Oracle® Secure Backup

Installation and Configuration Guide

Release 19.1
F89763-02
April 2025

ORACLE

Oracle Secure Backup Installation and Configuration Guide, Release 19.1

F89763-02

Primary Author: Manish Garodia

Contributing Authors: Aishwarya Minocha, Craig B. Foch, Kathy Rich, Lance Ashdown, Padmaja Potineni, Sarika Surampudi

Contributors: Anand Agrawal, Ashok Joshi, Basker Vedaraman, Chris Plakyda, Cris Pedregal-Martin, Donna Cooksey, Geoff Hickey, George Claborn, George Stabler, Jack Swan, Jay Cobau, Joe Wadleigh, Judy Ferstenberg, Marco Calmasini, Michael Chamberlain, Radhika Vullikanti, Rhonda Day, Roopesh Ashok Kumar, Sandhya GM, Senad Dizdar, Shailesh Sivasankaran, Steve Wertheimer, Steven Fried, Sumit Chougule, Tammy Bednar, Tony Dziedzic

Contents

3 Oracle Secure Backup User Interfaces

4 Installing Oracle Secure Backup on Linux or UNIX

5 Installing Oracle Secure Backup on Windows

9 Managing Security for Backup Networks

Preface

This Preface contains these topics:

Audience

This 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 must 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 Recovery Manager concepts.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

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

- *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 User's Guide*

  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).

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

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

You can download the Oracle Secure Backup software from the Download tab on this page.

Conventions

The following text conventions are used in this document:

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

Changes in This Release for Oracle Secure Backup Installation and Configuration Guide

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

Oracle Secure Backup 19.1 Release 1

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

New Features, Enhancements, and Updates

- Support for non-English backup directory paths.

  Windows hosts using older backup can now use `--charencoding` option while using the obtool to fix the garbled text that shows up in the directory paths.

  See Configure Character Encoding (Windows).

- Check the updated screenshot and image description for Web Tool Configure Page and updated image description for the screenshot *Oracle Secure Backup Setup Window* in Interactive Installation on Windows.

Additional options while installing Oracle Secure Backup

See Options for Installing on Linux or UNIX and Options for Installing on Windows.

- Configure customized port number for NDMP during installation on client hosts.

  You can now specify an NDMP port number other than the default port 10000 while installing Oracle Secure Backup on client hosts.

  See:

  - Interactive Installation on Linux or UNIX
  - Noninteractive or Unattended Installation on Linux or UNIX
  - Interactive Installation on Windows
  - Noninteractive or Unattended Installation on Windows

- Install Oracle Secure Backup administrative server with the web server disabled.

  See Installing Administrative Server on Linux or UNIX and Installing Administrative Server on Windows.

- View updated information regarding the Prerequisites for Installing on Linux or UNIX.
- Check the new section for Noninteractive or Unattended Installation on Windows.

Oracle Secure Backup Client Backward Compatibility

Oracle Secure Backup client supports backward compatibility and interoperability with the earlier versions. For more information, see Support for Client Backward Compatibility and Upgrading Oracle Secure Backup.

Deprecated Functionality

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

Desupported Functionality

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

Other Changes

Major revamp and editorial changes to these sections with language and grammar improvements.

- Support for Client Backward Compatibility
- Types of Installation
- Prerequisites for Installing on Linux or UNIX
- Options for Installing on Linux or UNIX
- Interactive Installation on Linux or UNIX
- Installing Administrative Server on Linux or UNIX
- Installing Client Role on Linux or UNIX
- Noninteractive or Unattended Installation on Linux or UNIX
- Prerequisites for Installing on Windows
- Options for Installing on Windows
- Interactive Installation on Windows
- Installing Administrative Server on Windows
- Installing Client Role on Windows
- Enabling Installer Logging on Windows
- Configuring Advanced Settings for Windows
- Preparing for Upgrade Installation
- Upgrade Installation on Linux or UNIX
- Upgrade Installation on Windows
- Administrative Server Files and Directories

1

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 contains these sections:

- What Is Oracle Secure Backup?
- Overview of Oracle Secure Backup Concepts
- Oracle Secure Backup Interfaces

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

What Is Oracle Secure Backup?

Oracle Secure Backup is a centralized network-based backup management application that provides scalable and distributed backup and recovery capabilities.

- It facilitates backup of Oracle Databases and file system data across heterogeneous network operating systems, such as Linux, Solaris, HP-UX, AIX and Windows.
- It supports many leading tape library and tape drive in the industry.
- It provides data protection from malware, ransomware, and data loss, for example physical hardware loss or accidental deletion by offering scheduled and configurable file system and Recovery Manager (RMAN) backups to cloud storage, disk pools, and tape libraries.
- It supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6) and mixed IPv4/IPv6 environments.
- It works with FC-SCSI and SCSI attached devices on SAN and Gigabit Ethernet (GbE) networks.

Oracle Cloud Infrastructure allows users to store huge volumes of backup data and run Oracle Secure Backup on compute instances. You can use disk pools to provide fast backups to disk that can be staged to backup to tape.

Oracle Secure Backup Features

Oracle Secure Backup provides the following features:

- Integration with other Oracle products thus enabling you to easily backup and restore both Oracle Databases and file-system data to tape

  Oracle Secure Backup is fully integrated with Recovery Manager (RMAN) and Oracle Enterprise Manager. You can use Oracle Enterprise Manager to backup both file-system data and Oracle Databases to tape. Oracle Secure Backup serves as a media

management layer, through the System Backup to Tape (SBT) interface, to securely backup Oracle Databases using RMAN.

- Support for disk pools and a wide range of tape drives and libraries that are accessible through various protocols such as SCSI, ISCSI, SAN, NDMP, and Fibre Channel
- Centralized tape backup management

  Oracle Secure Backup enables centralized backup management of diverse distributed servers and multiple platforms including UNIX, Linux, Windows, and SAN. It can backup and restore locally or over a LAN/WAN.
- Policy-based backup management

  Oracle Secure Backup provides customizable administrative policies that enable you to control backup operations in the administrative domain. Policies also enable you to control aspects of domain security.
- Flexible interface options that provide maximum ease of use

  Oracle Secure Backup functionality can be accessed using any of the following interfaces: Oracle Secure Backup Web Tool, Oracle Enterprise Manager DB Control, Oracle Enterprise Manager Cloud Control, or `obtool` command-line interface.
- Maximum security options for data and inter-host communication

  Inter-domain communication is secured using the Secure Socket Layer (SSL) protocol. All hosts in the Oracle Secure Backup administrative domain are identified and authenticated using SSL and X.509 certificates. Data transmission within the administrative domain is secured using encryption. You can also encrypt Oracle Database backups before they are stored to tape.
- Automated device discovery

  Oracle Secure Backup can automatically discover and configure each secondary storage device connected to certain types of NDMP servers, such as a Network Appliance filer. It can also discover devices connected to the Oracle Secure Backup media servers.
- Automated tape library and device management that includes automated control of tape libraries

  Oracle Secure Backup automates the management of tape libraries to ensure efficient and reliable use of their capabilities. It controls library robotics and enables automatic loading and unloading of volumes. It can also automatically clean tape drives in a tape library.
- Automated media management that includes volume and backup expiration

  Oracle Secure Backup enables automatic tape recycling by specifying when volumes can be recycled. You create policies to define when volumes are eligible to be recycled or rewritten.
- Flexible, multi-level, backup options

  Oracle Secure Backup enables you to create full, incremental, and differential backups.
- Flexible options for restoring backups

  Oracle Secure Backup enables you to restores backup data stored on tapes either to the original location or to an alternative server.

Overview of Oracle Secure Backup Concepts

This section discusses Oracle Secure Backup concepts that enable you to better understand the installation process.

This section contains these topics:

About Oracle Secure Backup Administrative Domains and Hosts

Oracle Secure Backup organizes hosts and tape devices into an administrative domain, representing the network of hosts containing data to be backed up, hosts with attached tape devices on which backups are stored, and each tape device with its attachment to the hosts. A host can belong to only one administrative domain.

Host Roles in an Administrative Domain

Each host in an administrative domain must be assigned one or more of the following Oracle Secure Backup roles:

- **Administrative server**

  Each administrative domain must have exactly one administrative server. During postinstallation configuration, the administrative server must be configured with complete data regarding the other hosts in the administrative domain, their roles, and their attached tape devices. This configuration information is maintained in a set of configuration files stored on the administrative server.

  The administrative server runs the scheduler, which starts and monitors each backup job. The scheduler also keeps a backup catalog with metadata for all backup and restore operations performed in the administrative domain.

