate daemons) with the privilege set associated with an existing Windows user account. You must fill in the Windows user account name and password.

If you choose this option, ensure that the Windows user account you select meets the following criteria:

- The account you choose must belong to the Backup Operators group.
- No change in password at login is required of the account.
- The account must be set so that the password never expires.
- The account must have backup and restore rights.
- The account must be able to restore files and directories.
- The account must be able to log on as a service.
- The account must be able to act as part of the operating system.
- The account must be able to increase quotas.
- The account must be able to replace a process level token.

16. Click *Finish* to complete the installation.

If you installed Windows as an administrative server—or combined media server and administrative server—a Command Prompt window runs briefly in the background. When this window terminates, installation is complete.

When you have performed all of the preceding tasks, Oracle Secure Backup installation on this host is complete. Repeat this installation process for each Windows host in your administrative domain.

Note: Depending upon your installation, you may have to perform subsequent configuration tasks, such as configuring your administrative domain.

[Chapter 3, "Configuring a Domain and Devices on Windows"](#) describes configuring the administrative domain and devices with `obtool` on Windows.

You can also perform configuration tasks using the Oracle Secure Backup Web tool or Oracle Enterprise Manager. See *Oracle Secure Backup Reference* for information about `obtool` commands, and *Oracle Secure Backup Administrator's Guide* for information about using `obtool`.

Configuring Firewalls for Oracle Secure Backup on Windows

If your Windows host is protected by a firewall, the firewall must be configured to permit Oracle Secure Backup daemons on the host to communicate with the other hosts in your administrative domain. Oracle Secure Backup includes daemon components that listen on ports 400 and 10000, as well as other dynamically assigned ports.

For example, Windows XP Service Pack 2 and Windows Server 2003 contain a built-in Windows Firewall which, in the default configuration, blocks inbound traffic on ports used by Oracle Secure Backup.

Because the dynamically assigned ports used by Oracle Secure Backup span a broad range of port numbers, your firewall must be configured to allow executables for the Oracle Secure Backup daemons to listen on all ports.

Note: The Oracle Secure Backup Windows installation provides a sample batch script called `obfirewallconfig.bat` in the `bin` directory under the Oracle Secure Backup home.

This script contains commands that make the required configuration changes for the Windows Firewall on Windows Server 2003 and Windows XP systems having a single network interface. Review the script to determine whether it is suitable for your environment. You can run the script after the installation completes.

For details on configuration of other firewalls, see the documentation provided by the vendor. You can refer to the sample script for the Windows Firewall to determine the names of executables that need permission to listen on ports.

Configuring a Domain and Devices on Windows

This chapter describes configuring libraries and tape drives for use by Oracle Secure Backup and setting up an administrative domain.

Note: The configuration tasks described in this chapter are to be performed after the installation process described in [Chapter 2, "Installing Oracle Secure Backup on Windows"](#) is complete. These configuration tasks are not required as part of the initial installation process, but may be required to make use of the software.

This chapter covers the following topics:

- [Configuring Libraries and Tape Drives on Windows: Overview](#)
- [Configuring an Administrative Domain on Windows: Overview](#)
- [Assigning Oracle Secure Backup Device Names on Windows](#)
- [Taking Inventory of Tape Devices on Windows](#)
- [Configuring NAS Libraries and Tape Drives on Windows](#)

Configuring Libraries and Tape Drives on Windows: Overview

This section assumes that your Windows system uses libraries and tape drives that need to be configured for use with Oracle Secure Backup. This section describes how to perform the following tasks:

1. Establish your administrative domain so that media servers can be associated with their attached devices.
["Configuring an Administrative Domain on Windows: Overview"](#) on page 3-2 describes how to perform this task.
2. Assign user-defined names to your devices (optional).
["Assigning Oracle Secure Backup Device Names on Windows"](#) on page 3-4 describes how to perform this task.
3. Inventory your devices.
["Taking Inventory of Tape Devices on Windows"](#) on page 3-6 describes how to perform this task.
4. Configure Network Attached Storage (NAS) tape drives and libraries, if any.

"[Configuring NAS Libraries and Tape Drives on Windows](#)" on page 3-6 describes how to perform this task.

Before proceeding to these tasks, review the conceptual information in the following sections:

- [About Oracle Secure Backup Logical Unit Numbers](#)
- [About Fibre Channel Shared Devices](#)

About Oracle Secure Backup Logical Unit Numbers

In addition to obtaining SCSI device information, each tape drive or tape library is assigned an Oracle Secure Backup logical unit number during the configuration process. This number, which must be between 0 and 31, is used to generate unique device names during device configuration. On Windows, Oracle Secure Backup logical unit numbers are assigned by the Oracle Secure Backup device driver. Values for devices of each type (library or tape drive) are assigned sequentially, starting from 0, and this number is used as part of the device name. Tape libraries are thus named ob10, ob11, ob12 and so on. Tape drives are named similarly, obt0, obt1, obt2 and so on.

Note:

- The Oracle Secure Backup logical unit number should not be confused with the SCSI logical unit number (SCSI LUN). The SCSI LUN is part of the hardware address of the device, while the Oracle Secure Backup logical unit number is part of the device special file name.
 - In the device name for tape libraries, the character 1 is a lower-case L, not a number 1.
-
-

About Fibre Channel Shared Devices

Unlike SCSI, which is a host-centric protocol, Fibre Channel is a storage architecture alternative in which tape libraries and tape drives are typically shared among multiple Oracle Secure Backup media servers. A Fibre Channel-attached tape drive or library often has multiple attachments, one for each host that can directly access it. You can use the `chdev` command in `obtool` to attach the same device to multiple hosts on a network.

Oracle Secure Backup can automatically arbitrate usage of shared devices so that no two users attempt to access a device independently of one another.

You configure Fibre Channel devices on Oracle Secure Backup in the same way that you configure SCSI and NAS devices.

See Also: *Oracle Secure Backup Reference* to learn more about the `chdev` command

Configuring an Administrative Domain on Windows: Overview

After Oracle Secure Backup has been installed on all the hosts in your network, you can use Oracle Secure Backup to configure your administrative domain. This involves configuring all media servers, client hosts, and NAS filers.

Use the `--access ob` option with the `mkhost` command to configure an Oracle Secure Backup host. The administrative server is configured by default during the installation process.

Note: In the following example, assume that you have an administrative server/media server called `BELLA`, a media server called `storabck05`, and a client host called `dlsun1976`.

To configure an administrative domain:

1. Log on to Windows as the Administrator user or as a user that is a member of the Administrators group.
2. To open Oracle Secure Backup, click the **Start** button and select **Programs, Oracle Secure Backup, and Oracle Secure Backup Command Line Interface**.

The `ob>` prompt displays.

3. Include a media server in your administrative domain. Specify options for access type, role, and IP address. For example:

```
ob> mkhost --access ob --role mediaserver --ip 133.2.22.59 storabck05
```

4. Include a client host in your administrative domain. Specify options for access type, role, and IP address. For example:

```
ob> mkhost --access ob --role client --ip 143.15.235.140 dlsun1976
```

5. List the names and attributes of all the hosts in your administrative domain. For example:

```
ob> lshost
BELLA          admin,mediaserver,client      (via OB)  in service
dlsun1976      client                        (via OB)  in service
storabck05     mediaserver                   (via OB)  in service
```

Note: You can also configure your administrative domain—or perform any of the other procedures in this chapter—with the Oracle Secure Backup Web tool. See the *Oracle Secure Backup Administrator's Guide* for more information.

Configuring NAS Filers

You can configure NAS filers as members of the administrative domain. Use the `--access ndmp` option with the `mkhost` command to configure an NAS filer. Under NAS, storage devices are made LAN-addressable, freeing stored data from a direct attachment to a specific locale.

The administrative server communicates with and manages NAS filers, which do not have Oracle Secure Backup installed, over Network Data Management Protocol (NDMP). NDMP defines a standard TCP/IP-based protocol for backing up and restoring data on heterogeneous networks, regardless of operating system or platform. NDMP minimizes demands on network resources, enables local backups and restores to tape, and allows for centralized management and control.

Note: In the following example, assume you have an administrative server/media server called BELLA and an NAS filer called mynasfiler5.

To configure an NAS filer:

1. Log on to Windows as the Administrator user or as a user that is a member of the Administrators group.
2. To open Oracle Secure Backup, click the **Start** button and select **Programs, Oracle Secure Backup, and Oracle Secure Backup Command Line Interface**.

The ob> prompt displays.

3. Include an NAS filer in your administrative domain. Specify options for access type, role, IP address, and NDMP password. For example:

```
ob> mkhost --access ndmp --role mediaserver --ip 138.1.14.128 --ndmppass
mypassword
mynasfiler5
```

Note: Oracle Secure Backup typically provides a default NDMP password for configuration of NAS filers. Alternatively, you can set the password as the --ndmppass option of the mkhost command.

4. List the names and attributes of all the hosts in your administrative domain. For example:

```
ob> lshost
BELLA          admin,mediaserver,client      (via OB)  in service
dlsun1976      client                       (via OB)  in service
mynasfiler5    mediaserver                  (via NDMP) in service
storabck05    mediaserver                  (via OB)  in service
```

Assigning Oracle Secure Backup Device Names on Windows

After you have established your administrative domain, you can configure any attached libraries and tape drives. Oracle Secure Backup supports both SCSI and Fibre Channel-connected devices, as well as NAS libraries and tape drives. Names for Oracle Secure Backup devices are user-defined.

In the following example, assume you have a combined administrative server and media server called BELLA with an attached library named ob10 and tape drive named obt0. The example uses obtool commands for device configuration, although you can also use the Oracle Secure Backup Web tool or Oracle Enterprise Manager to assign Oracle Secure Backup device names.

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

1. If you are already logged on to Oracle Secure Backup, skip to Step 3.

Otherwise, log on to Windows as the Administrator user or as a user that is a member of the Administrators group.

2. To open Oracle Secure Backup, click the **Start** button and select **Programs, Oracle Secure Backup, and Oracle Secure Backup Command Line Interface**.

The `ob>` prompt displays.

3. Create an Oracle Secure Backup device object and assign it a user-defined name for the tape library. Specify options for the device type and media server. The following example assigns the name `tc-lib` to tape library `ob10`:

```
ob> mkdev --type library --attach BELLA://./ob10 tc-lib
```

4. Create an Oracle Secure Backup device object and assign it a user-defined name for the tape drive. The following example assigns the name `tc-tape` to tape drive `obt0`:

```
ob> mkdev --type tape --library tc-lib --dte 1 --attach BELLA://./obt0 tc-tape
```

Note: Oracle Secure Backup identifies each tape drive within a library by its data transfer element (DTE) number. You must specify a `dte` if `library` is specified. DTEs are numbered 1 through *n*.

5. Check configuration information for both devices. For example:

```
ob> lsdev -l
```

In this example, the command displays the following output:

```
tc-lib:
  Device type:      library
  Model:           [none]
  In service:      yes
  Debug mode:      no
  Barcode reader:  default (hardware-selected)
  Barcodes required: no
  Auto clean:      no
  Clean interval:  (not set)
  Clean using emptiest: no
  UUID:           ca196e5e-af6d-4978-9172-3dad5d50ec7
  Attachment 1:
    Host:          BELLA
    Raw device:    //./ob10
tc-tape:
  Device type:      tape
  Model:           [none]
  In service:      yes
  Library:         tc-lib
  DTE:             1
  Automount:       yes
  Error rate:      8
  Query frequency: 1207KB (1236976 bytes) (from driver)
  Debug mode:      no
  Blocking factor: (default)
  Max blocking factor: (default)
  Current tape:    2
  Use list:        all
  Drive usage:     none
```

```
Cleaning required:    no
UUID:                d367a0dd-549c-4b99-9557-d9fc16d9d2c5
Attachment 1:
  Host:              BELLA
  Raw device:        //./obt0
```

Note: Device special files for tape libraries are named `obl n` by default, where n is a number (the Oracle Secure Backup logical unit number, which on Windows is assigned automatically by the Oracle Secure Backup Windows device driver). For example, in the preceding output, the name of the device special file for the tape library (the value for the `Raw device`) is `//./obl0`. Note that the third character in the device special file name is a lower-case letter `L`, not the number `1`.

Taking Inventory of Tape Devices on Windows

Now that your devices are configured, use Oracle Secure Backup to take inventory of the volumes in your tape library.

1. If you are already logged on to Oracle Secure Backup, skip to Step 3.
2. To open Oracle Secure Backup, click the **Start** button and select **Programs, Oracle Secure Backup, and Oracle Secure Backup Command Line Interface**.

The `ob>` prompt displays.

3. Specify the name of the library of which you are taking inventory. For example:

```
ob> inventory -L tc-lib
```

You can obtain library names by running the `lsdev` command.

4. List all the volumes in the library. For example:

```
ob> lsvol -L tc-lib
```

In this example, the command displays the following output:

```
Inventory of library tc-lib:
in   3:          barcode 00000153
in   4:          barcode 00000154
in   5:          barcode 000005
in   6:          barcode 00000151
in   7:          barcode 00000134
in   8:          barcode 00000133
in   9:          barcode 00000131
in  10:         barcode 00000130
in  11:         barcode 00000129
in  12:         barcode 00000128
in  15:         occupied
in   dte:       barcode 00000152, lastse 2
```

Configuring NAS Libraries and Tape Drives on Windows

This section explains how to configure the libraries and tape drives attached to a Network Attached Storage (NAS) filer so that Oracle Secure Backup can communicate with the filer and back up files on the filer to a tape drive.

Libraries and tape devices attached to NAS filers are automatically configured by the operating system on which the NAS device runs. Both SCSI device and Fibre Channel configurations occur automatically.

Libraries and tape drives must still be made accessible to the Oracle Secure Backup software. You accomplish this task by performing device discovery on each of the NAS filers in the administrative domain.

Note: An administrative server can use an NAS filer with attached devices as a media server.

Making NAS Device Names Accessible to Oracle Secure Backup

Oracle Secure Backup can detect devices attached to NAS filers that are part of an administrative domain and, based on this information, automatically update the domain's device configuration.