- **Media server**

  A media server is a host with at least one tape device attached to it. A media server transfers data to or from a volume loaded on one of these tape devices. A media server has at least one attachment to a tape drive or library. It might have attachments to multiple tape libraries and disk pools.

  You specify the attachments between media servers and tape devices during postinstallation configuration of Oracle Secure Backup.

- **Client**

  The client role is assigned to any host that has access to file-system or database data that can be backed up or restored by Oracle Secure Backup. Any host where Oracle Secure Backup is installed can be a client, including hosts that are also media servers or the administrative server. A network-attached storage device that Oracle Secure Backup accesses through NDMP can also serve the client role.

> **Note:**
>
> A host can be assigned multiple roles in an administrative domain. For example, a host with a tape drive attached could be both the administrative server and media server for a network that includes several other clients. For more examples of administrative domains, see "About Oracle Secure Backup Administrative Domain: Examples".

> **See Also:**
>
> "Choosing Secure Hosts for the Administrative and Media Servers"

Host Naming in an Administrative Domain

Each host in the administrative domain must have a unique name that pairs with a unique IP address that is used for TCP/IP communication among the hosts and the media management devices.

In general, the DNS host name can be a good choice for an Oracle Secure Backup host name. Though you can assign a different name to a host, ensure that you specify the IP address as the host object's IP name while configuring Oracle Secure Backup.

Oracle Secure Backup Host Access Modes

Oracle Secure Backup administrative domain uses NDMP to communicate between Compute Hosts and Storage Area Network appliances.

Oracle Secure Backup supports two host access modes: primary access mode and NDMP access mode.

Oracle Secure Backup compute hosts run in primary access mode and have the Oracle Secure Backup software package installed on them. A group of Oracle Secure Backup daemons run in the background that enable communication between the Oracle Secure Backup administrative server, clients, and media servers for performing both file system and RMAN database backups. NDMP access mode is used for communication with SAN appliances.

> **Note:**
>
> In the Oracle Secure Backup Web tool and the output of some `obtool` commands such as `lshost`, primary mode is referred to as OB access mode. In Oracle Enterprise Manager, primary access mode is referred to as native access mode.

NDMP access mode is used to communicate with Storage Area Network appliances for backup and restore. Oracle's ZFS Storage Appliance and other third party vendors, such as NetApp and Dell EMC, run their own implementations of NDMP which are supported in Oracle Secure Backup. However, additional parameters specific to the vendor's implementation of NDMP may be required while adding and configuring these devices in the Oracle Secure Backup administrative domain.

About Oracle Secure Backup Administrative Domain: Examples

Figure 1-1 shows a minimal administrative domain, in which a single host is administrative server, media server, and client. An Oracle database also runs on the same host.

Figure 1-1 Administrative Domain with One Host

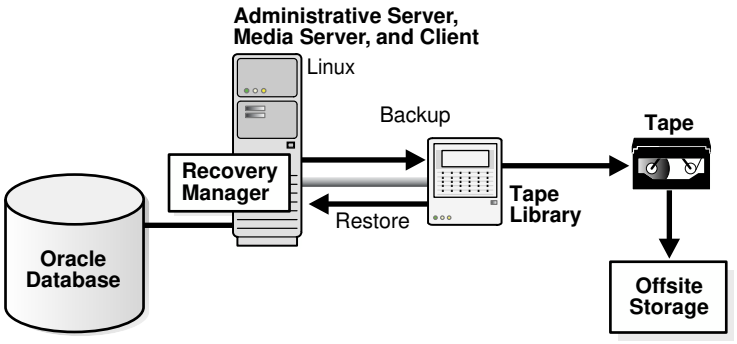
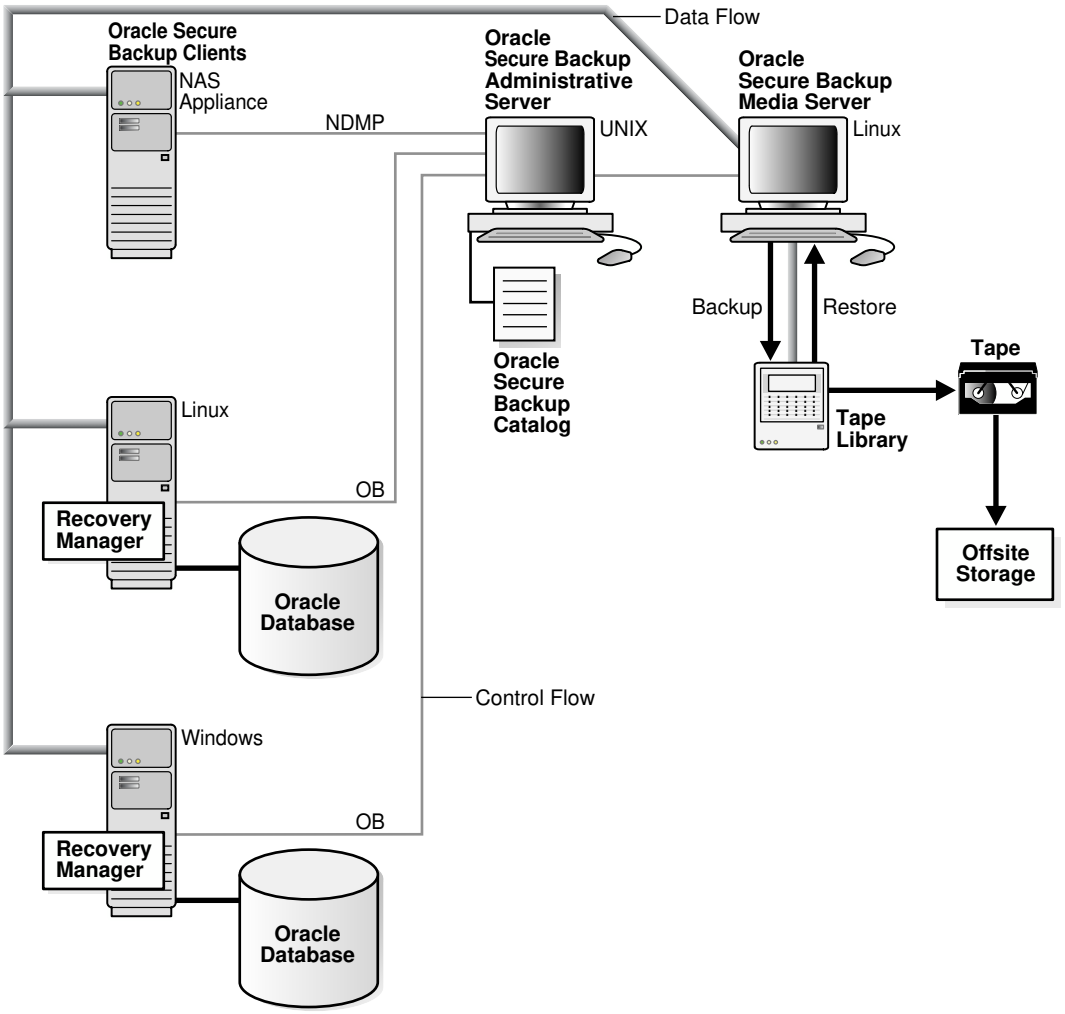


Figure 1-2 shows a possible Oracle Secure Backup administrative domain that includes three client hosts, one administrative server, and one media server. A NAS appliance contains ordinary file data. One client based on UNIX and another based on Windows contain databases and other file data. Oracle Secure Backup can back up to tape the non-database files on file systems accessible on client hosts. RMAN can back up to tape database files through the Oracle Secure Backup SBT interface.

Figure 1-2 Oracle Secure Backup Administrative Domain with Multiple Hosts



About Disk Pools

A disk pool is a file-system directory that acts as a repository for backup image instances. Disk pools can store file-system backups, RMAN backups of Oracle databases, and backups created by NDMP filers.

Each disk pool is represented as a device in Oracle Secure Backup. A disk pool can belong to only one administrative domain. To monitor space utilization on disk pools, you must delete expired backup image instances.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information on managing disk pools

About Tape Devices

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

This section contains these topics:

- Tape Drives
- Tape Libraries
- Device Names and Attachments

Tape Drives

A tape drive is a device that reads and writes data on magnetic tapes.

Magnetic tapes are sequential-access storage devices that provide long-term data storage. Unlike disks, the data stored on a tape does not require electricity to sustain it, hence are cost-effective and eco-friendly.

A tape drive uses precision motors to wind magnetic tapes from one reel to another. The tape passes a read/write head as it is wound. These reels are inside a tape cartridge, such as LTO series media, which is the most popular type of drive among Oracle Secure Backup users. A tape is sequential-access storage and since it has a beginning and an end, the tape drive must read through the tape in order to locate the position on the tape where the End of Media is located in order to append to a tape, or locate the position of the written data in the middle of the tape in order to perform a restore.

Tape drives write data in a block format and the block size can influence the backup data transfer rate. Each block is written in a single operation with gaps left between the blocks. The blocking factor can be adjusted to optimize the performance of backups and restores. Typically, large blocking factors are optimum for backing up large files while smaller blocking factors are optimum for backing up numerous small files.

The **block size** of a block of data is the size of the block in bytes as it was written to tape. All blocks read or written during a given backup or restore operation have the same block size. The blocking factor of a block of data expresses the number of 512-byte records contained in the block. For example, for a site that blocks up a large number of small files, you can set a small blocking factor to match the size of the source data, whereas for sites that back up huge files, you can specify a large blocking factor. The Oracle Secure Backup default blocking factor (128) results in a tape block size of 128*512 bytes or 64 KB.

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

You can specify the blocking factor and the maximum blocking factor. See "Configuring Tape Drives". The default value for `blockingfactor` and `maxblockingfactor` is 128 when Oracle Secure Backup is installed. You can configure domain-wide blocking and maximum blocking factors using the `media/blockingfactor` and `media/maxblockingfactor` polices. For more information about the policies, see *Oracle Secure Backup Reference*.

Things to consider:

- The `blockingfactor` (block size) must always be less than or equal to the `maxblockingfactor`.
- The tape drive itself must support the block size settings in use because often tape drives, device drivers, or operating systems have limitations which can supersede other conditions.
- The `maxblockingfactor` must always be set to be greater than or equal to the largest block you will want to restore.

  When a restore operation starts, Oracle Secure Backup is not aware of the block size that was used to write a given tape. Oracle Secure Backup starts a restore by reading the largest possible block size that is `maxblockingfactor`. If the blocking factor is too large, Oracle Secure Backup returns an error and displays a message to increase the `media/maxblockingfactor` policy in obtool.

Oracle Secure Backup supports the following tape drives:

- Linear Tape-Open (LTO)
- T10000

Information about the tape formats of tape devices supported by Oracle Secure Backup is available at:

`http://www.oracle.com/technetwork/products/secure-backup/learnmore/index.html`

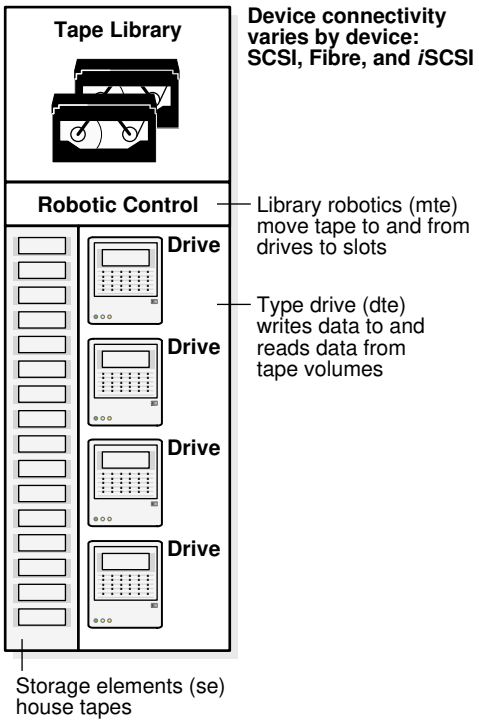
Tape Libraries

A tape library is a robotic tape device that operates on SCSI commands.

You can run SCSI commands to move a volume between a storage element and a tape drive. A tape library is often referred to as a medium changer.

A tape library contains one or more tape drives, slots (storage elements or se's) for holding tape cartridges, and provides an automation device to move tapes between drives and storage elements. Figure 1-3 illustrates a tape library containing four tape drives.

Figure 1-3 Tape Library



Oracle Secure Backup supports tape libraries for managing automatic loading and unloading of volumes to and from the tape drives and storage elements to optimize efficiency.

When a tape library is first configured in Oracle Secure Backup, you must perform an initial forced inventory so that Oracle Secure Backup identifies the contents of the storage elements. Most modern tape libraries require barcode labels on the tapes to perform management operations and for vaulting to other locations. Oracle Secure Backup checks the volume ID of a tape with the barcode to facilitate managing the tape inventory and to identify the tapes required for restore and recycle operations.

After the library and drives are configured, Oracle Secure Backup is configured to automount tapes for backups. Oracle Secure Backup sends commands to the library's robotic arm indicating the tapes to move between the drives and storage elements in order to provide the resources required for a job to backup or restore data. Oracle Secure Backup scans the tape library storage elements to find a suitable volume and uses internal records to optimize tape selection. When you have adequate tapes in the storage elements, Oracle Secure Backup does not require manual loading of tapes to complete backups that span across multiple volumes.

You can configure Oracle Secure Backup to automate the drive cleaning operations. For more information about the policies, see *Oracle Secure Backup Reference*.

Figure 1-3 shows a tape library with its set of addressable elements:

- Storage Elements (se) are locations where tapes can be stored and available for operations while not in use.
- A data transfer element (DTE) is a tape drive which is used for reading and writing data to and from the tape volume.
- Media Transfer Element (mte) is the robotic arm that moves tape cartridges from the storage elements to and from the tape drives.

- Import Export Element (iee) is a mechanism with a door that an operator uses to transfer tapes in and out of the library. After the door is closed, the robotic arm transfers cartridges to internal slots in the library. If the library is used to move the cartridges around, outside of Oracle Secure Backup, a reinventory is required to update the identification of the storage element contents.

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

Oracle Secure Backup supports several tape library operations. The following operations are the most basic:

- Inserting and extracting volumes
- Loading and unloading volumes
- Moving volumes
- Importing and exporting volumes

> **See Also:**
>
> *Oracle Secure Backup Reference* for details about the tape library commands that you can run in obtool

Virtual Tape Libraries

A virtual tape library is one or more large-capacity disk drives partitioned into virtual physical tape volumes. To Oracle Secure Backup the virtual tape library appears to be a physical tape library with at least one volume and at least one tape drive. The volumes and tape drives in the virtual tape library can be configured to match common physical tapes and tape drives.

Backup operations performed to a virtual tape library complete faster than backup operations to actual tape drives, because the underlying storage device is direct access media. But a virtual tape library is not suitable for long time storage, because it has limited storage capacity. If you back up to a virtual tape library, then you can take advantage of its faster backup and then use the volume migration feature of Oracle Secure Backup to migrate the data to tapes at a later point of time.

Device Names and Attachments

Because Oracle Secure Backup manages tape drive operations, it must be able to identify the tape drive and determine whether the tape drive is housed in a tape library. Oracle Secure Backup must further determine if a storage element is available for storing a volume while not in use by the tape drive. Thus, each tape device must be uniquely identified within Oracle Secure Backup by a user-defined name.

Oracle Secure Backup distinguishes a tape device and the means by which the tape device connects to a host. To be usable by Oracle Secure Backup, each tape device must have at least one attachment, which describes a data path between a host and the tape device. An attachment usually includes the identity of a host plus an attach point name in Linux or UNIX, a

device name in Windows, or a NAS device name. In rare cases, additional information is needed for the attachment definition.

> **See Also:**
>
> - "Adding Tape Devices to an Administrative Domain" to learn how to configure a tape device
> - *Oracle Secure Backup Reference* for a description of the `mkdev` command *aspec* placeholder, which describes the syntax and naming conventions for device attachments

About Cloud Storage Devices

Oracle Secure Backup cloud storage devices are used to backup and restore data to and from Oracle Cloud Infrastructure Object Storage Classic and from Oracle Cloud Infrastructure Object Storage.

- When used with Oracle Cloud Infrastructure, a cloud storage device operates on a container in the specified Oracle Cloud Infrastructure Object Storage namespace. Each cloud storage device is associated with only one container.

  > **Note:**
  >
  > The term "identity domain" is specific to Oracle Cloud Infrastructure Classic. Oracle Cloud Infrastructure uses a new term "namespace".

  A container is a logical grouping of resources. A bucket, which is created in a user-specified container, acts as the repository for backup image instances. Multiple administrative domains can use one container. However, a bucket can be used by only one administrative domain.

  The storage class for a container in Oracle Cloud Infrastructure can be standard storage class (`object`), archive storage class (`archive`), or infrequent access storage class (`infrequentaccess`).