To discover NAS device names and make them accessible to Oracle Secure Backup, complete the following steps:

1. If you are already logged on to Oracle Secure Backup, skip to Step 3.
Otherwise, log on to Windows as the Administrator user or as a user that is a member of the Administrators group.
2. To open Oracle Secure Backup, click the **Start** button and select **Programs, Oracle Secure Backup, and Oracle Secure Backup Command Line Interface**.
The `ob>` prompt displays.
3. Detect changes in device configuration and update the administrative domain for a media server called `mynasfiler5`, which was configured previously using `mkhost`. See "[Configuring NAS Filers](#)" on page 3-3 for more information.

```
ob> discoverdev --verbose --host mynasfiler5
```

In this example, the command displays the following output:

```
Info: beginning device discovery for mynasfiler5.
Info: connecting to mynasfiler5

Info: devices found on mynasfiler5:
Info: ATL      1500      ...
Info: mc3  attrs= [none]
Info: WWN: [none]
Info: SN:  PMC13A0007
Info: Quantum SDLT220...
Info: nrst7a  attrs= norewind raw
Info: WWN: [none]
Info: SN:  CXB45H1313
Info: Quantum SDLT220...
Info: nrst8a  attrs= norewind raw
Info: WWN: [none]
Info: SN:  PKB51H0286

mynasfiler5_mc3  (new library)
WWN: [none]
new attach-point on mynasfiler5, rawname mc3

mynasfiler5_nrst7a  (new drive)
WWN: [none]
```

```

new attach-point on mynasfiler5, rawname nrst7a

mynasfiler5_nrst8a (new drive)
  WWN: [none]
  new attach-point on mynasfiler5, rawname nrst8a

```

Note: By convention, NAS library names are characterized by `mc` and NAS tape drives are characterized by `nrst`.

4. List summary device information. For example:

```
ob> lsdev
```

`obtool` displays output similar to the following:

```

library   mynasfiler5_mc3      not in service
drive     mynasfiler5_nrst7a not in service
drive     mynasfiler5_nrst8a not in service
library   tc-lib             in service
drive 1   tc-tape           in service

```

Unless you change a device's default policy value, every newly discovered device is by default placed in the `not in service` state.

Note: The device names assigned automatically by Oracle Secure Backup are predicated on library and tape drive names reported by the NAS device. These names tend to be long and unwieldy. Consider renaming NAS library and tape drives to more concise names. The long names are used in this example.

5. Specify the name of the library in which the first tape drive resides. For example:

```
ob> chdev --library mynasfiler5_mc3 --dte 1 mynasfiler5_nrst7a
```

6. Specify the name of the library in which the second tape drive resides. For example:

```
ob> chdev --library mynasfiler5_mc3 --dte 2 mynasfiler5_nrst8a
```

7. Notice that none of the devices are in service. Put the library and tape drives in service. For example:

```
ob> chdev --inservice mynasfiler5_mc3 mynasfiler5_nrst7a mynasfiler5_nrst8a
```

8. List the library and devices now in service. For example:

```
ob> lsdev mynasfiler5_mc3
```

In this example, the command displays the following output:

```

library   mynasfiler5_mc3      in service
drive 1   mynasfiler5_nrst7a  in service
drive 2   mynasfiler5_nrst8a  in service

```

You may choose to take another inventory of your system at this point. For instructions, see ["Taking Inventory of Tape Devices on Windows"](#) on page 3-6.

Installing Oracle Secure Backup on Linux or UNIX

This chapter explains how to install Oracle Secure Backup on hosts running Linux or UNIX.

This chapter covers the following topics:

- [Preparing to Install Oracle Secure Backup on Linux and UNIX](#)
- [Creating the Oracle Secure Backup Home](#)
- [Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script](#)
- [Optional: Configuring Installation Parameters in the obparameters File](#)
- [Installing Oracle Secure Backup on Linux or UNIX with installob](#)

Preparing to Install Oracle Secure Backup on Linux and UNIX

Perform the following actions before you begin:

- Select hosts for the administrative server, media server and client roles, as described in "[Planning Your Administrative Domain](#)" on page 1-4.
- For Linux media servers, ensure that the SCSI Generic (SG) driver is installed. It is required for Oracle Secure Backup to interact with media devices.
- If you are running `setup` or `installob` on a Linux host, then the `compress` and `uncompress` utilities must be installed on the system.
- Determine the SCSI parameters for each tape drive and library attached to your Linux and UNIX media servers, as described in "[Determining SCSI Device Parameters on Linux and UNIX](#)" on page 5-1. You can configure these devices as part of your initial installation process or later, but you need the information in any case.
- Decide whether to perform an interactive or batch-mode installation.

In interactive mode, the `installob` program installs the software on one host at a time, prompting for the host name, roles, SCSI device information (for media servers), and any other required information for each installation. After each installation, you are asked whether you want to install Oracle Secure Backup on another host.

In batch mode, you must create or modify a **network description file**, which is a text file that describes your network configuration. The `installob` program uses the information in this file to perform a push installation, transferring the software

across the network to the designated hosts and performing required installation and configuration steps.

Examine the sample network description file `./install/obndf` for information on creating a network description file. The file contains extensive comments that document the required contents. If you plan to modify the file, then save a copy of the original.

Note: The example in ["Installing Oracle Secure Backup on Linux or UNIX with installob"](#) on page 4-6 describes installation in interactive mode.

- Ensure that each host has a network connection and runs TCP/IP.
- If using push installations, then configure destination hosts to allow rsh access for `root` from the administrative server without requiring a password. For more details on configuring rsh access for `root` without a password on your media servers and clients, refer to the operating system documentation for your platform.

If not using push installations, then decide how to make the installation media for Oracle Secure Backup available on each Linux or UNIX host in your administrative domain. For example, ensure that each host has a CD-ROM drive, or can mount a directory over NFS across the network containing the extracted archive of Oracle Secure Backup installation files.

Note:

- Consider the security implications of configuring your hosts to permit rsh access for `root` without passwords when deciding whether to use remote installation.
 - If support for rsh access for `root` without passwords across your administrative domain is not part of your normal system configuration, then remember to disable it on each host in your administrative domain when the installation process is complete.
-
-

- You must log in to each host with `root` privileges to perform the installation.
- If you are installing Oracle Secure Backup in an Oracle Real Application Clusters (RAC) environment, then you must install Oracle Secure Backup on each node in the cluster.

Creating the Oracle Secure Backup Home

You must create the Oracle Secure Backup home before beginning the process of loading and installing the software. The Oracle Secure Backup setup program uses this directory to store installation files specific to your host.

See also: ["Oracle Secure Backup Home Directory"](#) on page A-1 and *Oracle Secure Backup Administrator's Guide* for more details about the Oracle Secure Backup home.

The recommended location for the Oracle Secure Backup home is `/usr/local/oracle/backup`. You can, however, create the directory in a different location.

Note: Oracle recommends that you use `/usr/local/oracle/backup` as your Oracle Secure Backup home. If you use a different directory, then the `setup` program prompts you to confirm your selected directory.

After logging in as `root`, create the directory for your Oracle Secure Backup home. For example:

```
# mkdir -p /usr/local/oracle/backup
```

Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script

Loading the Oracle Secure Backup software is the process by which packages of files required to install Oracle Secure Backup on one or more platforms are extracted from the installation media and staged in the Oracle Secure Backup home for later use by the `installob` installation script. The `setup` script is used to perform this loading process.

Note: Network administrators may find it convenient to load Oracle Secure Backup installation files for multiple platforms on the administrative server. You can hold these binaries in reserve for installation to various hosts in their administrative domain at a later time. It is not, however, required that you load the installation files for all platforms on the administrative server. You can also extract installation files and run `setup` and `install` separately on each host.

This example illustrates the loading process on a Solaris 64-bit host called `d1sun1976`. However, these instructions apply to all Linux and UNIX operating systems.

To load Oracle Secure Backup into an Oracle Secure Backup home directory for later installation on one or more platforms:

1. Log into your Linux or UNIX operating system as `root`.
2. Change to the Oracle Secure Backup home directory created in "[Creating the Oracle Secure Backup Home](#)" on page 4-2. For example:

```
# cd /usr/local/oracle/backup
```

3. Run the `setup` script from your installation media or extracted archive directory. Enter the following command:

```
#!/media_dir/setup
```

where `/media_dir` is the CD-ROM mount point or the directory containing the files extracted from the downloaded archive.

For example, if you downloaded an archive from Oracle Technology Network (OTN) and extracted the setup software to the `/tmp/osbdownload/OB` directory, then you would run the `setup` program as follows:

```
# /tmp/osbdownload/OB/setup
```

The setup program displays output similar to the following for Linux x86 and Solaris Operating System (SPARC 64-Bit):

```
Welcome to Oracle's setup program for Oracle Secure Backup. This
program loads Oracle Secure Backup software from the CD-ROM to a filesystem
directory of your choosing.
```

```
This CD-ROM contains Oracle Secure Backup version 10.1.0.1.0.
```

```
Please wait a moment while I learn about this host... done.
```

```
- - - - -
```

```
You may load any of the following Oracle Secure Backup packages:
```

1. linux32 (RH 2.1, RHEL 3, RHEL 4, SuSE 8, SuSE 9)
administrative server, media server, client
2. solaris64 (Solaris 2.8 and later, SPARC)
administrative server, media server, client

```
Enter a space-separated list of packages you'd like to load. To load all
packages, enter 'all' [2]:
```

Note: The output for the setup program varies for Linux Itanium, Linux x86-64, and HP-UX PA-RISC (64-Bit).

4. Each package contains the binaries and other files required to install Oracle Secure Backup on that platform. Enter the number or numbers that identify the installation packages that you want to load, so that they will be staged for later installation on Linux or Unix hosts in your administrative domain.

Note: You can run setup again in the future if necessary, to load packages for more platforms into the Oracle Secure Backup home, without affecting existing installations of Oracle Secure Backup.

To load the Oracle Secure Backup installation package for a single host, enter the appropriate number for that platform. For this example, enter 2 to load only the package of Oracle Secure Backup for a Solaris 64 host. The following output is displayed:

```
- - - - -
```

```
Loading Oracle Secure Backup installation tools ... done.
Loading solaris64 administrative server, media server, client ... done.
```

```
- - - - -
```

```
Loading of Oracle Secure Backup software from CD-ROM is complete. You may
unmount and remove the CD-ROM.
```

Note: At this point the setup process is complete. The files required to install Oracle Secure Backup on the platforms you specified are stored in the Oracle Secure Backup home on this host.

Starting the Oracle Secure Backup installob Script From setup

setup now displays the following question:

```
Would you like to continue Oracle Secure Backup installation with 'installob'
now? (The Oracle Secure Backup Installation Guide
contains complete information about installob.)
Please answer 'yes' or 'no' [yes]:
```

At this point the setup script can start the `installob` script to install Oracle Secure Backup on the local host or, using a push installation, deploy it on other Linux or UNIX hosts on your network. You can also defer this task until later.

Choose one of the following:

- Enter `no` if you want to run `installob` later, or if you need to customize some aspect of your installation process using the `obparameters` file, as described in ["Optional: Configuring Installation Parameters in the obparameters File"](#) on page 4-5.

In this case, the following message displays:

```
When you are ready to continue:
1. log in as (or 'su' to) root
2. cd to /usr/local/oracle/backup
3. run install/installob
```

The setup script then exits.

- Enter `yes` to start the `installob` script. The steps for running `installob` are described in ["Installing Oracle Secure Backup on Linux or UNIX with installob"](#) on page 4-6.

Note: If the setup script is interrupted, it is possible that some temporary files, named `OBnnnn` or `OBnnnn.Z`, remain in `/usr/tmp`. You can delete these files.

Optional: Configuring Installation Parameters in the obparameters File

Oracle Secure Backup uses a parameter file called `obparameters` to customize the operation of the `installob` installation script.

The setup script (described in ["Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script"](#) on page 4-3) creates the `obparameters` file in the `install` subdirectory of the Oracle Secure Backup home. For example, if the Oracle Secure Backup home is in the default location `/usr/local/oracle/backup`, the parameter file is located at `/usr/local/oracle/backup/install/obparameters`.

During the installation process the setup program prompts you either to accept the default settings in the `obparameters` file or customize those settings.

In most cases, it is not necessary to change the defaults in the `obparameters` file. However, you should review the parameters you can control in this file as part of planning your installation, and determine whether any of them should be changed.

Reasons to change the parameters in the `obparameters` file include:

- You can customize installation directories and symbolic links created during installation on different platforms.
- If using Oracle Secure Backup to back up Oracle databases to tape, you can create an Oracle Secure Backup user named `oracle` for use in RMAN backups. You can

associate this user with Linux or UNIX operating system credentials by setting parameters in `obparameters`. (You can also configure a pre-authorized `oracle` user later.)

Note: Before electing to create an Oracle Secure Backup `oracle` user, be aware that this choice involves a trade-off between convenience and security. For more information on the security issues, see *Oracle Secure Backup Reference*.

See Also: *Oracle Secure Backup Administrator's Guide* for more information about the pre-authorized `oracle` user and RMAN backups.

`obparameters` is a plain text file that can be edited using any standard UNIX text editor, such as `emacs` or `vi`. Complete reference documentation for the `obparameters` file is contained in [Appendix B, "Oracle Secure Backup `obparameters` Installation Parameters"](#).

Note: If you intend to use Oracle Secure Backup to perform one-time, RMAN-initiated, or unprivileged backups on Windows clients, then you must modify the Oracle Secure Backup `admin` and `oracle` users to assign them Windows credentials (a domain, username and password) that are valid at the client with required privileges after you complete the Oracle Secure Backup installation. Otherwise, Oracle Secure Backup is unable to perform these types of backup operation. This requirement applies regardless of the platform that acts as the administrative server.

See *Oracle Secure Backup Administrator's Guide* for more details on the role of the preauthorized `oracle` Oracle Secure Backup user in RMAN backups.

Installing Oracle Secure Backup on Linux or UNIX with `installob`

To install the Oracle Secure Backup software on Linux or UNIX, run the `installob` script.

Note: Before starting `installob` on a media server, have the SCSI parameters for tape devices available. You will have the option of entering those parameters to configure SCSI devices as part of the initial installation. See ["Determining SCSI Device Parameters on Linux and UNIX"](#) on page 5-1 for details on collecting this information.

installob Step 1: Starting the `installob` Script

The Oracle Secure Backup setup script described in ["Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script"](#) on page 4-3 ends by asking whether to start the installation process using the `installob` script for you after the software is loaded. If you entered `yes` to this question, the setup script runs the `installob` script for you.

Otherwise, start `installob` from the shell prompt. While logged in as `root`, change directory to the Oracle Secure Backup home and enter the following command:

```
install/installob
```

The `installob` program displays the following output:

```
- - - - -
Welcome to installob, Oracle Secure Backup's UNIX installation program.

It installs Oracle Secure Backup onto one or more UNIX, Linux, or other
supported open-source systems on your network. (Install Oracle Secure
Backup for Windows using the CD-ROM from which you loaded this software.)

For most questions, a default answer appears enclosed in square brackets.
Press return to select this answer.

Please wait a few seconds while I learn about this machine... done.
```

installob Step 2: Confirm Settings in obparameters File

The next step depends upon the value of the customized `obparameters` parameter in the `obparameters` file described in ["Optional: Configuring Installation Parameters in the obparameters File"](#) on page 4-5.

If you have already edited `obparameters` and set customized `obparameters` to `yes`, then `installob` assumes that you have made any desired changes in the `obparameters` file and uses those parameters during the installation. Continue to ["installob Step 3: Choosing Interactive or Batch Mode Install"](#) on page 4-8.