  > **See Also:**
  >
  > Oracle Cloud Infrastructure Object Storage for more information about using Oracle Cloud Infrastructure Object Storage

- When used with Oracle Cloud Infrastructure Classic, a cloud storage device operates on a cloud storage container in the Oracle Cloud user's identity domain. The cloud storage container acts as a repository for backup image instances. Each cloud storage device is associated with only one cloud container. The storage class for a cloud container in Oracle Cloud Infrastructure Classic can be standard storage class (`object`) or archive storage class (`archive`).

> **Note:**
>
> The term "identity domain" is specific to Oracle Cloud Infrastructure Classic. Oracle Cloud Infrastructure uses a new term "namespace".

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

> **See Also:**
>
> - Oracle Cloud Infrastructure Object Storage Classic for more information about the Oracle Cloud Infrastructure Object Storage Classic
> - The obtool commands "mkdev"and "lsdev"for more information about Cloud storage class options

Backups to Cloud Storage Devices

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

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

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

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

Cloud Storage Devices and Staging

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

You can move a backup image instance from a standard storage class (object) container to an archive storage class (archive) container or an infrequent access storage class (infrequent access) container with a manual copy job. If both containers or buckets are located in the same identity domain, Oracle Secure Backup copies data between containers or buckets. If

both containers or buckets are located in different identify domains, the data is downloaded from source device and then uploaded to the target device.

Cloud Storage Devices and System Memory Usage

The cloud device requires a certain amount of system memory from the media server attached to the device. The amount of media server system memory required is derived from the cloud device's `segmentsize`, `streamsperjob`, and `concurrentjobs` values, and the number of cloud devices attached to the media server.

The total amount of system memory on the media server that is needed to support Oracle Secure Backup cloud devices is derived as follows:

```
(# of attached cloud devices) * (concurrentjobs) * (1 + streamsperjob) *
(segmentsize)
```

> **See Also:**
>
> - Configuring Cloud Storage Devices
> - *Oracle Secure Backup Administrator's Guide* for information about managing cloud storage devices

Oracle Secure Backup Daemons

Daemons are background processes that perform Oracle Secure Backup operations. Some daemons run continuously while others run only to perform a particular task and then exit when the task is complete.

A daemon can run either on the administrative server, the media server, or a client. Oracle Secure Backup uses a combination of daemons to perform a particular backup, restore, or configuration task.

The Oracle Secure Backup daemons include the following: Service daemon, Schedule daemon, Index daemon, Apache Web Server daemon, NDMP daemon, Robot daemon, and Proxy daemon.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information about daemons

Oracle Secure Backup Interfaces

There are four different interfaces for accessing different elements of Oracle Secure Backup:

- The obtool command line utility provides the fundamental interface for Oracle Secure Backup functions, including configuration, media handling, and backup and restore of file-system files.
- Oracle Enterprise Manager offers access to most Oracle Secure Backup functions available through `obtool` as part of its Cloud Control interface.

- Oracle Secure Backup includes its own Web-based interface, called the Oracle Secure Backup Web tool, which exposes all functions of `obtool`. The Oracle Secure Backup Web tool is primarily intended for use in situations where Oracle Secure Backup is being used independently of an Oracle Database instance. It does not provide access to database backup and recovery functions.

  The Oracle Secure Backup Web tool supports Internet Protocol v4 (IPv4), Internet Protocol v6 (IPv6), and mixed IPv4/IPv6 environments on all platforms that support IPv6.
- Backup and restore operations for Oracle Database instances and configuration of the Oracle Secure Backup media management layer are performed through the RMAN command-line client or through Oracle Enterprise Manager.

Note:

Oracle Secure Backup documentation focuses on the use of Enterprise Manager wherever possible, and describes the Oracle Secure Backup Web Tool only when there is no equivalent functionality in Enterprise Manager, as in a file-system backup.

See also:

- Oracle Secure Backup User Interfaces for details on using the different Oracle Secure Backup interfaces.
- *Oracle Database Backup and Recovery User's Guide* for details on using Recovery Manager (RMAN) for Oracle database backups

2

Oracle Secure Backup Installation Overview

This chapter provides an overview of the Oracle Secure Backup installation requirements.

This chapter contains these sections:

- Overview of Installing and Configuring Oracle Secure Backup
- Preparing to Install Oracle Secure Backup
- Overview of Customizing Configuration Parameters During Installation

Overview of Installing and Configuring Oracle Secure Backup

Before you can use Oracle Secure Backup to manage your data protection requirements, you must install Oracle Secure Backup on all hosts and then configure the administrative domain.

About Installing Oracle Secure Backup

The Oracle Secure Backup software must be installed on all hosts, except NDMP hosts, in the administrative domain. The administrative domain consists of one administrative server, one or more media servers, and one or more clients. The software that you install on a host depends on the role assigned to the host in the administrative domain. During the installation, you can specify the role for which you want to install Oracle Secure Backup.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information about the administrative domain

The Oracle Secure Backup installer determines if a host system has Oracle Secure Backup software installed or if it contains data from an earlier Oracle Secure Backup installation. If no Oracle Secure Backup software or data exists, then Oracle Secure Backup is installed. If Oracle Secure Backup software or data exists on the host, then depending on the release of the software or data, either an upgrade is performed or the installer exits.

> **See Also:**
>
> - "Types of Installation"
> - Installing Oracle Secure Backup on Linux or UNIX
> - Installing Oracle Secure Backup on Windows
> - Performing Upgrade Installation of Oracle Secure Backup

The directories containing Oracle Secure Backup data are protected by restricting access to these directories to only privileged users.

About Configuring Oracle Secure Backup

After the Oracle Secure Backup software is installed on all hosts in the administrative domain, you must configure the administrative domain. Configuring the administrative domain ensures that the administrative server has information about all the hosts and backup containers (tape devices and disk pools) that are part of the administrative domain.

Configuring Oracle Secure Backup includes the following tasks:

- Adding each host to the administrative domain
- Configuring backup containers that are attached to media servers

> **See Also:**
>
> Configuring and Managing the Administrative Domain

About Oracle Secure Backup Client Backward Compatibility

An Oracle Secure Backup client supports backward compatibility and interoperability between the current version and its immediate previous release.

Support for Client Backward Compatibility

You can use backward compatibility with limited feature availability for Oracle Secure Backup clients after the administrative server and the media server are upgraded to the same version of Oracle Secure Backup.

Oracle Secure Backup 19.1 supports backward compatibility with the following:

- Oracle Secure Backup 18.1.0.2
- Oracle Secure Backup 18.1.0.1
- Oracle Secure Backup 18.1.0.0

Oracle Secure Backup 19.1 supports the Oracle Secure Backup 18.1.0.2 features and is interoperable with their functionality.

Oracle Secure Backup 19.1 does not support backward compatibility with Oracle Secure Backup 12. However, Oracle Secure Backup 19.1 can restore backups created in Oracle Secure Backup 12.

Oracle Secure Backup 19.1 is not supported on Linux 32-bit platforms or Windows 32-bit platforms. Therefore, it does not support any clients on these platforms. For more information, see Supported Platforms and Tape Devices.

For any queries related to compatibility with Oracle Secure Backup versions, contact Oracle Support.

About Certificate Lifetime

The Certification Authority (CA) maintains a signing certificate that authorizes the CA to sign the identity certificates for the other hosts in the domain.

Oracle Secure Backup allows you to set the duration for which each signing certificate is valid. This duration is set using the certificate lifetime policy.

- Certificates with shorter lifetimes are more secure
- Certificates with longer lifetimes are easier to manage

Select a lifetime for certificates based on your corporate policy.

The default certificate lifetime is 10 years. To change the certificate lifetime throughout the domain, complete the following steps:

1. Change the value of the `security/certlifetime` policy.
2. Run the `obcm recertifydomain` command.

For more information on the certificate lifetime policy and `obcm recertifydomain` command, see the *Oracle Secure Backup Reference*.

Types of Installation

This section explains the types of installation for Oracle Secure Backup and outlines a high-level installation procedure.

You can install Oracle Secure Backup on Linux or UNIX and on Windows operating system. For installation, you can use the following methods:

- Interactive Installation on Linux or UNIX
- Noninteractive or Unattended Installation on Linux or UNIX
- Interactive Installation on Windows
- Noninteractive or Unattended Installation on Windows

> **Note:**
>
> For unattended installation on Linux or UNIX and on Windows, you can either specify an adding host or disable this feature and install Oracle Secure Backup without an adding host.

While installing Oracle Secure Backup, you can also select whether to install the administrative server or the client role on your host.