If customized `obparameters` is set to `no` (the default), then `installob` displays the following output:

```
Have you already reviewed and customized install/obparameters for your
Oracle Secure Backup installation [yes]?
```

Select one of the following options:

- Enter `yes` or press the Enter key to indicate that you do **not** want to customize the `obparameters` file. Continue to ["installob Step 3: Choosing Interactive or Batch Mode Install"](#) on page 4-8.
- Enter `no` to choose to customize the `obparameters` file.

The `installob` program displays the following output:

```
Would you like to do this now [yes]?
```

You have the following options:

- Enter `no` to indicate that you do not want to customize the file now. Installation proceeds, based upon the current settings specified in the `obparameters` file. Continue to ["installob Step 3: Choosing Interactive or Batch Mode Install"](#) on page 4-8.
- Enter `yes` to indicate that you want to customize the file now. The `installob` program displays the following output:

```
After you've reviewed and updated install/obparameters, re-run installob.
```

```
installob then exits.
```

Make the desired changes in the `install/obparameters` file under the Oracle Secure Backup home and restart `installob` as described in "[installob Step 1: Starting the installob Script](#)" on page 4-6.

See Also: "[customized obparameters](#)" on page B-1 for details about the `customize obparameters` parameter.

installob Step 3: Choosing Interactive or Batch Mode Install

The `installob` program displays the following output:

```
- - - - -
You can choose to install Oracle Secure Backup in one of two ways:
  (a) interactively, by answering questions asked by this program, or
  (b) in batch mode, by preparing a network description file

Use interactive mode to install Oracle Secure Backup on a small number of
hosts. Use batch mode to install Oracle Secure Backup on any number of
hosts.

Which installation method would you like to use (a or b) [a]?
- - - - -
```

Choose one of the following:

- (a) interactive mode
When you choose this mode, the `installob` program installs the software on one host at a time, prompting for the host name, role and any other information required for each installation. After each installation, you are asked whether you want to install Oracle Secure Backup on another host using a push installation. This example describes an interactive mode installation.
- (b) batch mode
Choose this mode to create or modify a network description file, which is a text file that describes your network configuration. The `installob` program uses the information in this file to perform a push install of the software across the network to the designated host.
Examine the sample network description file `./install/obndf` for information on creating a network description file.

Note: If you plan to modify the network description file, then save a copy of the original sample network description file.

Enter a (or press the Enter key to accept the default choice a).

installob Step 4: Specifying Host Role

The `installob` program displays the following output:

```
- - - - -
Oracle Secure Backup is not yet installed on this machine.

Oracle Secure Backup's Web server has been loaded, but is not yet configured.

You can install this host one of three ways:
```

- (a) administrative server
(the host will also be able to act as a media server or client)
- (b) media server
(the host will also be able to act as a client)
- (c) client

If you are not sure which way to install, please refer to the Oracle Backup Installation Guide. (a,b or c) [a]?

You determined the roles for each host when planning your administrative domain. Choose one of the following:

- Enter a to install the software as an administrative server. An **administrative server** stores configuration information and database files for clients.
- Enter b to install the software as a media server.
A **media server** has one or more secondary storage devices, such as a library and tape drives, connected to it.
- Enter c to install the software as a client. A **client** contains files that Oracle Secure Backup backs up or restores.

Note:

- On Linux and UNIX, an administrative server installation also includes the required components and settings for the media server and client roles. A media server installation also includes the required components for the client role.
 - You can add or remove a role later with the `chhost` command in `obtool`. (To add the media server role to a client after initial installation, you must create device special files using `makedev` or `installob`.) See *Oracle Secure Backup Reference* for details.
-
-

See Also: "[Planning Your Administrative Domain](#)" on page 1-4 to learn more about the roles of administrative server, media server and client in Oracle Secure Backup

This example describes installation for an administrative server.

Enter a (or press the Enter key to accept the default choice a).

The `installob` program displays output similar to the following:

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

```
Installing Oracle Secure Backup on dlsun1976 (solaris version 5.8)
```

Note: The specific output varies according to your operating system.

installob Step 5: Setting Administrative User Password

If you are installing on this host as an administrative server, `installob` prompts for an initial password for the Oracle Secure Backup administrative user. You are prompted to enter the password, and then to re-enter it for confirmation. For example:

You must now enter a password for the Oracle Secure Backup 'admin' user.

Oracle suggests you choose a password of at least 8 characters in length, containing a mixture of alphabetic and numeric characters.

Please enter the admin password:
Re-type password for verification:

Note: When you type in the password, your entry is not echoed to the display.

installob Step 6: installob Completes Installing Software

installob now displays informational messages as it installs and configures the Oracle Secure Backup software on this host. This process may take a few minutes, and the output may vary depending upon the roles specified for this host. For example:

```
generating links for admin installation with Web server
checking Oracle Secure Backup's configuration file (/etc/obconfig)
setting Oracle Secure Backup directory to /usr/local/oracle/backup 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 /usr/local/oracle/backup/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: /usr/local/oracle/backup/.drv.solaris64/ob copied to /usr/kernel/drv/ob
NOTE: /usr/local/oracle/backup/.drv.solaris64/ob.conf copied to
/usr/kernel/drv/ob.conf
NOTE: /usr/local/oracle/backup/.drv.solaris64/ob64 copied to
/usr/kernel/drv/sparcv9/ob
```

At this point, the Oracle Secure Backup software required for the roles you specified is installed on this host.

installob Step 7: (Optional, Media Servers Only): Configuring Tape Drives and Libraries

For a media server or administrative server installation, installob now displays the following output:

```
NOTE: The Oracle Secure Backup device driver has been successfully installed.
Would you like to configure (or reconfigure) any Oracle Secure Backup devices that
are attached to dlsun1976 [no]?
```

Note:

- Because `installob` includes both the administrative and media server roles when installing an administrative server, this prompt is displayed when installing on an administrative server even if there are no attached tape libraries or drives.
 - Although the following example concerns SCSI libraries and tape drives, the same procedures apply to Fibre Channel devices.
-
-

Configuring Oracle Secure Backup devices in `installob` creates the device special files required for Oracle Secure Backup to communicate with the devices.

In general, creating device special files can be performed using the `makedev` tool, described in "[Creating Device Special Files on Solaris and Linux](#)" on page 5-8. However, you can also use `installob` to configure several media devices attached to a host at once.

Note:

- You must collect the SCSI parameter information and assign Oracle Secure Backup logical unit numbers for the media devices on this host, as described in "[Determining SCSI Device Parameters on Linux and UNIX](#)" on page 5-1.
 - You can configure devices during the initial installation, or you can run `installob` again later, as described in "[Running installob Again for Device Configuration or Push Installs](#)" on page 4-15.
-
-

Choose one of the following:

- Enter `no` to not configure your devices at this time.

Note: If you are installing on an administrative server with no attached media devices, enter `no`.

- Enter `yes` to configure devices now.

Device configuration can be performed separately from the initial installation process, and can be performed using either the `installob` or `makedev` tools. This task is therefore described at more length in "[Creating Device Special Files with installob](#)" on page 5-10. Refer to that discussion if you require detailed instructions to perform this task.

In brief, `installob` prompts you for whether there are tape libraries connected to this host, and if so, the SCSI parameters for each, and then asks the same questions about tape drives. As described in "[Preparing to Install Oracle Secure Backup on Linux and UNIX](#)" on page 4-1, collecting this information for each of your media servers is part of preparing for the installation process.

The `installob` prompts and the required parameters are slightly different on Solaris and Linux, and are shown in the following examples:

- [Example 4-1, "Configuring Devices During Installation on Solaris"](#) on page 4-12
- [Example 4-2, "Configuring Devices During Installation on Linux"](#) on page 4-13

Note: If you enter the wrong parameters, device special file creation fails. To resolve the resulting errors, run `installob` again, as described in "[Running installob Again for Device Configuration or Push Installs](#)" on page 4-15, entering the correct values.

Example 4-1 Configuring Devices During Installation on Solaris

For Solaris host `dlsun1976`, assume there is one attached tape library and one attached drive. Based on "[Determining SCSI Device Parameters on Solaris](#)" on page 5-3, the SCSI parameters are as follows:

Device	Oracle Secure Backup LUN	SCSI Bus Name-Instance	SCSI Target ID	SCSI LUN
Exabyte library	0	glm1	1	0
Exabyte drive	0	glm1	0	0

Enter each parameter value in response to the prompts from `installob`. You can press `Enter` to accept a default value. Note, however, that the default SCSI parameters offered by the script may not be correct. For example:

```
Is dlsun1976 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 dlsun1976 [1]?
```

```
Please describe each tape library by answering the following questions.
```

```
Oracle Secure Backup logical unit number [0]:
SCSI bus name-instance [glm1]: glm1
SCSI target ID [3]: 1
SCSI lun 0-7 [0]: 0
```

```
Is the information you entered correct [yes]? yes
```

```
How many Oracle Secure Backup tape drives are attached to dlsun1976 [1]? 1
```

```
Please describe each tape drive by answering the following questions.
```

```
Oracle Secure Backup logical unit number [0]: 0
SCSI bus name-instance [glm1]: glm1
SCSI target ID [4]: 0
SCSI lun 0-7 [0]: 0
```

```
Is the information you entered correct [yes]? yes
```

```
- - - - -
```

```
Beginning device driver configuration and device special file creation.
```

```
NOTE: table for devlinks...
type=ddi_pseudo;name=ob;addr=0,0;minor=glm1 obt0
/dev/obt0 created
NOTE: table for devlinks...
type=ddi_pseudo;name=ob;addr=1,0;minor=glm1 obl0
/dev/obl0 created
```

```
- - - - -
```

NOTE: You must configure the new devices via the Web interface or via the command line using the obtool 'mkdev' command.

 The device special files are created. /dev/obt0 represents the tape drive, and /dev/obl0 represents the tape library. (Note that the l character is a lower-case L, not a numeral 1.)

When this step is complete, continue to ["installob Step 8: Push Installations to Other Hosts"](#) on page 4-14.

Example 4-2 Configuring Devices During Installation on Linux

For Linux host storabck05, assume there is one attached tape library and one attached drive. Based on ["Determining SCSI Device Parameters on Linux"](#) on page 5-2, the SCSI parameter values are as follows:

Device	Oracle Secure Backup LUN	Host Bus Adapter	SCSI Bus Address	Target ID	SCSI LUN
Library	0	0	0	2	0
Tape drive	0	0	0	4	0

Enter these parameters as prompted by installob. You can press Enter to accept a default value. Note, however, that the default SCSI parameters offered by the script may not be correct. For example:

```
Is storabck05 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 storabck05 [1]?
```

Please describe each tape library by answering the following questions.

```
Oracle Secure Backup logical unit number [0]: 0
Host SCSI adapter number 0-15 [0]: 4
SCSI bus address [0]: 0
SCSI target ID [3]: 1
SCSI lun 0-7 [0]: 0
```

```
Is the information you entered correct [yes]?
```

```
Is storabck05 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 storabck05 [1]?
```

Please describe each tape drive by answering the following questions.

```
Oracle Secure Backup logical unit number [0]: 0
Host SCSI adapter number 0-15 [0]: 4
SCSI bus address [0]: 0
SCSI target ID [4]: 2
SCSI lun 0-7 [0]: 0
```

```
Is the information you entered correct [yes]? yes
```

 Beginning device driver configuration and device special file creation.

```
NOTE: No driver installation is required for Linux.
/dev/obt0 created
/dev/obl0 created
```

- - - - -

NOTE: You must configure the new devices via the Web interface or via the command line using the obtool 'mkdev' command.

The device special files are created. /dev/obt0 represents the tape drive, and /dev/obl0 represents the tape library. (Note that the l character is a lower-case L, not a numeral 1.)

When this step is complete, continue to ["installob Step 8: Push Installations to Other Hosts"](#) on page 4-14.

installob Step 8: Push Installations to Other Hosts

At this point installob displays the following output:

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

You can now perform push installs from this server to other Linux or UNIX hosts, as described in ["Overview of Installation of Oracle Secure Backup on Linux and UNIX"](#) on page 1-12. To perform push installations, your environment must already meet the following conditions:

- You have staged the proper installation files on this host for the platform of the destination host, as described in ["Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script"](#) on page 4-3. For example, you cannot perform a push install from a Solaris 64-bit administrative server to Linux 32-bit if you did not include Linux 32-bit in the set of platforms specified during setup.
- You have configured permissions on the destination host so that you can use rsh as root on that host without providing a password.

Select one of the following:

- Enter no to not perform push installs at this time. You can run installob again to perform push installation at a future time. Installation continues with ["installob Step 9: Final Installation Summary"](#) on page 4-14.

For the examples in this section, enter no.

- Enter yes to perform a push install to another host.

installob prompts you for the name of the destination host. For example:

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

```
Enter the name of the destination host. installob then prompts for the host role (media server or client) and, for media servers, SCSI device information for the remote host.
```

```
installob asks repeatedly about whether to perform more installations until you enter no.
```

installob Step 9: Final Installation Summary

installob now displays a summary of installation activities during this session and exits. For example:

```
Installation summary:
```


Installation Mode	Host Name	OS Name	Driver Installed?	OS Move Required?	Reboot Required?
admin	dlsun1976	solaris	no	no	no

Oracle Secure Backup is now ready for your use.
#

Note: This installation summary does not include any information about device configuration tasks performed during the installob session.

Running installob Again for Device Configuration or Push Installs

You can run `installob` again on a host on which Oracle Secure Backup is already installed. Reasons to do so include:

- To configure additional tape libraries or drives on a media server without using `makedev` to configure them individually
- To perform push installations to other hosts from an administrative server

The install script detects the existing installation and asks you whether to install Oracle Secure Backup again (overwriting the previous installation), and whether you want to configure media devices (overwriting any existing device special files).

If you run the `installob` script on a host on which it has already been run, the script detects the existing installation and asks you whether to perform each installation stage again. You can skip tasks that were correctly completed before by entering `no` when asked whether you want to perform them again. For example, log in as `root`, change directory to the Oracle Secure Backup home, and run `installob`:

```
# cd /usr/local/oracle/backup
# install/installob
Welcome to installob, Oracle Secure Backup's UNIX installation program.
.
.
.
Oracle Secure Backup is already installed on this machine (dlsun1976).
Would you like to re-install it here [no]? no

Would you like to configure (or reconfigure) any Oracle Secure Backup devices that
are attached to dlsun1976 [no]?
.
.
.
```

You can then continue to device configuration, or to installing Oracle Secure Backup on other hosts.

Configuring a Domain and Devices on Linux and UNIX

This chapter describes configuring an administrative domain and configuring tape drives and libraries on Linux and Solaris media servers for use by Oracle Secure Backup. This chapter also describes configuring Network Attached Storage (NAS) filers and NAS libraries and tape drives.