Oracle Secure Backup Installation Procedure

1. Install Oracle Secure Backup on all hosts in the administrative domain.
   - Select a host to perform as the administrative server and install the Oracle Secure Backup administrative server. Use this host to start and manage backup and restore jobs.

This initializes the administrative domain but it contains only one host, that is, the administrative server.

- On all hosts that contain RMAN or file system data or both, install the client role. The installation procedure is similar to the administrative server with an exception of selecting the client role instead.

> **See Also:**
>
> For detailed installation steps -
>
> - Installing Oracle Secure Backup on Linux or UNIX
> - Installing Oracle Secure Backup on Windows

2. Postinstallation, configure the Oracle Secure Backup administrative domain.
   a. From the administrative server, log in to obtool and add the clients and media servers to the domain.

      You can add Network Attached Storage (NAS) and Storage Area Network (SAN) appliances to the administrative domain as clients or media servers.
   b. Add media server role to clients.
   c. Configure devices on the media server to store data. These devices include but are not limited to tape library, disk pool, and cloud buckets.

> **See Also:**
>
> Configuring and Managing the Administrative Domain

Preparing to Install Oracle Secure Backup

Before you install Oracle Secure Backup on your hosts, certain decisions about how to configure and manage the administrative domain needs to be made. These decisions will determine how the software is installed, configured, and used.

The tasks involved in preparing to install Oracle Secure Backup are described in the following sections:

- System Requirements for Oracle Secure Backup
- Acquiring Oracle Secure Backup Installation Media
- Decide Which Role the Host Performs in the Administrative Domain

System Requirements for Oracle Secure Backup

Before you install Oracle Secure Backup on a host, ensure that the host satisfies the specified system requirements.

This following topics describe the various system requirements:

- Supported Platforms and Tape Devices
- Disk Space Requirements for Oracle Secure Backup

- Other System Requirements for Oracle Secure Backup

Supported Platforms and Tape Devices

For the list of operating systems, web browsers and Network Attached Storage (NAS) devices supported by Oracle Secure Backup, see Certify on My Oracle Support at the following URL:

`https://support.oracle.com`

Information about every tape device supported by Oracle Secure Backup is available at the following URL:

`http://www.oracle.com/technetwork/products/secure-backup/learnmore/index.html`

Disk Space Requirements for Oracle Secure Backup

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. Table 2-1 describes approximate disk space requirements.

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

Oracle Secure Backup Installation	Disk Space for Administrative Server	Disk Space for Client or Media Server
Linux x86 64-bit	75 MB	75 MB
Solaris x86 64-bit	130 MB	130 MB
Solaris SPARC 64-bit	130 MB	130 MB
HP-UX	130 MB	130 MB
IBM AIX	610 MB	610 MB

Table 2-2 describes approximate disk space required for an installation of Oracle Secure Backup on Windows with and without the administrative server.

Table 2-2 Disk Space Requirements for Oracle Secure Backup on Windows

Oracle Secure Backup Installation	Disk Space
Administrative server (can include the media server, client, or both)	112 MB
Media server, client, or both (no administrative server)	103 MB

The disk space required for the Oracle Secure Backup catalog depends on many factors. But as a general rule, plan for catalog space equal to 250% of your largest index created after a backup.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for guidelines on the growth of the Oracle Secure Backup catalog over time

Other System Requirements for Oracle Secure Backup

Each host that participates in an Oracle Secure Backup administrative domain must have a network connection and run TCP/IP. Oracle Secure Backup uses this protocol for all communication within each of its components and between its components and other system components.

Each appliance that employs a closed operating system, such as Network Attached Storage (NAS) and tape servers, must support a version of Network Data Management Protocol (NDMP) described in "Oracle Secure Backup Host Access Modes".

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 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.

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, then you must ensure that the DHCP server guarantees that a given host is always assigned the same IP address.

> **Note:**
>
> You can change the static IP of a host from one address to another, but you must restart the Oracle Secure Backup administrative server for the change to take effect.

On Oracle Secure Backup 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 restore operations from backup files.

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.

Acquiring Oracle Secure Backup Installation Media

Oracle Secure Backup installation media for each supported platform is available as a CD-ROM or as a ZIP file downloaded from the Oracle Software Delivery Cloud website:

`https://edelivery.oracle.com/`

The contents of the CD-ROM and download archive are identical.

> **Note:**
>
> If you have multiple platforms in your environment, then you must download the ZIP file or acquire the CD-ROM for each platform.

To download and extract the Oracle Secure Backup installation software:

1. Log on to your host.
   - On Windows, log in as a user with Administrator privileges.
   - On Linux/UNIX, log in as a user with `root` privileges.
2. Create a directory called `osbdownload` on a file system with enough free space to hold the downloaded installation file.
3. Open a Web browser and sign in to the Oracle Software Delivery Cloud website:

   `https://edelivery.oracle.com/`
4. On the Terms & Restrictions page, accept the **Oracle Trial License Agreement** and the **Export Restrictions**.

   Click **Continue**.
5. On the Search page, select **Oracle Database** from the product pack drop-down list.

   From the Platform drop-down list, select the platform you intend to install Oracle Secure Backup on.

   Click **Go**.
6. Select Oracle Secure Backup 18.1 from the product list.

   Click **Continue**.

   The Downloads page appears.
7. On the Downloads page, click **Download** to download the Oracle Secure Backup 18.1 installation software for the required platform.
8. Save the compressed Oracle Secure Backup 18.1 installation software to a temporary directory.
9. Expand the compressed installation software to the `osbdownload` directory you created in step 2.

You now have all of the files required to install Oracle Secure Backup release 18.1.

Decide Which Role the Host Performs in the Administrative Domain

The Oracle Secure Backup administrative domain is a set of hosts that are managed as a unit to perform backup and restore operations. Each host in the administrative domain must be assigned one of the following roles: administrative server, media server, or client.

> **See Also:**
>
> "Host Roles in an Administrative Domain"

Before you install Oracle Secure Backup on a host, you must decide the role that will be assigned to this host in the administrative domain. The software that you install depends on the role that is assigned to the host.

When you install software for the administrative role, the *software* required for the media server and client roles are also installed. The *software* required for the media server role is also installed when you install the client role. However, the host does not have the media server

role until the `admin` user grants that role with the `chhost` command after Oracle Secure Backup is installed.

> **Note:**
>
> To add the media server role to an administrative server or client after initial installation, you must create attach points using `makedev`. See *Oracle Secure Backup Reference* for details.

When you install the client role, the *software* for the media server role is also installed on the host. However, you must configure the host as a media server.

Overview of Customizing Configuration Parameters During Installation

Oracle Secure Backup enables you to customize your installation by modifying some configuration parameters that control the installation and administration process. The installation programs provide default values for all these configuration parameters. In most cases, the default values are sufficient. However, you can choose to modify the configuration parameters while installing Oracle Secure Backup.

The following are configuration parameters that you can modify during an Oracle Secure Backup installation:

- Oracle Secure Backup Temporary Directory
- Oracle Secure Backup Home Directory
- Preauthorized User for Performing Oracle Database Backup and Restore Operations
- Length of Oracle Secure Backup User Passwords
- Identity Key Certificate Length
- Oracle Secure Backup Database Directory

Oracle Secure Backup Temporary Directory

While installing Oracle Secure Backup on a host, a temporary directory is used to store 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 restart process. For these reasons, the directory must be on the local disk.

Default values are set for this parameter depending on the operating system. You can modify the default directory and specify a different directory by specifying advanced settings at the time of installation.

For Linux/UNIX and Solaris 64-bit hosts, the default temporary directory is `/usr/tmp`. For Windows, the default temporary directory is `C:\Program Files\Oracle\Backup\temp\`.

Table 2-3 Temporary Directory Requirements for Oracle Secure Backup

Oracle Secure Backup Installation	Disk Space Required
Linux x86 64-bit	600 MB
Solaris x86 64-bit	1100 MB
Solaris SPARC 64-bit	1000 MB
Windows 64-bit	600 MB
HP-UX	1200 MB
IBM AIX	1200 MB

Oracle Secure Backup Home Directory

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. The home directory, referred to as *OSB_HOME* in the documentation, is the directory into which the Oracle Secure Backup software is installed. This directory must be private to each platform and not shared through Network File System (NFS) or a similar remote file system.

The installation programs use an operating system-specific default value set for the home directory. These defaults may be changed based on the availability of disk space on your computer. You can override the default value and install the Oracle Secure Backup software into a different directory by modifying the advanced settings during installation.

The default home directory on Linux/UNIX and Solaris is `/usr/local/oracle/backup`. On Windows, the default home directory is `C:\Program Files\Oracle\Backup`. It is recommended that you install Oracle Secure Backup into the default home directory.