This chapter covers the following topics:

- [Determining SCSI Device Parameters on Linux and UNIX](#)
- [Configuring an Administrative Domain on Linux and UNIX with obtool](#)
- [Creating Device Special Files on Solaris and Linux](#)
- [Configuring Devices on Linux and UNIX with obtool](#)
- [Taking Inventory of Devices on Linux and UNIX](#)
- [Configuring NAS Libraries and Tape Drives on Linux and UNIX](#)

Determining SCSI Device Parameters on Linux and UNIX

As part of installing Oracle Secure Backup and configuring your administrative domain, you will need to configure libraries and tape drives for use with Oracle Secure Backup. Collecting this information should be considered part of planning your administrative domain.

Oracle Secure Backup supports both SCSI and Fibre Channel devices for Linux and UNIX. The process of collecting the required parameters is the same for both device types.

To prepare for configuring each SCSI device, collect the device parameters required for your platform. On Linux this includes:

- The host bus adapter number for the SCSI adapter
- The SCSI bus address
- The SCSI target ID
- The SCSI logical unit number (or SCSI LUN)

On Solaris this includes:

- The SCSI bus name-instance
- The SCSI target ID
- The SCSI logical unit number (or SCSI LUN)

Also assign each tape library and each tape device an Oracle Secure Backup logical unit number, as described in "[Assigning Oracle Secure Backup Logical Unit Numbers to Devices](#)" on page 1-9.

Note: Do not confuse the SCSI logical unit number with the Oracle Secure Backup logical unit number. The Oracle Secure Backup logical unit number is a number you assign that is used in generating device special file names.

The following sections describe how to probe different operating systems for the required SCSI parameters.

- [Determining SCSI Device Parameters on Linux](#)
- [Determining SCSI Device Parameters on Solaris](#)

Determining SCSI Device Parameters on Linux

To obtain device information on Linux, use the `cat` command to view the contents of `/proc/scsi/scsi`. For example:

```
# cat /proc/scsi/scsi
```

[Example 5-1](#) shows sample output for a host called `storabck05` with two attached devices.

Example 5-1 Sample `/proc/scsi/scsi` Contents

Attached devices:

```
Host: scsi0 Channel: 00 Id: 02 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD2      Rev: 4772
  Type:   Sequential-Access      ANSI SCSI revision: 03
Host: scsi0 Channel: 00 Id: 04 Lun: 00
  Vendor: ADIC     Model: Scalar 24      Rev: 237A
  Type:   Medium Changer      ANSI SCSI revision: 02
```

Devices of type `Sequential-Access`, such as the first device in the list, are tape drives. Devices of type `Medium Changer`, such as the second device, are tape libraries.

For each device, the information needed is found in the line that reads:

```
Host: scsi0 Channel: 00 Id: 02 Lun: 00
```

The output can be interpreted as follows:

- The host bus adapter number is the numeric part of the value `scsin`. For example, for both devices in this output the host bus adapter number is 0.
- The value for `Channel` is the SCSI bus address. For example, in this output the SCSI bus address is 0.
- The value for `Id` is the target ID. For example, in this output the ID of the tape drive is 2, and the ID of the tape library is 4.
- The value for `Lun` is the SCSI LUN. For example, in this output the SCSI LUN of both devices is 0.

By convention, the tape library and tape drive can each be assigned 0 as the Oracle Secure Backup logical unit number.

Based on the output shown in [Example 5–1](#), [Table 5–1](#) summarizes the device information for storabck05.

Table 5–1 storabck05 Device Summary

Device	Host Bus Adapter	SCSI bus address	Target ID	SCSI LUN
Library	0	0	2	0
Tape drive	0	0	4	0

Determining SCSI Device Parameters on Solaris

To determine the SCSI device parameter information on Solaris, there are two major tasks required:

- To identify the SCSI target ID and SCSI LUN for each device, you must probe the SCSI bus of your system for attached devices using commands at the console in the Open Boot PROM. This task is described in ["Probing SCSI Target ID and LUN for Media Devices From Solaris Open Boot PROM"](#) on page 5-3.

Note: Accessing the Open Boot PROM requires shutting down and rebooting the operating system.

- To determine the SCSI bus name-instance for each device, you must install the Oracle Secure Backup Solaris device driver, and then view the devices that were recognized by the driver and associate them with the device information gathered in the first step.

Note: Installing the Oracle Secure Backup device driver is performed after loading Oracle Secure Backup with `setup`, as described in ["Loading Oracle Secure Backup Software on Solaris or Linux Using setup Script"](#) on page 4-3, but prior to installing Oracle Secure Backup as described in ["Installing Oracle Secure Backup on Linux or UNIX with installob"](#) on page 4-6.

This task is described in ["Viewing SCSI Bus Name-Instance Parameter Values in Solaris"](#) on page 5-4.

Probing SCSI Target ID and LUN for Media Devices From Solaris Open Boot PROM

To view SCSI target ID and SCSI LUN parameters for media devices from the Solaris Open Boot PROM:

1. Log into the media server as `root`.
2. Bring the host to run level 0. For example:

```
# init 0
```

The system shuts down and eventually the Open Boot PROM `ok` prompt is displayed on the console.

3. At the `ok` prompt, set the Open Boot `auto-boot?` variable to `false`. For example:

```
ok setenv auto-boot? false
auto-boot? = false
```

ok

4. At the `ok` prompt, run the Open Boot `reset-all` command. For example:

```
ok reset-all
```

The system resets and eventually returns to an `ok` prompt again.

5. At the `ok` prompt, run the Open Boot `probe-scsi-all` command to display the SCSI parameters for all devices attached to this host. For example:

```
ok probe-scsi-all
```

Find the information in the output that corresponds to your SCSI devices. For example, this excerpt from the output for `dl_sun1976` includes the following information for the tape library and drive:

```
/pci@1f,4000/scsi@3,1
Target 0
  Unit 0      Removable Tape      EXABYTE EXB-85058SQANXR1
Target 1
  Unit 0      Removable Device type 8  EXABYTE EXB-10e      1.8
```

The output can be interpreted as follows:

- The device tree path for the SCSI bus to which both devices are attached is `/pci@1f,4000/scsi@3,1`. Make a note of this value.

Note: This value is not used directly in Oracle Secure Backup device configuration, but is needed when determining the SCSI bus name-instance parameter for each device, using the process in "[Viewing SCSI Bus Name-Instance Parameter Values in Solaris](#)" on page 5-4.

- The value for `Target` is the target ID. For example, in this output the target ID of the tape drive is 0, and the target ID of the tape library is 1.
- The value for `Unit` is the SCSI LUN. For example, in this output the SCSI LUN of both devices is 0.

For this example, assign each device the Oracle Secure Backup logical unit number 0.

Record the discovered parameters and the assigned Oracle Secure Backup logical unit number for each device.

6. To reboot the host into Solaris, enter the following commands at the `ok` prompt:

```
ok setenv auto-boot? true
ok reset-all
```

Viewing SCSI Bus Name-Instance Parameter Values in Solaris

To determine the SCSI Bus name-instance parameter to use for each device in Oracle Secure Backup:

1. Log into your media server as `root`.
2. Change directory to the `install` subdirectory under the Oracle Secure Backup home. For example:

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

3. Run the `installdriver` script to install the Oracle Secure Backup driver. For example:

```
# installdriver
NOTE: /usr/local/oracle/backup/.drv.solaris64/ob copied to /usr/kernel/drv/ob
NOTE: /usr/local/oracle/backup/.drv.solaris64/ob.conf copied to
/usr/kernel/drv/ob.conf
NOTE: /usr/local/oracle/backup/.drv.solaris64/ob64 copied to
/usr/kernel/drv/sparcv9/ob
```

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

Once installed, the Oracle Secure Backup driver is associated with the media devices that it can control on this media server.

4. Run the following command to view devices associated with the Oracle Secure Backup driver:

```
# du -a /devices|grep ob|cut -f2
/devices/pci@1f,4000/scsi@3,1/ob@0,0:glm1
/devices/pci@1f,4000/scsi@3,1/ob@1,0:glm1
```

The output contains the needed device information.

5. Parse the output from Step 4 using information from the output of probing the SCSI bus in ["Probing SCSI Target ID and LUN for Media Devices From Solaris Open Boot PROM"](#) on page 5-3. For example, consider the line of output that reads:

```
/devices/pci@1f,4000/scsi@3,1/ob@1,0:glm1
```

- To identify the SCSI bus used for each device in the `du` output, match the device tree paths in the `probe-scsi-all` output to the device tree paths in the output from Step 4 for each device.

For example, in this case the bus used for both media devices is identified in the `probe-scsi-all` output as `/pci@1f,4000/scsi@3,1`, and in the `du` output as `/devices/pci@1f,4000/scsi@3,1`.

- The `ob@` in the path from the `du` output indicates that the device is controlled by the Oracle Secure Backup driver.
- The two numbers (in this case, 1, 0) following the `ob@` are the SCSI target ID and SCSI LUN for each device. For this example, the SCSI target ID is 1 and the SCSI LUN is 0. These values correspond to the Exabyte tape library on `d1sun1976`, as identified in ["Probing SCSI Target ID and LUN for Media Devices From Solaris Open Boot PROM"](#) on page 5-3.
- The value following the colon (`:`) is the needed SCSI bus name-instance value for this device. For this example, the value is `glm1`.

For host `d1sun1976`, parsing both lines of output from Step 4 leads to the final SCSI parameters shown in [Table 5-2](#).

Table 5-2 *d1sun1976 Tape Device Summary*

Device	Oracle Secure Backup LUN	SCSI Bus Name-Instance	SCSI Target ID	SCSI LUN
Exabyte library	0	glm1	1	0

Table 5–2 (Cont.) dlsun1976 Tape Device Summary

Device	Oracle Secure Backup LUN	SCSI Bus Name-Instance	SCSI Target ID	SCSI LUN
Exabyte drive	0	glm1	0	0

Configuring an Administrative Domain on Linux and UNIX with obtool

After Oracle Secure Backup has been installed on the hosts in your network, you can configure your administrative domain. This task involves configuring all media servers, client hosts, and Network Attached Storage (NAS) filers.

Note: You can also perform this task with the Oracle Secure Backup Web tool. See the *Oracle Secure Backup Administrator's Guide* for more information.

Use the `--access ob` option with the `mkhost` command to configure an Oracle Secure Backup host. The administrative server is configured by default during the installation process.

Note: For help on an `obtool` command, enter:

```
ob> help command
```

Note: In the following example, assume you have a Windows administrative server/media server called `BELLA`, a Linux media server called `storabck05` and a Solaris client host called `dlsun1976`.

To configure an administrative domain:

1. If you are already logged on to Oracle Secure Backup, skip to Step 3. Otherwise, log on as `root`.
2. To open Oracle Secure Backup, enter `obtool` at a system prompt. For example:

```
# obtool
```

The `ob>` prompt displays.

3. Configure each media server in your administrative domain. Specify options for access type, role, and IP address. For example:

```
ob> mkhost --access ob --role mediaserver --ip 133.2.22.59 storabck05
```

4. Configure each client in your administrative domain. Specify options for access type, role, and IP address. For example:

```
ob> mkhost --access ob --role client --ip 143.15.235.140 dlsun1976
```

5. To verify the results of configuring the administrative domain, use the `lshost` command in `obtool` to view the names and attributes of all the hosts in your administrative domain. For example:


```
ob> lshost
BELLA          admin,mediaserver,client      (via OB)  in service
dlsun1976      client                       (via OB)  in service
storabck05     mediaserver                   (via OB)  in service
```

Configuring Administrative Domain NAS Filers Using obtool

To configure a NAS filer as a member of the administrative domain, use the `mkhost` command in `obtool` with the `--access ndmp` option.

Note: You can also perform this task with the Oracle Secure Backup Web tool. See the *Oracle Secure Backup Administrator's Guide* for more information.

Under NAS, storage devices are made LAN-addressable, freeing stored data from a direct attachment to a specific locale.

The administrative server communicates with and manages NAS filers, which do not have Oracle Secure Backup installed, over Network Data Management Protocol (NDMP). NDMP defines a standard TCP/IP-based protocol for backing up and restoring data on heterogeneous networks, regardless of operating system or platform.

NDMP provides the following features:

- Minimizes demands on network resources
- Enables local backups and restores to tape
- Allows for centralized management and control

Note: In the following example, assume you have an administrative server/media server called `BELLA` and an NAS filer called `mynasfiler5`.

To configure an NAS filer:

1. If you are already logged on to Oracle Secure Backup, skip to Step 3. Otherwise, log on as `root`.
2. To open Oracle Secure Backup, enter `obtool` at a system prompt.
The `ob>` prompt displays.
3. Include an NAS filer in your administrative domain. Specify options for access type, role, IP address, and NDMP password. For example:

```
ob> mkhost --access ndmp --role mediaserver --ip 138.1.14.128 --ndmppass
mypassword
mynasfiler5
```

Note:

- Oracle Secure Backup typically provides a default NDMP password for configuration of NAS filers. Alternatively, users can set the password as the `--ndmppass` option of the `mkhost` command.

- For help on an `obtool` command, enter:

```
ob> help command
```

4. List the names and attributes of all the hosts in your administrative domain. For example:

```
ob> lshost
BELLA          admin,mediaserver,client      (via OB)  in service
dlsun1976      client                       (via OB)  in service
mynasfiler5    mediaserver                  (via NDMP) in service
storabck05     mediaserver                  (via OB)  in service
```

Creating Device Special Files on Solaris and Linux

Device special files are required before devices can be configured for use with Oracle Secure Backup. Specifically, device special files are links that will be referenced as attachments when devices are configured for use with Oracle Secure Backup.

After the device special files are created for devices, you can use the `mkdev` command in `obtool`, the Oracle Secure Backup Web tool, or the Oracle Secure Backup interface in Oracle Enterprise Manager to configure devices for use with Oracle Secure Backup.

This section assumes that you have already performed the following tasks:

1. Established your administrative domain so that media servers can be associated with their attached devices. See ["Configuring an Administrative Domain on Linux and UNIX with obtool"](#) on page 5-6.
2. Determined the operating system-specific SCSI (or Fibre Channel) device data required for device configuration. See ["Determining SCSI Device Parameters on Linux and UNIX"](#) on page 5-1.

You can create the device special files either by using the `installob` script or the `makedev` tool.

Follow the instructions in the appropriate section:

- [Creating Device Special Files with makedev](#)
- [Creating Device Special Files with installob](#)

Note: It is generally most convenient to use `installob` to configure all SCSI devices immediately after the installation process.

Creating Device Special Files with makedev

The `makedev` tool is used to create device special files for a single media device that Oracle Secure Backup uses to access the device.

The `makedev` tool provides an alternative to creating device special files with `installob`. `makedev` does not require you to run the `installob` script again. It handles only device special file creation and configuration, and does not relate to other installation and configuration tasks. `makedev` can be used on media servers before they are added to the administrative domain. `makedev` only creates device special files for a single device at a time, so if you have multiple devices to configure, consider using `installob`.

See Also: *Oracle Secure Backup Reference* for `makedev` syntax

This section assumes that you have already determined the operating system-specific SCSI (or Fibre Channel) device data required for device configuration and decided upon Oracle Secure Backup logical unit numbers for each device. See "[Determining SCSI Device Parameters on Linux and UNIX](#)" on page 5-1 for details on performing this task on your operating system.

For this example, `makedev` is used to configure the single tape library attached to Solaris 64-bit host `d1sun1976`. As determined in "[Determining SCSI Device Parameters on Linux and UNIX](#)" on page 5-1, the tape library is assigned Oracle Secure Backup logical unit number 0, and has SCSI bus name-instance `g1m1`, SCSI target ID 1, and SCSI logical unit number 0.

To use `makedev` to create device special files for a device:

1. Log on as `root`.

2. Change to the Oracle Secure Backup home directory. For example:

```
# cd /usr/local/oracle/backup
```

3. Enter the `makedev` command at the shell prompt:

```
# install/makedev
```

4. `makedev` prompts for the Oracle Secure Backup logical unit number. For example:

```
Enter logical unit number 0-31 [0]:
```

Enter the Oracle Secure Backup logical unit number for the device. For this example, enter 0.

Note: Do not confuse the Oracle Secure Backup logical unit number with the SCSI LUN.

5. `makedev` prompts for the device type, tape drive or tape library. For example:

```
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
tape library [d]:
```

Note: For a tape library, enter a lower-case L, not a number 1.

To specify a tape library, enter 1.

6. `makedev` prompts for the SCSI bus name-instance. For example:

```
Enter SCSI bus name [g1m1]:
```

7. Enter the SCSI bus name-instance for this device. For this example, enter `g1m1`.

8. `makedev` prompts for the SCSI target ID. For example:

```
Enter SCSI target id 0-15 [4]:
```

Enter the SCSI target ID for this device. For this example, enter 1.

9. `makedev` prompts for the SCSI logical unit number. For example:

```
Enter SCSI logical unit number (lun) 0-7 [0]:
```

Enter the SCSI logical unit number. For this example, enter 0.

10. `makedev` creates the device special file, displaying messages indicating its progress. For this example, on Solaris the following output appears:

```
NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=0,0;minor=glm1  obt0
/dev/obt0 created
```

`makedev` now exits. The device special file has been created.

Note: Oracle Secure Backup can also replace an old device, rather than adding a new one. If you re-use an Oracle Secure Backup logical unit number for a tape library or tape drive, the device special files for the old device are overwritten.

Before Oracle Secure Backup can access the device, you must still add the media server and the device to the administrative domain. See the following sections for the required tasks:

- ["Configuring Devices on Linux and UNIX with obtool"](#) on page 5-18
- ["Taking Inventory of Devices on Linux and UNIX"](#) on page 5-19

Creating Device Special Files with `installob`

You can create device special files using the `installob` installation script. The advantages of doing so include:

- You can perform this task immediately after the software installation process, if you have collected the SCSI device parameters for your platform as described in ["Determining SCSI Device Parameters on Linux and UNIX"](#) on page 5-1.
- You can enter SCSI parameters for all of your devices during one session. Using `makedev` requires that you perform this task separately for each device.

Follow the instructions appropriate for your operating system:

- [Configuring SCSI Devices on Solaris with `installob`](#)
- [Configuring SCSI Devices on Linux with `installob`](#)

Configuring SCSI Devices on Solaris with `installob`

Note: Although the following example describes SCSI libraries and tape drives, the same procedures apply to Fibre Channel devices.

To create device special files with `installob` on Solaris:

1. Start the `installob` script. From a shell prompt, change your working directory to the Oracle Secure Backup home, and start `installob` in interactive mode. For example:

```
# cd /usr/local/oracle/backup
# install/installob
Welcome to installob, Oracle Secure Backup's UNIX installation program.
.
.
.
You can choose to install Oracle Secure Backup in one of two ways:
  (a) interactively, by answering questions asked by this program, or
  (b) in batch mode, by preparing a network description file

Which installation method would you like to use (a or b) [a]? a
```

Enter `a` to run the script in interactive mode.

2. `installob` now prompts you about whether to reinstall the software. For example:

```
Oracle Secure Backup is already installed on this machine (dlsun1976).
Would you like to re-install it here [no]?
```

Enter `no` to leave the current software installation intact and move on to device configuration.

3. `installob` now prompts for whether to configure tape libraries and tape drives on this host. For example:

```
Would you like to configure (or reconfigure) any Oracle Secure Backup devices
that
are attached to dlsun1976 [no]?
```

Enter `yes` at this prompt to configure tape drives or libraries.

4. `installob` now prompts for the number of tape libraries attached to your host. For example:

```
How many Oracle Secure Backup SCSI tape libraries are attached to dlsun1976
[1]?
```

Enter the number of tape libraries to configure (or press `Enter` to accept the default). If there are no tape libraries, enter `0`.

5. If you have tape libraries to configure, `installob` now prompts you for information about each library. `installob` displays the following output:

```
Please describe each tape library by answering the following questions.
```

For each library, enter the device information you collected in ["Determining SCSI Device Parameters on Solaris"](#) on page 5-3.

For this example, the single tape library attached to `dlsun1976` is assigned Oracle Secure Backup logical unit number `0`, and has SCSI bus name-instance `glm1`, target ID `1`, and logical unit number `0`.

Note: When entering these values, do not confuse the Oracle Secure Backup logical unit number with the SCSI LUN.

The `installob` program displays the following output:

Oracle Secure Backup logical unit number [0]:

If the default is correct, then press `Enter`. Otherwise, enter the desired Oracle Secure Backup logical unit number for this device.

SCSI bus name-instance [glm1]:

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI bus name-instance for this device.

The `installob` program displays the following output:

SCSI target ID [0]:

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI target ID for this device.

The `installob` program displays the following output:

SCSI lun 0-7 [0]:

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI LUN for this device.

The `installob` program displays the following output:

Is the information you entered correct [yes]?

If the information is not correct, enter `no`. `installob` will prompt for the parameters for this library again. Otherwise, enter `yes` to continue to the next library.

6. Once you have entered parameters for all tape libraries, `installob` prompts for information about tape drives. For example:

Is dlsun1976 connected to any SCSI tape drives that you'd like to use with Oracle Secure Backup [no]?

If there are tape drives to configure, enter `yes`. Otherwise, enter `no`.

If you entered `yes`, then `installob` prompts for the number of tape drives. For example:

How many Oracle Secure Backup SCSI tape drives are attached to dlsun1976 [1]?

For this example, there is one tape drive attached, so enter `1` and press `Enter`.

7. `installob` now displays the following output:

Please describe each tape drive by answering the following questions.

`installob` now prompts you for the parameters for each tape drive. Enter the device information you collected in "[Determining SCSI Device Parameters on Solaris](#)" on page 5-3.

For this example, the single tape drive attached to `dlsun1976` is assigned Oracle Secure Backup logical unit number `0`, and has SCSI bus name-instance `glm1`, SCSI target ID `0`, and SCSI logical unit number `0`.

`installob` now displays the following output:

Oracle Secure Backup logical unit number [0]:

If the default is correct, press `Enter`. Otherwise, enter the correct Oracle Secure Backup logical unit number for this device.

The `installob` program displays the following output:

```
SCSI bus name-instance [glm1]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI bus name-instance value for this device.

The `installob` program displays the following output:

```
SCSI target ID [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI target ID for this device.

The `installob` program displays the following output:

```
SCSI lun 0-7 [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI LUN for this device.

The `installob` program displays the following output:

```
Is the information you entered correct [yes]?
```

If the information is not correct, enter **no**. `installob` will prompt for the parameters for this drive again. Otherwise, enter **yes** to continue to the next drive.

8. Once parameters are entered for all tape libraries and drives, `installob` configures the device drivers for the devices and creates the device special files. It displays the following output:

```
Beginning device driver configuration and device special file creation.
This will likely take between one and five minutes.
```

`installob` generates descriptive output for each device it configures during this process. For example:

```
NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=0,0;minor=pci1000,f1    obt0
/dev/obt0 created
NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=0,1;minor=pci1000,f1    obl0
/dev/obl0 created
-----
```

At the end of the process, device special files have been created for two devices: `/dev/obt0` (the tape drive) and `/dev/obl0` (the library).

When the process is complete, `installob` generates the following output:

```
NOTE: You must configure the new devices via the Web interface or via
      the command line using the obtool 'mkdev' command.
-----
```

Note: Note that the name of the tape library device special file `/dev/obl0` contains a lower-case letter `L`, not a number `1`.

9. `installob` now displays the following prompt:

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

Enter `no`. The `installob` script then displays the installation summary described in ["installob Step 9: Final Installation Summary"](#) on page 4-14 and exits

Note: As stated in the output of `installob`, you must complete configuration of the devices as part of the administrative domain before they can be used. These tasks cannot be performed until the media server and its devices have been added to the administrative domain.

The remaining tasks are described in the following sections:

- ["Configuring Devices on Linux and UNIX with obtool"](#) on page 5-18
 - ["Taking Inventory of Devices on Linux and UNIX"](#) on page 5-19
-
-

Configuring SCSI Devices on Linux with `installob`

Note: Although the following example describes SCSI libraries and tape drives, the same procedures apply to Fibre Channel devices.

To create device special files with `installob` on Linux:

1. Start the `installob` script. From a shell prompt, change your working directory to the Oracle Secure Backup home, and start `installob` in interactive mode. For example:

```
# cd /usr/local/oracle/backup
# install/installob
Welcome to installob, Oracle Secure Backup's UNIX installation program.
.
.
.
You can choose to install Oracle Secure Backup in one of two ways:
  (a) interactively, by answering questions asked by this program, or
  (b) in batch mode, by preparing a network description file

Which installation method would you like to use (a or b) [a]? a
```

Enter `a` to run the script in interactive mode.

2. `installob` now prompts you about whether to reinstall the software. For example:

```
Oracle Secure Backup is already installed on this machine (storabck05).
Would you like to re-install it here [no]?
```

Enter `no` to leave the current software installation intact and move on to device configuration.

3. `installob` now prompts for whether to configure tape libraries and tape drives on this host. For example:

```
Would you like to configure (or reconfigure) any Oracle Secure Backup devices
that
are attached to storabck05 [no]?
```

Enter `yes` at this prompt to configure tape drives or libraries.

4. `installob` now prompts for the number of tape libraries attached to your host. For example:

```
How many Oracle Secure Backup SCSI tape libraries are attached to storabck05
[1]?
```

Enter the number of tape libraries to configure (or press `Enter` to accept the default). If there are no tape libraries, enter 0.

5. If you have tape libraries to configure, `installob` now prompts you for information about each library. `installob` displays the following output:

```
Please describe each tape library by answering the following questions.
```

For each library, enter the device information you collected in "[Determining SCSI Device Parameters on Linux](#)" on page 5-2.

For this example, the single tape library attached to `storabck05` is assigned Oracle Secure Backup logical unit number 0, and has host SCSI adapter number 0, SCSI bus address 0, SCSI target ID 2, and SCSI logical unit number 0.

Note: When entering these values, do not confuse the Oracle Secure Backup logical unit number with the SCSI LUN.

The `installob` program displays the following output:

```
Oracle Secure Backup logical unit number [0]:
```

If the default is correct, then press `Enter`. Otherwise, enter the desired Oracle Secure Backup logical unit number for this device. For this example, enter 0.

`installob` now displays the following output:

```
Host SCSI adapter number [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct host SCSI adapter number for this device. For this example, enter 0.

```
SCSI bus address [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI bus address for this device. For this example, enter 0.

The `installob` program displays the following output:

```
SCSI target ID [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI target ID for this device. For this example, enter 2.

The `installob` program displays the following output:

```
SCSI lun 0-7 [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI LUN for this device. For this example, enter 0.

The `installob` program displays the following output:

```
Is the information you entered correct [yes]?
```

If the information is not correct, enter `no`. `installob` will prompt for the parameters for this library again. Otherwise, enter `yes` to continue to the next library.

6. Once you have entered parameters for all tape libraries, `installob` prompts for information about tape drives. For example:

```
Is storabck05 connected to any SCSI tape drives that you'd like to use with
Oracle Secure Backup [no]?
```

If there are tape drives to configure, enter `yes`. Otherwise, enter `no`.

If you entered `yes`, then `installob` prompts for the number of tape drives. For example:

```
How many Oracle Secure Backup SCSI tape drives are attached to storabck05 [1]?
```

For this example, there is one tape drive attached, so enter `1` and press `Enter`.

7. `installob` now displays the following output:

```
Please describe each tape drive by answering the following questions.
```

`installob` now prompts you for the parameters for each tape drive. Enter the device information you collected in "[Determining SCSI Device Parameters on Linux](#)" on page 5-2.

For this example, the single tape drive attached to `storabck05` is assigned Oracle Secure Backup logical unit number `0`, and has host SCSI adapter number `0`, SCSI bus address `0`, SCSI target ID `4`, and SCSI logical unit number `0`.

For example:

```
Oracle Secure Backup logical unit number [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct Oracle Secure Backup logical unit number for this device. For this example, enter `0`.

`installob` now displays the following output:

```
Host SCSI adapter number [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct host SCSI adapter number for this device. For this example, enter `0`.

```
SCSI bus address [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI bus address for this device. For this example, enter `0`.

The `installob` program displays the following output:

```
SCSI target ID [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI target ID for this device. For this example, enter `4`.

The `installob` program displays the following output:

```
SCSI lun 0-7 [0]:
```

If the default is correct, press `Enter`. Otherwise, enter the correct SCSI LUN for this device. For this example, enter `0`.

The `installob` program displays the following output:

Is the information you entered correct [yes]?

If the information is not correct, enter **no**. `installob` will prompt for the parameters for this drive again. Otherwise, enter **yes** to continue to the next drive.

8. Once parameters are entered for all tape libraries and drives, `installob` configures the device drivers for the devices and creates the device special files. It displays the following output:

```
Beginning device driver configuration and device special file creation.
This will likely take between one and five minutes.
```

`installob` generates descriptive output for each device it configures during this process. For example:

```
-----
Beginning device driver configuration and device special file creation.

NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=0,0;minor=glm1  obt0
/dev/obt0 created
NOTE: table for devlinks...
      type=ddi_pseudo;name=ob;addr=1,0;minor=glm1  obl0
/dev/obl0 created
-----
```

At the end of the process, device special files have been created for two devices: `/dev/obt0` (the tape drive) and `/dev/obl0` (the library).

When the process is complete, `installob` generates the following output:

```
NOTE: You must configure the new devices via the Web interface or via
      the command line using the obtool 'mkdev' command.
```

Note: Note that the name of the tape library device special file `/dev/obl0` contains a lower-case letter L, not a number 1.

9. `installob` now displays the following prompt:

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

Enter **no**. The `installob` script then displays the installation summary described in ["installob Step 9: Final Installation Summary"](#) on page 4-14 and exits.

Note: As stated in the output of `installob`, you must complete configuration of the devices as part of the administrative domain before they can be used. These tasks cannot be performed until the media server host has been added to the administrative domain.

The remaining tasks are described in the following sections:

- ["Configuring Devices on Linux and UNIX with obtool"](#) on page 5-18
 - ["Taking Inventory of Devices on Linux and UNIX"](#) on page 5-19
 - ["Configuring NAS Libraries and Tape Drives on Linux and UNIX"](#) on page 5-20
-
-

Configuring Devices on Linux and UNIX with obtool

This section illustrates the configuration of tape libraries and tape drives on your media servers. This step assigns user-defined names to these devices for use in later Oracle Secure Backup procedures. The following procedure uses `obtool` commands, although you can also use the Oracle Secure Backup Web tool or Oracle Enterprise Manager to assign Oracle Secure Backup device names.

For the following examples, assume that you are configuring devices on a Solaris system on which the following device special files have been created:

- `/dev/ob10` (the tape library)
- `/dev/obt0` (the tape drive)

While this example demonstrates performing this task on Solaris, the `obtool` commands on Linux are the same.

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

If necessary, log in as `root`, and then open Oracle Secure Backup, type `obtool` at a system prompt. When the `ob>` prompt is displayed, perform the following steps for each tape library on each media server:

1. Create an Oracle Secure Backup device object with a user-defined name for each tape library. The device special file is the attach point for the library.

For example, you can associate the name `tc-lib` with `/dev/ob10` on host `dlsun1976` as follows:

```
ob> mkdev --type library --attach dlsun1976:/dev/ob10 tc-lib
```

Note:

- If you attempt to assign device names to devices on a host that is not already configured as a media server, then Oracle Secure Backup automatically configures the host as a media server.
- For help on an `obtool` command, enter:

```
ob> help command
```

2. For each tape drive attached to the library you defined in the previous step, create an Oracle Secure Backup device object with a user-defined name for the tape drive. The library for the drive is referenced using the library name that you created in the previous step.

Note: Oracle Secure Backup identifies each tape drive within a library by its data transfer element (DTE) number. You must assign each device a `dte` if `library` is specified. DTEs are numbered 1 through *n*. See *Oracle Secure Backup Reference* for more details on the `--dte` option to `mkdev`.

The following example associates the name `tc-tape` with the tape drive `/dev/obt0` in the library named `tc-lib`:

```
ob> mkdev --type tape --library tc-lib --dte 1 --attach dlsun1976:/dev/obt0
tc-tape
```

You can verify the configuration information for your devices using the `lsdev` command in `obtool`. For example:

```
ob> lsdev
```

Oracle Secure Backup displays the following output:

```
library    tc-lib          in service
drive 1   tc-tape        in service
```

See Also: *Oracle Secure Backup Administrator's Guide* to learn how to use the Oracle Secure Backup Web tool

Taking Inventory of Devices on Linux and UNIX

After you have configured your devices, use `obtool` to take inventory of the volumes in your tape library.

Note: You can also perform this task with the Oracle Secure Backup Web tool. See the *Oracle Secure Backup Administrator's Guide* for more information.

This example assumes that your devices have been named `tc-lib` (a library) and `tc-tape` (a tape drive) as described in "[Configuring Devices on Linux and UNIX with obtool](#)" on page 5-18.

1. Run the `inventory` command in `obtool`, specifying the name of the library of which you are taking inventory. This causes Oracle Secure Backup to actually inventory the device. For example:

```
ob> inventory -L tc-lib
```

2. To view the inventory information for the library, use the `lsvol` command in `obtool`. For example:

```
ob> lsvol -L tc-lib
```

The command generates the following output:

```
Inventory of library tc-lib:
in   3:          barcode 00000153
in   4:          barcode 00000154
in   5:          barcode 000005
in   6:          barcode 00000151
```

```
in 7:          barcode 00000134
in 8:          barcode 00000133
in 9:          barcode 00000131
in 10:         barcode 00000130
in 11:         barcode 00000129
in 12:         barcode 00000128
in 15:         occupied
in dte:        barcode 00000152, lastse 2
```

Configuring NAS Libraries and Tape Drives on Linux and UNIX

This section explains how to configure the libraries and tape drives attached to a Network Attached Storage (NAS) Filer so that the filer can communicate with Oracle Secure Backup.

Libraries and tape devices attached to NAS filers are automatically configured by the operating system on which the NAS device runs. Both SCSI device and Fibre Channel configuration occur behind the scenes, transparent to the user.

Nevertheless, you must still make libraries and tape drives accessible to the Oracle Secure Backup software. You accomplish this task by performing device discovery on each of the NAS filers in the administrative domain.

Note: An administrative server can use an NAS filer with attached devices as a media server.

Making NAS Device Names Accessible to Oracle Secure Backup

Oracle Secure Backup can detect devices attached to NAS filers that are part of an administrative domain and, based on this information, automatically update the domain's device configuration.

See Also: *Oracle Secure Backup Administrator's Guide* to learn how to use the Oracle Secure Backup Web tool to perform this task

To discover NAS device names and make them accessible to Oracle Secure Backup, log on to the administrative server as `root` and start `obtool`. Then complete the following steps:

1. Use the `obtool discoverdev` command to detect changes in NAS device configuration and update the administrative domain with the correct information about your devices.

This example illustrates using `discoverdev` in `obtool` on a NAS device called `mynasfiler5`, which was configured previously using `mkhost`.

See "[Configuring Administrative Domain NAS Filers Using obtool](#)" on page 5-7 for information on configuring hosts.

```
ob> discoverdev --verbose --host mynasfiler5
```

The command generates the following output:

```
Info: beginning device discovery for mynasfiler5.
Info: connecting to mynasfiler5

Info: devices found on mynasfiler5:
Info: ATL      1500      ...
Info: mc3  attrs= [none]
```

```

Info: WWN: [none]
Info: SN: PMC13A0007
Info: Quantum SDLT220...
Info: nrst7a attrs= norewind raw
Info: WWN: [none]
Info: SN: CXB45H1313
Info: Quantum SDLT220...
Info: nrst8a attrs= norewind raw
Info: WWN: [none]
Info: SN: PKB51H0286

mynasfiler5_mc3 (new library)
WWN: [none]
new attach-point on mynasfiler5, rawname mc3

mynasfiler5_nrst7a (new drive)
WWN: [none]
new attach-point on mynasfiler5, rawname nrst7a

mynasfiler5_nrst8a (new drive)
WWN: [none]
new attach-point on mynasfiler5, rawname nrst8a

```

Note:

- By convention, NAS library names are characterized by `mc` and NAS tape drives are characterized by `nrst`.
- For help on an `obtool` command, enter:

```
ob> help command
```

2. List summary device information. For example:

```
ob> lsdev
```

The command generates the following output:

```

library   mynasfiler5_mc3      not in service
drive     mynasfiler5_nrst7a  not in service
drive     mynasfiler5_nrst8a  not in service
library   tc-lib                in service
drive 1   tc-tape              in service

```

Unless you change the default policy value for a device, every newly discovered NAS device is by default placed in the `not in service` state.

Note: The device names assigned automatically by Oracle Secure Backup are generated from the library and tape drive names reported by the NAS device. These names tend to be long and unwieldy. Consider renaming NAS library and tape drives to more concise names.

The long names are used in this example.

3. Specify the name of the library in which the first tape drive resides. For example:

```
ob> chdev --library mynasfiler5_mc3 --dte 1 mynasfiler5_nrst7a
```

4. Specify the name of the library in which the second tape drive resides. For example:

```
ob> chdev --library mynasfiler5_mc3 --dte 2 mynasfiler5_nrst8a
```

5. Put the library and tape drives in service.

```
ob> chdev --inservice mynasfiler5_mc3 mynasfiler5_nrst7a mynasfiler5_nrst8a
```

6. List the library and devices now in service. For example:

```
ob> lsdev mynasfiler5_mc3
```

The command generates the following output:

```
library    mynasfiler5_mc3      in service
drive 1    mynasfiler5_nrst7a   in service
drive 2    mynasfiler5_nrst8a   in service
```

You may choose to take another inventory of your system at this point.

See Also: ["Taking Inventory of Devices on Linux and UNIX"](#) on page 5-19

Uninstalling Oracle Secure Backup

This chapter describes how to uninstall Oracle Secure Backup. The following topics are covered:

- [Uninstalling Oracle Secure Backup on Windows](#)
- [Uninstalling Oracle Secure Backup on Linux or UNIX](#)

Uninstalling Oracle Secure Backup on Windows

Complete the following steps to uninstall Oracle Secure Backup on Windows:

1. Open the Task Manager and click the **Processes** tab.
2. Select the `obhttpd.exe` image name and click **End Process**. This action stops the Apache Web server.
3. Open the Windows Control Panel and click **Add or Remove Programs**.
4. Select **Oracle Secure Backup** from the Currently Installed Programs window.
5. Click **Remove**. The Add or Remove Programs confirmation window displays.
6. Click **Yes** to remove Oracle Secure Backup from your computer.
7. If you configured your host as an administrative server, an additional window opens asking if you want to preserve the files specific to your administrative domain. Choose one of the following:
 - Click **Delete** if you do not want to retain the administrative domain files.
 - Click **Keep** if you want to retain the administrative domain files.

Note: If you click **Keep** to retain the administrative domain files, then you can reinstall the Oracle Secure Backup software later and the configuration of your administrative domain is preserved.

8. Restart the computer.

Oracle Secure Backup is now uninstalled from your host.

Uninstalling Oracle Secure Backup on Linux or UNIX

The following example uninstalls Oracle Secure Backup on a Linux host called `storaback04`. The same procedures apply to Solaris hosts.

In this example Oracle Secure Backup is uninstalled from the administrative server. The procedure is the same when using the administrative server to uninstall Oracle Secure Backup from other hosts.

1. Log on as `root` to the administrative server.
2. Shut down Oracle Secure Backup-related processes such as the http processes for Oracle Secure Backup Web tool. To identify processes for Oracle Secure Backup, use the following command:

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

Use `kill -9 pid` commands to kill each process in the list associated with Oracle Secure Backup.

3. Change directory to the parent directory of the Oracle Secure Backup home directory. For example:

```
# cd /usr/local/oracle
```

Note: If you uninstall Oracle Secure Backup from the administrative server, then the `uninstallob` uninstall script removes the Oracle Secure Backup home directory at the end of the uninstall process.

4. Run the `uninstallob` program:

```
# backup/install/uninstallob
```

The following output appears:

```
Welcome to Oracle's Un-Install program for Oracle Secure Backup.
```

```
This program will remove Oracle Secure Backup from one or more machines on your network. If you are going to remove Oracle Secure Backup from this host, make sure you do it last (lest the un-install program disappear before you're done with it).
```

```
For most questions, a default answer appears enclosed in square brackets. Press return to select this answer.
```

```
Please wait a few seconds while I learn about this machine... done.
```

```
- - - - -
```

```
Enter the name of a host from which you'd like to remove Oracle Secure Backup:
```

5. Enter the host name. For example:

```
storabck05
```

The following output appears:

```
Just a moment while I learn about storabck05...done.
```

```
You selected this machine, storabck05, from which to remove Oracle Secure Backup.
```

```
(Note: once Oracle Secure Backup is removed from this host, you will not be able to remove Oracle Secure Backup from other hosts.)
```

```
Enter the name of a obparameters file that was used to install Oracle Secure Backup on storabck05 [install/obparameters]:
```

6. Press the `Enter` key to accept the default.

The following output appears:

```
Do you want to remove the Oracle Secure Backup directory [no]?
```

7. Select one of the following:
- Enter `no` if you do not want to remove the Oracle Secure Backup home directory.
 - Enter `yes` to remove the Oracle Secure Backup home directory.

Note: If you answer `yes`, then all files in the home directory will be deleted. The only exception is the `admin` directory, which you can elect to retain by answering `yes` at the next prompt.

Regardless of whether you enter `yes` or `no`, the following output appears:

```
Do you want to save the admin directory on storabck05 [yes]?
```

8. Select one of the following:
- Enter `no` to remove the administrative directory.
 - Enter `yes` to save the administrative directory.

Note: If you keep the `admin` directory, then you can reinstall the Oracle Secure Backup software later without destroying your administrative domain.

This example assumes that you have elected to retain both the backup directory and the `admin` directory. The following output appears:

```
Oracle Secure Backup will be removed from this host.
The Oracle Secure Backup directory will be retained.
The admin directory will be retained.
```

```
Do you wish to continue [no]?
```

9. Select one of the following:
- Enter `no` to exit the program.

The following output displays:

```
Would you like to remove Oracle Secure Backup from any other machines
[yes]?
```

You are given the opportunity to select other hosts from which to remove Oracle Secure Backup. If you enter `yes`, the uninstall process in Steps 4 through 7 is repeated for a new host. If you enter `no`, the uninstaller exits.

- Enter `yes` to continue.

The following output appears:

```
Un-installing Oracle Secure Backup from storabck05...
```

```
Removing /usr/bin links to Oracle Secure Backup components...
Removing /etc links to Oracle Secure Backup components...
```