> **Note:**
>
> To enable users other than `root` to use `obtool` or the Oracle Secure Backup Web tool, install Oracle Secure Backup to a file system that can use the `suid` mechanism. On Linux/Unix platforms you can do this by excluding the `nosuid` option from the `/etc/fstab` file entry for that file system.

The directory that you specify as the Oracle Secure Backup home is created by the install program, but its parent folder must exist before you start the installation. For example, if you specify `/usr/local/oracle/backup` as your home, the `/usr/local/oracle` path must exist. The installer creates the `backup` directory and sets the correct owner, group, and permissions on it

Preauthorized User for Performing Oracle Database Backup and Restore Operations

Oracle Secure Backup integrates with Recovery Manager (RMAN) to enable you to backup and restore Oracle Databases. To back up Oracle Database files using RMAN with Oracle Secure Backup, you must specify an Oracle Secure Backup user who has the permissions required to perform backup and restore operations with RMAN.

During the Oracle Secure Backup installation, you can create a preauthorized user, with the rights of the `oracle` class, that is used for Oracle Database operations. If you choose to configure user preauthorization, the Oracle Secure Backup preauthorized user that you create is mapped to an operating system user whose credentials will be used to perform Oracle Database backup and restore operations. The default name for the preauthorized user is `oracle`.

To back up databases on Linux/UNIX platforms, you must specify a Linux/UNIX user name and a Linux/UNIX group name whose credentials will be used by the preauthorized user. The user name must be defined in `/etc/password` and the group name must be defined in `/etc/group`. To backup databases on Windows platforms, you must specify the domain account whose credentials are used by the preauthorized user.

> **Note:**
>
> Before you choose to create the preauthorized user, be aware that this choice involves a trade-off between convenience and security.

If you intend to use Oracle Secure Backup to perform one-time, RMAN-initiated, or unprivileged backup operations on Windows clients, then you must modify the Oracle Secure Backup `admin` and `oracle` users to assign them Windows credentials (a domain, user name and password) that are valid at the client with required privileges after you complete the Oracle Secure Backup installation. Otherwise, Oracle Secure Backup cannot perform these types of backup operations. This requirement applies regardless of the platform that acts as the administrative server.

If you do not create a preauthorized user during the installation, you can set up user preauthorization at a later stage.

> **See Also:**
>
> "Setting Up User Preauthorization in Oracle Secure Backup"

Length of Oracle Secure Backup User Passwords

Each user needs a valid Oracle Secure Backup user name and password to log in to Oracle Secure Backup and perform operations. By default, passwords for Oracle Secure Backup users must be at least 8 characters. During installation, you can modify the advanced settings and specify a different length, between 8 characters and 16 characters, for user passwords. The length specified during installation applies to the passwords used for all Oracle Secure Backup users.

Identity Key Certificate Length

Oracle Secure Backup enables secure communication between the hosts in the administrative domain. Each host is uniquely identified by an X.509 certificate signed by the Certification Authority (CA). Connections between hosts are established only after the hosts authenticate themselves to each other using identity certificates.

As of Oracle Secure Backup version 12.1.0.3, the installation program uses a default value of 3072 bits for the identity certificate key size. You can modify this value to configure the level of

security associated with every host identity certificate issued by the administrative service daemon.

The values you can set for identity certificate key length, in bits, are: 512, 768, 1024, 2048, 3072, and 4096. 1024 bits is the minimum length required for adequate security. A value of 2048 bits offers adequate security. A very high level of security can be provided by setting the key size to 3072 bits or 4096 bits.

> **Note:**
>
> Certificate key sizes smaller than 1024 are not considered secure. Certificate key sizes of 3072 or more are considered very secure.

Oracle Secure Backup Database Directory

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 Network File System (NFS) or a similar remote file system.

The installation program uses operating system-specific defaults for the database directory. You can modify the default values by configuring the advanced settings during an Oracle Secure Backup installation.

The default database directory is for Linux/UNIX and Solaris 64-bit hosts is `/usr/etc/ob`. On Windows, the default database directory is `C:\Program Files\Oracle\Backup\db`.

3

Oracle Secure Backup User Interfaces

This chapter introduces the interfaces that you can use with Oracle Secure Backup. The major interfaces to Oracle Secure Backup are:

- Oracle Enterprise Manager

  This is the primary graphical user interface for managing Oracle Secure Backup.
- Oracle Secure Backup Web tool

  This interface is used to manage file-system level backups and to perform certain other tasks not possible in Oracle Enterprise Manager.
- obtool

  This command line client exposes the full functionality of Oracle Secure Backup and is invoked by the Oracle Secure Backup Web Tool and Oracle Enterprise Manager.
- Recovery Manager (RMAN)

  The RMAN command-line utility can backup Oracle Databases to tape using Oracle Secure Backup.

> **Note:**
>
> All backup and restore operations in Oracle Secure Backup ultimately call upon a command line tool called obtar. It is generally not necessary to call obtar directly. See *Oracle Secure Backup Reference* for more details about obtar.

This chapter contains these sections:

Using Oracle Secure Backup in Enterprise Manager

You can use Oracle Enterprise Manager 10*g* (10.2) or Oracle Enterprise Manager 11*g* to perform most Oracle Secure Backup tasks, including administrative domain and hardware configuration, managing your media, and backing up and restoring databases. Oracle Enterprise Manager is the preferred Web interface for Oracle Secure Backup tasks.

This document describes the use of Oracle Enterprise Manager for most tasks, and describes the Oracle Secure Backup Web Tool only when there is no equivalent functionality in Enterprise Manager.

This section contains these topics:

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

Enabling Oracle Secure Backup Links in Oracle Enterprise Manager

If you are using releases 10.2.0.1 or 10.2.0.2 of Oracle Enterprise Manager Grid Control or release 10.2.0.2 of Oracle Enterprise Manager Database Control, then the Maintenance page does not include the Oracle Secure Backup section by default. If the Oracle Secure Backup section does not appear in the Maintenance page, then you must configure Oracle Enterprise Manager to enable the links.

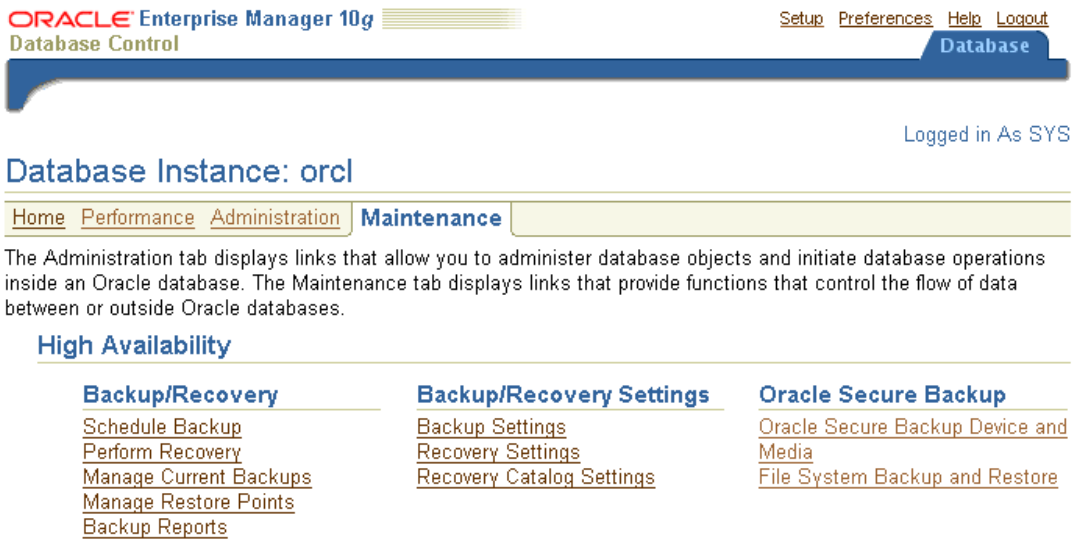
To enable the Oracle Secure Backup section in Oracle Enterprise Manager:

1. Go to the *ORACLE_HOME*`/`*hostname_SID*`/sysman/config` directory and open the `emoms.properties` file in a text editor.
2. Set `osb_enabled=true` and save the file.
3. Stop and restart the Oracle Enterprise Manager Cloud Control console with the `emctl` command:

   ```
   emctl stop dbconsole
   emctl start dbconsole
   ```

4. Go to the Maintenance page and confirm that the Oracle Secure Backup section appears, as shown in Figure 3-1.

Figure 3-1 Maintenance Page



Registering an Administrative Server in Oracle Enterprise Manager

You can make RMAN backups to the Oracle Secure Backup SBT interface three ways:

- Oracle Enterprise Manager Cloud Control
- RMAN command-line client

The Cloud Control console must run on the administrative server and can only back up an Oracle database on the administrative server. You can run the Cloud Control console on any

database host in the administrative domain and use it to back up any database. This section describes how to get started with Cloud Control.