```
Removing /lib links to Oracle Secure Backup components...
Stopping Oracle Secure Backup daemons...
Waiting for daemons to stop...
Removing (if necessary) logic to start Oracle Secure Backup daemons at boot
time...
Removing local database directory /usr/etc/ob...
Cleaning out /usr/tmp...
Removing /etc/obconfig...
Saving /usr/local/oracle/backup/admin...
Removing everything else in /usr/local/oracle/backup...
```

Oracle Secure Backup has been successfully removed from storabck05.

Oracle Secure Backup is now uninstalled.

Note:

- If you uninstall Oracle Secure Backup from the local machine, then the `uninstallob` script removes the directory `/usr/local/oracle/backup` when it completes.
 - On Solaris it may be necessary to remove the driver for Oracle Secure Backup manually from each media server after uninstalling the rest of the product. See ["Manually Uninstalling the Oracle Secure Backup Driver on Solaris"](#) on page C-3 for details.
-
-

Oracle Secure Backup Directories and Files

This appendix explains the structure and contents of the Oracle Secure Backup directories. The following topics are covered:

- [Oracle Secure Backup Home Directory](#)
- [Administrative Server Directories and Files](#)
- [Media Server Directories and Files](#)
- [Client Host Directories and Files](#)

Note: Some of the directories and files listed in this appendix are not created until after a backup has been performed by Oracle Secure Backup.

Oracle Secure Backup Home Directory

When you installed Oracle Secure Backup, you specified an Oracle Secure Backup home directory for the installation. The recommended defaults for the Oracle Secure Backup home are:

- On Windows:
`C:\Program Files\Oracle\Backup`
- On Linux and UNIX:
`/usr/local/oracle/backup`

The Oracle Secure Backup home directory is created on every host where you install Oracle Secure Backup, although the contents of the directory vary depending on the roles you assigned to the host.

Oracle Secure Backup Configuration File

Each host on which Oracle Secure Backup is installed contains a configuration file that records details of the configuration of Oracle Secure Backup on the host. On Windows, the configuration file is called `obconfig.txt` in the `db` subdirectory of the Oracle Secure Backup home. On Linux and UNIX, the file is called `obconfig` and is located in the `/etc` directory.

Administrative Server Directories and Files

An administrative server contains a set of executables and data files for each installed operating system.

This section contains the following tables:

- [Table A-1](#) lists the directories and files on an administrative server on any operating system.
- [Table A-2](#) lists the directories on an administrative server that are specific to Windows operating systems.
- [Table A-3](#) lists the directories and files on an administrative server that are specific to Linux and UNIX operating systems.

Table A-1 Architecture-Independent Directories and Files for an Administrative Server

Directory or File	Description
admin/	Administrative domain databases
admin/config/	Configuration databases
admin/config/class/	User class data
admin/config/dataset/	Datasets
admin/config/default/	Defaults and policies data
admin/config/device/	Device data
admin/config/family/	Media family data
admin/config/host/	Host data
admin/config/schedule/	Backup schedules
admin/config/summary/	Summary data
admin/config/user/	User data
admin/history/	History data generated by Oracle Secure Backup
admin/history/edcf/	Network Data Management Protocol (NDMP) environment data container files
admin/history/host/	Host-specific history data
admin/history/host/ <i>host_name</i> /	Backup catalog for <i>host_name</i>
admin/log/	Generated log files
admin/log/device/	Log files for devices
admin/log/device/ <i>device_name</i> /	Log files for <i>device_name</i>
admin/log/index/	Backup catalog manager logs
admin/log/scheduler/	Scheduler-generated logs
admin/log/scheduler/summary/	Log files for email summary reports
admin/state/	Dynamic state data
admin/state/device/	Device state
admin/state/device/ <i>device_name</i> /	State for <i>device_name</i>
admin/state/family/	Media family state
admin/state/family/ <i>media_family_name</i>	State for <i>media_family_name</i>
admin/state/general/	Miscellaneous state

Table A-1 (Cont.) Architecture-Independent Directories and Files for an Administrative Server

Directory or File	Description
admin/state/host/	Host state
admin/state/host/host_name/	State for <i>host_name</i>
admin/state/scheduler/	Scheduler state
admin/state/scheduler/job/	Job state
apache/	Apache Web server files
apache/conf/	Apache server configuration files
apache/conf/ssl.crl/	Apache server certificate revocation list
apache/conf/ssl.crt/	Apache server certificate
apache/conf/ssl.csr/	Apache server certificate signing request
apache/conf/ssl.key/	Apache server SSL key
apache/conf/ssl.prm/	Apache server public DSA parameter files
apache/htdocs/	Apache server HTML document root
apache/htdocs/css/	Apache server custom style sheets
apache/htdocs/include/	Apache server PHP files
apache/htdocs/include/policies/	Apache server PHP files
apache/htdocs/js/	Apache server Java script files
apache/htdocs/php/	Apache server PHP files
apache/images/	Apache server Web image files
apache/logs/	Apache server log files
bin/	Executables or links to executables: <ul style="list-style-type: none"> ■ In an installation on a Windows operating system, this directory contains the executables for the Windows operating system. ■ In an installation on a Linux or UNIX operating system, this directory contains links to the executables for the operating system.
device/	Device tables
help/	Oracle Secure Backup help files
samples/	Sample tools for scripting with Oracle Secure Backup

Table A-2 Windows Operating System Directories for an Administrative Server

Directory	Description
db\xcr\	Transcripts for jobs that ran on this host
db\.hostid	Identifying information for this host
db\wallet	Security credentials for this host
temp\	Log file for <i>observed</i> and temporary files

Table A-3 Linux and UNIX Operating System Directories and Files for an Administrative Server

Directory or File	Description
<code>.bin.operating_system/</code>	Executables for <i>operating_system</i> , where <i>operating_system</i> is a derivative of the operating system name. For example, the directory for Sun Solaris is <code>.bin.solaris</code> .
<code>.drv.operating_system/</code>	Device drivers for <i>operating_system</i>
<code>etc/</code>	Architecture-independent executables for daemons and maintenance tools
<code>.etc.operating_system/</code>	Daemons and utility programs for <i>operating_system</i>
<code>install/</code>	Installation programs
<code>lib/</code>	Architecture-independent shared library for the system backup to tape (SBT) interface
<code>.lib.operating_system/</code>	Shared library for the SBT interface for <i>operating_system</i> , where <i>operating_system</i> is a derivative of the operating system name. For example, the directory for Sun Solaris is <code>.lib.solaris</code> .
<code>man/</code>	Man pages for Oracle Secure Backup components
<code>man/man1</code>	Man pages for Oracle Secure Backup executables
<code>man/man8</code>	Man pages for daemons and maintenance tools
<code>tools.operating_system/</code>	Maintenance tools
<code>/usr/etc/ob/.hostid</code>	Identifying information for this host
<code>/usr/etc/ob/wallet</code>	Security credentials for this host
<code>/usr/etc/ob/xcr/</code>	Transcripts for jobs that ran on this host
<code>/usr/tmp/</code>	Log files for <code>observed</code> files, <code>obndmpd</code> files, and temporary files
<code>.wrapper</code>	Shell program that selects an executable from a <code>.bin.*</code> or <code>.etc.*</code> directory, based on the computer architecture of the host executing the command. Symbolic links and the architecture-independent <code>.wrapper</code> shell program enable hosts to contain executables for multiple computer architectures.

Media Server Directories and Files

Every Windows and Linux or UNIX media server contains a subset of the directories and files found on an administrative server. The only files included are those pertinent to the server's computer architecture and its function as a media server and client.

This section contains the following tables:

- [Table A-4](#) lists the directories on a media server on any operating system.
- [Table A-5](#) lists the directories on a media server that are specific to Windows operating systems.
- [Table A-6](#) lists the directories and files on a media server that are specific to Linux and UNIX operating systems.

Table A-4 Architecture-Independent Directories for a Media Server

Directory	Description
bin/	Executables or links to executables: <ul style="list-style-type: none"> ■ In an installation on a Windows operating system, this directory contains the executables for the Windows operating system. ■ In an installation on a Linux or UNIX operating system, this directory contains links to the executables for the operating system.
device/	Device tables

Table A-5 Windows Operating System Directories for a Media Server

Directory	Description
drv\	Device driver
help\	Oracle Secure Backup help files
temp\	Log file for <code>observed</code> and temporary files
db\.hostid	Identifying information for this host
db\wallet	Security credentials for this host

Table A-6 Linux and UNIX Operating System Directories and Files for a Media Server

Directory or File	Description
<code>.bin.operating_system/</code>	Executables for <i>operating_system</i> , where <i>operating_system</i> is a derivative of the operating system name. For example, the directory for Sun Solaris is <code>.bin.solaris</code> .
<code>.drv.operating_system/</code>	Device drivers for <i>operating_system</i>
<code>etc/</code>	Architecture-independent executables for daemons and maintenance tools
<code>.etc.operating_system/</code>	Daemons and utility programs for <i>operating_system</i>
<code>man/</code>	Man pages for Oracle Secure Backup components
<code>/usr/etc/ob/.hostid</code>	Identifying information for this host
<code>/usr/etc/ob/xcr/</code>	Transcripts for jobs that ran on this host
<code>/usr/tmp/</code>	Log files for <code>observed</code> files, <code>obndmpd</code> files, and temporary files
<code>.wrapper</code>	Shell program that selects an executable from a <code>.bin.*</code> or <code>.etc.*</code> directory, based on the computer architecture of the host executing the command. Symbolic links and the architecture-independent <code>.wrapper</code> shell program enable hosts to contain executables for multiple computer architectures.

Client Host Directories and Files

Every Windows and Linux or UNIX computer that only acts as a client host contains the minimum set of directories and files needed for Oracle Secure Backup operations.

This section contains the following tables:

- [Table A-7](#) lists the directory on a client host on any operating system.
- [Table A-8](#) lists the directories on a client host that are specific to Windows operating systems.

- [Table A-9](#) lists the directories and files on a client host that are specific to Linux and UNIX operating systems.

Table A-7 Architecture-Independent Directory for a Client Host

Directory	Description
bin/	Executables or links to executables <ul style="list-style-type: none"> ■ In an installation on a Windows operating system, this directory contains the executables for the Windows operating system. ■ In an installation on a Linux or UNIX operating system, this directory contains links to the executables for the operating system.

Table A-8 Windows Operating System Directories and Files for a Client Host

Directory	Description
db\ .hostid	Identifying information for this host
db\wallet	Security credentials for this host.
temp\	Log file for observed and temporary files
help\	Oracle Secure Backup help files

Table A-9 Linux and UNIX Operating System Directories and Files for a Client Host

Directory or File	Description
.bin.operating_system/	Executables for <i>operating_system</i> , where <i>operating_system</i> is a derivative of the operating system name. For example, the directory for Sun Solaris is .bin.solaris.
etc/	Architecture-independent executables for daemons and maintenance tools
.etc.operating_system/	Daemons and utility programs for <i>operating_system</i>
man/	Man pages for Oracle Secure Backup components
/usr/etc/ob/.hostid	Identifying information for this host
/usr/etc/ob/xcr/	Transcripts for jobs that ran on this host
/usr/tmp/	Log files for observed files, obndmpd files, and temporary files
.wrapper	Shell program that selects an executable from a .bin.* or .etc.* directory, based on the computer architecture of the host executing the command. Symbolic links and the architecture-independent .wrapper shell program enable hosts to contain executables for multiple computer architectures.

Oracle Secure Backup obparameters Installation Parameters

This appendix describes the installation parameters for Oracle Secure Backup on Linux or UNIX. You can set these parameters in the `obparameters` file, which is a plain text file located in the `install` subdirectory of the Solaris or Linux Oracle Secure Backup home.

Note: The `obparameters` file is not used in Windows installations.

The following installation parameters are described in this appendix:

- [customized obparameters](#)
- [start daemons at boot](#)
- [create pre-authorized oracle user](#)
- [default UNIX user](#)
- [default UNIX group](#)
- [identity certificate key size](#)
- [<os-name> ob dir](#)
- [<os-name> db dir](#)
- [<os-name> temp dir](#)
- [<os-name> links](#)
- [ask about ob dir](#)
- [default protection](#)
- [run obopenssl](#)

customized obparameters

If you customize any of the parameters in the `obparameters` file, then set the `customized obparameters` parameter to `yes`.

Table B-1 *customized obparameters: Values*

Value	Meaning
no (default)	Indicates that installation parameters in the <code>obparameters</code> file have not been changed. The value of <code>no</code> is set by default.

Table B-1 (Cont.) customized obparameters: Values

Value	Meaning
yes	Specifies that installation parameters in the <code>obparameters</code> file have been changed.

start daemons at boot

The installation tools can update each host's control files to automatically start Oracle Secure Backup each time you boot the system.

Table B-2 start daemons at boot: Values

Value	Meaning
no	Specifies that you do not want the Oracle Secure Backup daemons to start automatically at boot time.
yes (default)	Specifies that you want to the Oracle Secure Backup daemons to start automatically at boot time.

create pre-authorized oracle user

This parameter controls whether or not the Oracle Secure Backup installation process creates an Oracle Secure Backup user named `oracle` which has been pre-authorized to perform database backup and restore operations.

Table B-3 create pre-authorized oracle user: Values

Value	Meaning
yes	An Oracle Secure Backup user is created during installation. The parameters <code>default UNIX user</code> and <code>default UNIX group</code> specify the user and group parameters with which the Oracle Secure Backup user is created.
no (default)	No Oracle user is created.

default UNIX user

After the Oracle Secure Backup installation is successfully completed and the administrative domain has been initialized, you can create a default Oracle Secure Backup user named `oracle` if requested (see [create pre-authorized oracle user](#)). By setting this parameter, you specify the Linux or UNIX operating system user to which the Oracle Secure Backup user named `oracle` will be mapped. Note that you can also perform this task through the Web tool.

Table B-4 default UNIX user: Values

Value	Meaning
<code>UNIX_user</code>	Specifies the Linux or UNIX operating system username defined in <code>/etc/passwd</code> to which the Oracle Secure Backup user named <code>oracle</code> will be mapped. By default, the Linux/UNIX user is named <code>oracle</code> .

default UNIX group

After the installation is successfully completed and the administrative domain has been initialized, a default group will be created on Linux or UNIX if requested (see

`create pre-authorized oracle user`). The user specified by the default `UNIX user` parameter is a member of this group.

Table B-5 *default UNIX group: Values*

Value	Meaning
<code>UNIX_group</code>	Specifies a Linux or UNIX group defined in <code>/etc/group</code> . By default, the Linux/UNIX group is <code>dba</code> .

identity certificate key size

This option configures the key size in bits, and thus the level of security, associated with the host identity certificates issued by the administrative service daemon.

The default is 1024.

Note: Certificate key sizes smaller than 1024 are not considered secure. Certificate key sizes of 3072 or more are considered very secure.

Table B-6 *identity certificate key size: Values*

Value	Meaning
512	Specifies a 512-bit long certificate key size.
768	Specifies a 768-bit long certificate key size.
1024 (default)	Specifies a 1024-bit key length. This is the minimum required value for adequate security.
2048	Specifies a 2048-bit key length. This value offers adequate security.
3072	Specifies a 3072-bit key length. This value offers a very high level of security.
4096	Specifies a 4096-bit key length. This value offers a very high level of security.

<os-name> ob dir

To keep the installation and administration of Oracle Secure Backup as straightforward as possible, Oracle provides a mechanism for you to identify the name of the Oracle Secure Backup home directory for each platform in your network. This directory must be private to each platform and not shared through NFS or a similar remote file system.

When the installation programs install Oracle Secure Backup software, they choose these home directories for the installation or verify that these are the directories you have used. These defaults may be changed based on the availability of disk space on your machine.

`os-name` is a placeholder for `linux` or `solaris64`.

Table B-7 *os-name ob dir: Parameters and Values*

Parameter	Meaning
<code>linux ob dir</code>	Specifies Oracle Secure Backup home location for Linux hosts. The default is <code>/usr/local/oracle/backup</code> .

Table B-7 (Cont.) os-name ob dir: Parameters and Values

Parameter	Meaning
solaris64 ob dir	Specifies Oracle Secure Backup home location for Solaris 64-bit hosts. The default is /usr/local/oracle/backup.

<os-name> db dir

Each platform has a discrete directory in which Oracle Secure Backup retains host-specific information. This directory must be private to each platform and not shared through NFS or a similar remote file system.

os-name is a placeholder for `linux` or `solaris64` platforms.

Table B-8 os-name db dir: Parameters and Values

Parameter	Meaning
linux db dir	Specifies the directory where host-specific information is retained for Linux hosts. The default directory is /usr/etc/ob.
solaris64 db dir	Specifies the directory where host-specific information is retained for Solaris 64-bit hosts. The default directory is /usr/etc/ob.

<os-name> temp dir

Oracle Secure Backup typically uses the /usr/tmp directory on each host for storage of transient files. Oracle Secure Backup requires that the temporary directory be able to contain lockable files and that it be accessible during the beginning of the reboot process. The directory must be on the local disk. You can specify a different directory for each platform by modifying any of these <os-name> temp dir parameters.

os-name is a placeholder for `linux` or `solaris64`.

Table B-9 os-name temp dir: Parameters and Values

Parameter	Meaning
linux temp dir	Specifies the directory where transient files are stored for Linux hosts. The default directory is /usr/tmp.
solaris64 temp dir	Specifies the directory where transient files are stored for Solaris 64-bit hosts. The default directory is /usr/tmp.

<os-name> links

During installation, symbolic links are created, typically in /usr/bin and /etc, so that Oracle Secure Backup users do not need to change their search paths. You can modify this behavior as follows:

- Comment out or delete these parameters if you do not want the installation programs to create any links.
- Change the value of these parameters if you want the installation programs to create links in another directory for a specific platform.

These parameters are particular to each supported platform. On some systems, it may be more appropriate to place links in /bin instead of /usr/bin or in /usr/etc instead of /etc.

This parameter must be followed by three values, in the order shown:

1. The name of the directory in which to create the `bin` link.
2. The name of the directory in which to create the `etc` link.
3. The name of the directory in which to create the `lib` link.

`os-name` is a placeholder for `linux` or `solaris64`.

Note: Oracle recommends using the defaults provided for this parameter.

Table B-10 *os-name links: Parameters and Values*

Parameter	Meaning
<code>linux links</code>	Specifies the directories where symbolic links are created for Linux hosts. The default directory list is <code>/usr/bin /etc /lib</code> .
<code>solaris64 links</code>	Specifies the directories where symbolic links are created for Solaris 64-bit hosts. The default directory list is <code>/usr/bin /etc /lib</code> .

Note: If the `obparameters` file specifies a `lib` directory for the operating system type of the current installation, then `installob` creates a `libobk.so` symbolic link in that directory. That symbolic link points to the actual `libobk.so` file in a platform-specific `lib` directory in the Oracle Secure Backup home (such as `.lib.linux32`).

ask about ob dir

The installation notifies you when you are about to install Oracle Secure Backup into a directory other than the default Oracle Secure Backup home.

Table B-11 *ask about ob dir: Values*

Value	Meaning
<code>yes</code>	Enables notification when you select a directory other than the default Oracle Secure Backup home.
<code>no (default)</code>	Suppresses notification when you select a directory other than the default Oracle Secure Backup home.

default protection

Specifies directory and file protection information that is in effect when the Oracle Secure Backup installation is complete.

Caution: The file protection information is provided for reference only. Oracle strongly recommends using the defaults provided because changing them can prevent the product from functioning.

Values

Each line in the default protection section of the obparameters file indicates the file owner, group number and permissions for the file or files specified by name, or by wildcard pattern. The default values are as follows:

```
default protection:
root.0      755 ./wrapper
root.0      644 ./device/*
root.0      755 ./install/*
root.0      644 ./help/*
root.0      755 ./man/*
root.0      644 ./man/man1/*
root.0      644 ./man/man8/*
root.0      644 ./samples/*
root.0      755 ./samples/autoobtar
root.0      755 ./samples/bdf2ds
root.0      755 ./samples/*.sh
root.0      700 ./admin
root.0      700 ./admin/*
root.0      700 ./admin/config/*
root.0      755 ./bin.*/
root.0      4755 ./bin.*/obtar
root.0      4755 ./bin.*/obt
root.0      4755 ./bin.*/obtool
root.0      755 ./etc.*/
root.0      4755 ./etc.*/obixd
root.0      4755 ./etc.*/observed
root.0      4755 ./etc.*/obscheduled
root.0      4755 ./etc.*/obrobotd
root.0      755 ./etc.*/
root.0      4755 ./etc.*/doswitch
root.0      644 ./drv.*/
root.0      755 ./lib.*/
root.0      755 ./
root.0      755 /usr/etc/ob
root.0      644 /usr/etc/ob/.hostid
root.0      755 /usr/etc/ob/xcr
root.0      644 /etc/obconfig
```

run obopenssl

The installation prompts you to create the certificates for the Apache Web server.

Note: Oracle recommends using the default provided to ensure proper initialization of your Web tool.

Table B–12 *run obopenssl: Values*

Value	Meaning
yes (default)	Indicates that you want to create the certificate (default).
no	Indicates that you do not want to create the certificate.

Manually Configuring UNIX Drivers

This appendix explains how to manually install and uninstall the Oracle Secure Backup kernel device driver for Solaris.

Note: The steps in this chapter are only required for Solaris installations. Oracle Secure Backup automatically uses pass-through drivers for Linux systems.

You only need to perform the procedures described in this appendix in one of the following circumstances:

- Chose not to or were unable to use the automated installation program (`installob`) explained in [Chapter 4, "Installing Oracle Secure Backup on Linux or UNIX"](#).
- Used `installob` but did not specify any libraries or drives (or left the `device_list` field blank in your network description file). In this case, `installob` did not install the Oracle Secure Backup device driver or create any device special files.

Note: It is generally possible to run `installob` again to configure devices for your media server. See ["Running installob Again for Device Configuration or Push Installs"](#) on page 4-15 for details.

This chapter covers the following topics:

- [Installing the Oracle Secure Backup Device Driver Manually](#)
- [Uninstalling the Oracle Secure Backup Device Driver Manually](#)

Installing the Oracle Secure Backup Device Driver Manually

If your media server has missing or modified system files, major device numbers already in use, unexpected protection attributes, or other site-specific characteristics, then using `installdriver` to install the driver might not work. Rather, you need to install the driver kernel manually.

This section contains the following topics:

- [Installing the Driver on Solaris 2.8 and Later](#)

Installing the Driver on Solaris 2.8 and Later

Perform the following steps to install the Oracle Secure Backup device driver under Solaris 2.8 and later using operating system commands.

Note: These are the same steps performed by the `install/installdriver` shell script. It is strongly recommended that you perform this task by running that script instead of using the manual process described here.

1. Ensure you are logged in as `root`.
2. Check if there is a version of the Oracle Secure Backup driver currently installed:

```
# /usr/sbin/modinfo | grep ob
```

If this indicates that the driver named `ob` is installed, ensure there are no processes using the device driver. (If any Oracle Secure Backup daemons are running, stop them at this time using `kill -9`.)

Then uninstall the current driver. For example:

```
# /usr/sbin/rem_drv ob
```

3. Copy the driver from the Oracle Secure Backup Solaris driver directory to `/usr/kernel/drv`. For example:

```
cp /usr/local/oracle/backup/.drv.solaris64/ob /usr/kernel/drv/ob
```

4. Copy the driver's `ob.conf` file:

```
cp /usr/local/oracle/backup/.drv.solaris64/ob.conf /usr/kernel/drv/ob.conf
```

This `ob.conf` file allows Oracle Secure Backup devices to reside at any SCSI target, logical unit number (LUN) 0 or 1, on any bus. You can modify `ob.conf` to specify SCSI targets that correspond only to the devices you want to configure for use by Oracle Secure Backup. Also, you might need to modify the `ob.conf` file to include LUNs other than 0 or 1 for devices to be claimed by the Oracle Secure Backup driver.

5. Copy the 64-bit version of the driver to `/usr/kernel/drv/sparcv9`. For example:

```
cp /usr/local/oracle/backup/.drv.solaris64/ob64 /usr/kernel/drv/sparcv9/ob
```

6. Add the driver to the system using `add_drv`:

```
/usr/sbin/add_drv -m '* 0666 bin bin' ob
```

7. Use `install/makedev` to create device files for your libraries and drives.

See Also: ["Creating Device Special Files with makedev"](#) on page 5-8

Uninstalling the Oracle Secure Backup Device Driver Manually

You might need to uninstall the Oracle Secure Backup driver from your operating system. In most cases, you should use the Oracle Secure Backup `uninstallob` program. See [Chapter 6, "Uninstalling Oracle Secure Backup"](#) for more information.

On Solaris, manual action is required. You should first login as `root`. Then ensure that the driver is not currently active, that is, ensure that none of the drives or libraries are in use. After performing the following steps, you can delete the special devices files (in `/dev`) that were created as part of driver installation.

Note: Since some of the following procedures involve renaming and deleting files, you should make a backup copy of the appropriate directory trees (`/etc/conf`, `/stand/build`, and so on) before proceeding.

Manual removal of drivers is described for the following operating system:

- [Manually Uninstalling the Oracle Secure Backup Driver on Solaris](#)

Manually Uninstalling the Oracle Secure Backup Driver on Solaris

To uninstall the Oracle Secure Backup driver on Solaris:

- Log into the host as `root`.
- Run the `rem_drv` command to uninstall the Oracle Secure Backup driver. For example:

```
# /usr/sbin/rem_drv ob
```

- Delete the driver files from `/usr/kernel/drv`. For example:

```
# cd /usr/kernel/drv
# rm ob ob.conf sparcv9/ob
```

Index

A

administrative domain
 planning, 1-4
 roles, 1-4
administrative server
 defined, 1-2
 directories, A-2
 files, A-2
ask about osb dir
 obparameters, B-5

B

backup catalog
 defined, 1-2
batch mode, 4-8

C

client
 defined, 1-2
client host
 directories, A-5
 files, A-5
configuration file parameters
 ask about osb dir, B-5
 create pre-authorized oracle user, B-2
 customized obparameters, B-1
 default protection, B-5
 default UNIX/LINUX group, B-2
 default UNIX/LINUX user, B-2
 linux db dir, B-4
 linux links, B-4
 linux ob dir, B-3
 linux temp dir, B-4
 run obopenssl, B-6
 solaris db dir, B-4
 solaris links, B-4
 solaris ob dir, B-3
 solaris temp dir, B-4
 solaris64 db dir, B-4
 solaris64 links, B-4
 solaris64 ob dir, B-3
 solaris64 temp dir, B-4
 start daemons at boot, B-2

configuring
 NAS devices, 5-20
 on Windows, 3-6
create pre-authorized oracle user
 obparameter, B-2
creating device names, 3-4
customized obparameters, B-1

D

default protection
 obparameters, B-5
default UNIX/LINUX group
 obparameters, B-2
default UNIX/LINUX user
 obparameters, B-2
device drivers
 removing, C-2
device names, 3-7, 5-20
device names, creating, 3-4
device parameters
 Oracle Secure Backup Logical Unit Numbers, 1-8
 SCSI, 1-8
device special files
 creating
 with installob, 4-10
 with makedev, 5-8
driver installation
 Solaris, C-2

F

Fibre Channel
 sharing devices, 3-2

I

installation
 batch mode, 4-8
 interactive mode, 4-8
 manually installing the Oracle Secure Backup
 driver, C-1
 remote, for Linux and Unix, 1-12
installation parameters
 ask about osb dir, B-5
 create pre-authorized oracle user, B-2

- customized obparameters, B-1
- default protection, B-5
- default UNIX/LINUX group, B-2
- default UNIX/LINUX user, B-2
- linux db dir, B-4
- linux links, B-4
- linux ob dir, B-3
- linux temp dir, B-4
- run obopenssl, B-6
- solaris db dir, B-4
- solaris links, B-4
- solaris ob dir, B-3
- solaris temp dir, B-4
- solaris64 db dir, B-4
- solaris64 links, B-4
- solaris64 ob dir, B-3
- solaris64 temp dir, B-4
- start daemons at boot, B-2
- installing
 - client on Windows, 2-3
 - media server on Windows, 2-3
- interactive mode
 - installation, 4-8
- inventory
 - Solaris devices, 3-6, 5-19

L

- Linux
 - probing SCSI parameters, 5-2
- linux db dir
 - obparameters, B-4
- Linux hosts
 - configuration, 5-1
- linux links
 - obparameters, B-4
- linux ob dir
 - obparameters, B-3
- linux temp dir
 - obparameters, B-4
- lun numbers
 - SCSI devices, 3-2

M

- makedev
 - device special files, 5-8
- media server
 - defined, 1-2
 - directories, A-4
 - files, A-4

N

- NAS devices
 - configuring, 5-20
 - on Windows, 3-6
- NDMP, 1-2

O

- obparameters
 - ask about osb dir, B-5
 - create pre-authorized oracle user, B-2
 - customized, B-1
 - default protection, B-5
 - default UNIX/LINUX group, B-2
 - default UNIX/LINUX user, B-2
 - linux db dir, B-4
 - linux links, B-4
 - linux ob dir, B-3
 - linux temp dir, B-4
 - run obopenssl, B-6
 - solaris db dir, B-4
 - solaris links, B-4
 - solaris ob dir, B-3
 - solaris temp dir, B-4
 - solaris64 db dir, B-4
 - solaris64 links, B-4
 - solaris64 ob dir, B-3
 - solaris64 temp dir, B-4
 - start daemons at boot, B-2
- obparameters file
 - configuring, 4-5
 - reference, B-1
- Oracle database object
 - creating, 2-8
- Oracle Real Application Clusters
 - and Oracle Secure Backup, 2-1
 - Oracle Secure Backup, 2-3, 4-2
- Oracle Secure Backup
 - and Oracle Real Application Clusters, 2-1
 - directories, A-1
 - files, A-1
 - installation
 - directory, A-1
 - Oracle Real Application Clusters, 2-3, 4-2
 - system requirements, 1-4

P

- Probing SCSI parameters
 - on Linux, 5-2
- push installation
 - for Linux and Unix, 1-12

R

- remote installation
 - for Linux and Unix, 1-12
- requirements
 - Oracle Secure Backup, 1-4
- run obopenssl
 - obparameters, B-6

S

- SCSI devices
 - obtaining configuration data
 - on Linux, 5-1

- obtaining configuration data for, 5-1
- obtaining lun numbers, 1-9, 3-2
- obtaining target IDs, 5-1
- shared devices
 - Fibre Channel, 3-2
- Solaris
 - configuring, 5-10, 5-14
- solaris db dir
 - obparameters, B-4
- solaris links
 - obparameters, B-4
- solaris ob dir
 - obparameters, B-3
- solaris temp dir
 - obparameters, B-4
- solaris64 db dir
 - obparameters, B-4
- solaris64 links
 - obparameters, B-4
- solaris64 ob dir
 - obparameters, B-3
- solaris64 temp dir
 - obparameters, B-4
- start daemons at boot
 - obparameter, B-2

T

- target ID
 - SCSI devices, 5-1

U

- uninstalling
 - Oracle Secure Backup on Linux, 6-1
 - Oracle Secure Backup on UNIX, 6-1
 - Oracle Secure Backup on Windows, 6-1
- UNIX
 - devices, C-1
- UNIX hosts
 - configuration, 5-1
 - installation, 4-3

W

- Windows drivers
 - stopping, 2-2