To use Enterprise Manager to manage your backups, you must make Enterprise Manager aware of your administrative server, which stores the configuration data and catalog for the Oracle Secure Backup administrative domain.

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

1. Log in to the Oracle Enterprise Manager Cloud Control console as a user with database administrator rights.
2. In the Oracle Secure Backup section, click **Oracle Secure Backup Device and Media**.

   The Add Administrative Server page appears.
3. Log in to your Oracle Secure Backup administrative domain as follows:
   a. Enter the Oracle Secure Backup home directory in the **Oracle Secure Backup Home** field. This directory is usually `/usr/local/oracle/backup` on UNIX and Linux and `C:\Program Files\Oracle\Backup` on Windows.
   b. Enter the name of an Oracle Secure Backup administrative user in the **Username** field. For example, enter `admin`.
   c. Enter the password for the Oracle Secure Backup administrator in the **Password** field.
   d. Click **OK**.

   The Host Credentials page appears.
4. Enter the username and password of the operating system user on the administrative server. This user needs `root` privileges.

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

After you have registered the administrative server, you are ready to use Oracle Enterprise Manager with Oracle Secure Backup.

> **See Also:**
>
> *Oracle Database 2 Day DBA* for an introduction to using Oracle Enterprise Manager for database backup and recovery with RMAN

Accessing the Web Tool from Enterprise Manager

The Oracle Enterprise Manager console for a database provides a link to the Oracle Secure Backup Web tool. You can use this link when you need access to Oracle Secure Backup Web tool functions, such as file-system backup information.

To access the Oracle Secure Backup Web tool through Oracle Enterprise Manager Database Control:

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

If the Oracle Secure Backup section does not appear in the Maintenance page, then see "Enabling Oracle Secure Backup Links in Oracle Enterprise Manager".

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

   The Oracle Secure Backup Web tool interface opens, as described in "Starting a Web Tool Session".

Using the Oracle Secure Backup Web Tool

The Oracle Secure Backup Web tool is a browser-based interface that does not require installation of Oracle Enterprise Manager. It is also the only graphical interface to the file-system backup capabilities of Oracle Secure Backup.

> **Note:**
>
> You can access all functionality of Oracle Secure Backup through the Oracle Secure Backup Web Tool, including file-system level backups. However, Oracle Enterprise Manager is the preferred interface for most functionality, and provides the only graphical interface for Oracle Database backups to tape.

You can access the Oracle Secure Backup Web tool from any supported browser that can connect to the administrative server through SSL. The Apache Web server supplied with Oracle Secure Backup must be running to respond to these requests. Supported browsers are listed on Certify on My Oracle Support, at the following URL:

`https://support.oracle.com/`

> **Note:**
>
> The PHP software installed with Oracle Secure Backup is not supported for direct use by customers. It is only supported for use in implementing the Oracle Secure Backup Web tool.

This section contains these topics:

- Starting a Web Tool Session
- Web Tool Home Page
- Web Tool Configure Page
- Web Tool Manage Page
- Web Tool Backup Page
- Web Tool Restore Page

Starting a Web Tool Session

This section explains how to use the Oracle Secure Backup Web tool to access your Oracle Secure Backup administrative domain.

To start an Oracle Secure Backup Web tool session:

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

   ```
   https://hostname
   ```

   For example, you might invoke the following URL:

   ```
   https://osblin1.oracle.com
   ```

2. The browser displays a warning that the certificate is not trusted. Oracle Secure Backup installs a self-signed certificate for the Apache Web server. The Web server requires a signed certificate for data encryption purposes. The security warning appears because the browser does not recognize the signer as a registered Certification Authority (CA). This alert does not mean that your data is not encrypted, only that the CA is not recognized.

   Accept the certificate. It is not necessary to view the certificate or make any configuration changes.

   The Oracle Secure Backup Login page appears.

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

   If you are logging into the Oracle Secure Backup Web tool for the first time, then log in as the `admin` user. You can create additional users after you log in.

   > **Note:**
   >
   > Oracle recommends that you not use browser-based password managers to store Oracle Secure Backup passwords.

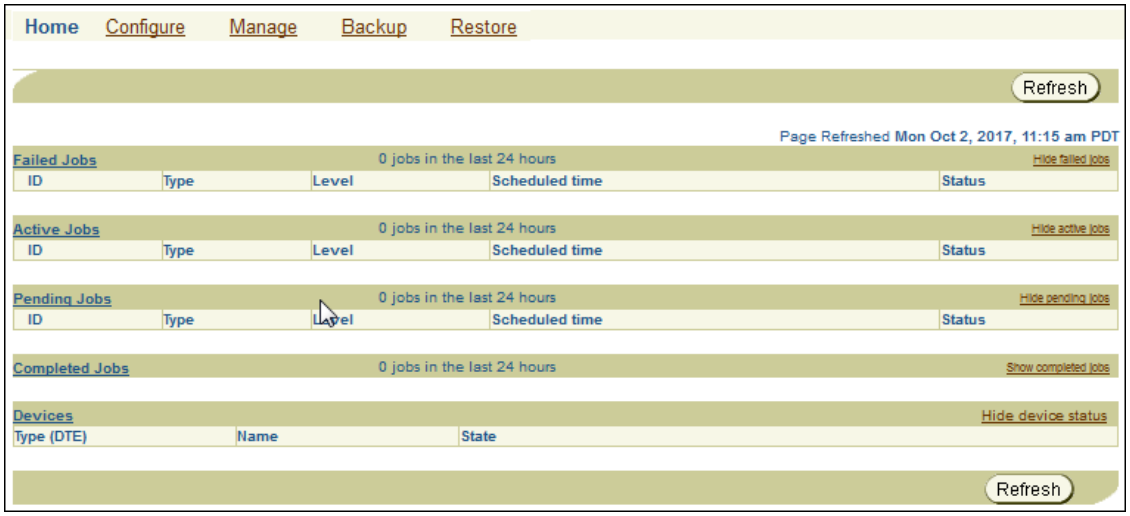
4. Click **Login**. The Oracle Secure Backup Home page appears.

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

Web Tool Home Page

After you log in to the Oracle Secure Backup Web tool interface, the Oracle Secure Backup Home page appears. This page provides a summary of the current status of each Oracle Secure Backup job, tape device, and disk pool. Figure 3-2 shows an example of the Home page.

Figure 3-2 Oracle Secure Backup Home Page



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

The **Devices** link lists the tape devices and disk pools associated with each job along with information concerning type, name, and state. The information in the State field shows the device's status and whether it is in use. For example, the states shown could be as follows:

```
tape (1) vtape1 In service, in use by obtool on localhost by process 17029
tape (2) vtape2 In service
tape (3) vtape3 Not in service
tape (4) vtape4 Not in service, in use by obtool on localhost by process 18443
```

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

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

Persistent Page Links

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

- **Help**

  Use this link to access online documentation for Oracle Secure Backup in PDF format.

- **Logout**

Logs the current user out of the Oracle Secure Backup Web tool, clears user name and password cookies, and returns to the Login page.

- **Preferences**

  Use this link to access settings for the following options:

  – Extended command output

    This option displays obtool commands used to perform actions and generate output pages for the Oracle Secure Backup Web Tool at the bottom of each page.

  – Background timeout

    This option sets the maximum idle time for `obtool` background processes used by the Oracle Secure Backup Web tool to retain state information across requests.

    Operations such as catalog browsing, data restore operations, and on-demand backup operations use a background `obtool` process to retain state information across HTTP requests. When the time between requests exceeds this limit, the process exits gracefully and the associated user's session state is lost. The default is 24 hours.

  – Select table size

    This option sets the number of rows in the display window of the Oracle Secure Backup Web tool interface. The default is 8 rows.

- **About**

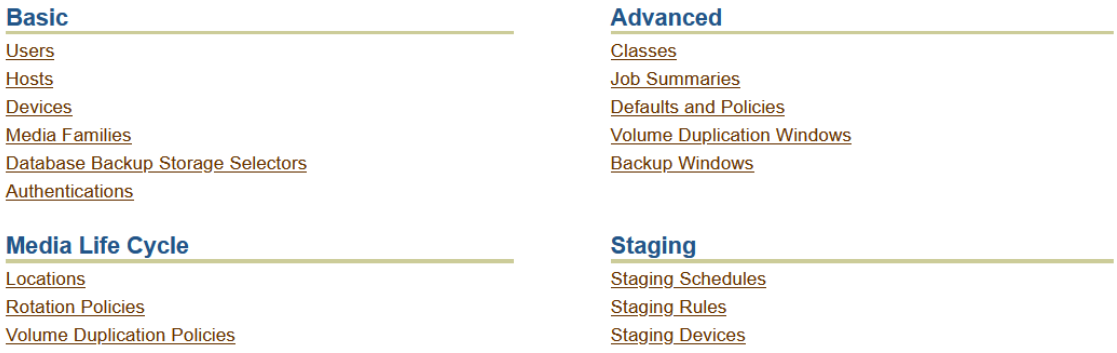
  This link displays information about the Oracle Secure Backup software, including release date, system information, administrative server name, and IP address.

Web Tool Configure Page

The Configure page contains various configuration options for Oracle Secure Backup.

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

Figure 3-3 Oracle Secure Backup Configure Page



The Configure page is divided into basic and advanced sections. The basic section contains the following links:

- **Users**

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

- **Hosts**

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

- **Devices**

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

- **Media Families**

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

- **Database Backup Storage Selectors**

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

- **Authentications**

  Click this link to configure one or more authentication options for using Oracle Cloud Infrastructure with Oracle Secure Backup. It contains information related to tenancy, user ocid, identity domain, and so on of Oracle Cloud Infrastructure.

The advanced section contains the following links:

- **Classes**

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

- **Job Summaries**

  Click this link to create a job summary schedule for generation of job summaries for email distribution.

  A job summary is a generated text file report that tells you whether a backup operation was successful. Oracle Secure Backup can generate and email job summaries detailing the status of each scheduled backup.

- **Defaults and Policies**

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

Web Tool Manage Page

Click the **Manage** tab to display management options. Figure 3-4 shows an example of the Manage page.

Figure 3-4 Oracle Secure Backup Manage Page

The Manage page is divided into four sections.

The Devices section includes the following links:

- **Disk Pools**

  Click this link to view the disk pool space utilization and to delete expired backup image instances from disk pools.

- **Tape Drives**

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

- **Libraries**

  Click this link to view and control libraries.

- **Device Reservations**

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

- **Cloud Storage**

  Click this link to view and control Oracle Secure Backup cloud storage.

The Management section includes the following links:

- **Jobs**

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

- **Volumes**

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

- **Backup Images**

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

- **On Demand Stage Scan**

  Click this link to manage on-demand stage scans.

The Advanced Section includes the following links:

- **Backup Image Instances**

  Click this link to modify the properties of backup image instances or to delete backup image instances. A backup image instance contains the actual data that is backed up. The first backup image instance is created by the backup operation. Multiple backup image instances can be created for one backup image, with each instance being stored in a different storage medium.

- **Database Backup Pieces**

  Click this link to manage backup pieces created by Recovery Manager (RMAN) for Oracle Database backups.

- **Catalog Imports**

  Click this link to import backup catalog data from disk pools or tapes into the administrative domain.

- **Checkpoints**

  Click this link to list and delete checkpoints describing certain in-progress, failed, and completed Network Data Management Protocol (NDMP) backups.

- **Daemons**

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

The Media Life Cycle section contains the following links:

- **Schedule Vaulting Scan**

  Click this link to create, modify, or delete vaulting scans.

- **Schedule Volume Duplication Scans**

  Click this link to create, modify, or delete volume duplication scans.

- **Pick and Distribution Reports**

  Click this link to view distribution reports.

- **Location Reports**

  Click this link to display location reports for tape devices. The details include the next location and the date on which the tape moves to that location.

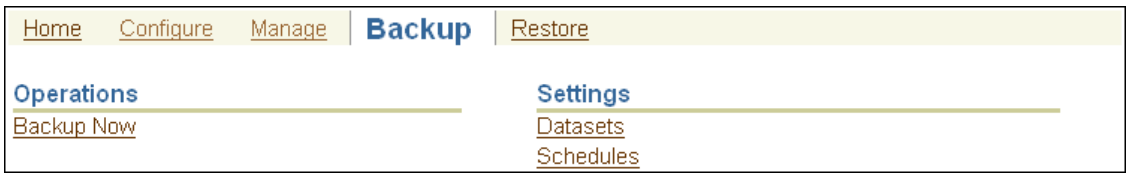
- **Vault Now**

  Click this link to perform vaulting.

Web Tool Backup Page

Click the **Backup** tab to display backup image options. Figure 3-5 shows a sample page.

Figure 3-5 Oracle Secure Backup Backup Page



The Backup page is divided into Operations and Settings sections. The Operations section contains the following link:

- **Backup Now**

  Click this link to perform one-time backups of data described by an existing dataset file.

The Settings section contains the following links:

- **Datasets**

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

- **Schedules**

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

Web Tool Restore Page

Click the **Restore** tab to display restore options. Figure 3-6 shows a sample page.

Figure 3-6 Oracle Secure Backup Restore Page

The Restore page has a single Operations section with the following links:

- **Backup Catalog**

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

- **Directly from Media**

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

Using obtool

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

This section contains these topics:

- Displaying Help for Invoking obtool
- Starting obtool in Interactive Mode
- Running obtool Commands in Interactive Mode
- Executing obtool Commands in Noninteractive Mode
- Ending an obtool Session
- Starting obtool as a Specific User

> **See also:**
>
> *Oracle Secure Backup Reference* for a more detailed discussion of invoking `obtool` and for more information on obtar, which is mostly used internally by `obtool`

Displaying Help for Invoking obtool

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

```
% obtool help invocation
```

Starting obtool in Interactive Mode

Enter `obtool` at the command line to use obtool in interactive mode.

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

> **Note:**
>
> The installer for Oracle Secure Backup creates the `admin` user automatically, and prompts for a password. Use these credentials when you log in to Oracle Secure Backup for the first time after installation.
>
> The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the user be prompted for the password.

Running obtool Commands in Interactive Mode

You can enter the commands described in *Oracle Secure Backup Reference* at the obtool prompt. For example, the `lshost` command displays information about the hosts in your administrative domain:

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

Redirecting obtool Input from Text Files

You can use the < command in interactive mode to read text files containing multiple obtool commands. For example, you can create a file called my_script.txt with multiple `obtool` commands and redirect the `obtool` input to this script as follows:

```
ob> < /my_dir/my_script.txt
```

`obtool` runs the commands from the file and then returns to the `ob>` prompt for your next command.

Executing obtool Commands in Noninteractive Mode

You can run obtool in noninteractive mode from the Linux or UNIX shell or from the Windows command prompt with arguments that specify the command to run. `obtool` runs the specified command immediately and exits. Use the following syntax:

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

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

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

Running Multiple Commands in Noninteractive Mode

You can run multiple commands in one invocation of obtool by separating the commands with a semicolon on the command line.

> **Note:**
>
> Follow the quoting conventions of your host operating system shell or command line interpreter when entering a semicolon in the command line. For example, in a bash shell session, quote the semicolon as follows:
>
> ```
> $ obtool lshost ';' lsdev
> ```

Redirecting Input in Noninteractive Mode

You can use the < command in noninteractive mode to read text files containing multiple obtool commands. For example, you can create a file called my_script.txt with multiple `obtool` commands and redirect the `obtool` input to this script as follows:

```
% obtool < /my_dir/my_script.txt
```

`obtool` runs the commands from the file and then returns to the operating system prompt for your next command.

Ending an obtool Session

You can end an obtool session by using one of these commands:

- `exit`

  This command ends the `obtool` session, but a login token preserves your credentials, so that the next time you start `obtool` you are not prompted for a user name or password.

- `quit`

  This command is a synonym for `exit`.

- `logout`

  This command ends the `obtool` session and destroys the login token, so that you are prompted for credentials at the start of your next `obtool` session.

In the following example, login credentials are required for the first session, because the login token has expired. This first session is ended with an `exit` command, and a second session is started. No login credentials are required for this second session, because the login token was preserved. The second session is ended with a `logout` command, and a third session is started. The third session requires login credentials because the login token was destroyed by the `logout` command.

```
[cfoch@stbcs06-1 ~]$ obtool
Oracle Secure Backup 18.1.0.0.0
Warning: auto-login failed - login token has expired
login: admin
ob> exit
[cfoch@stbcs06-1 ~]$ obtool
ob> logout
[cfoch@stbcs06-1 ~]$ obtool
Oracle Secure Backup 18.1.0.0.0
login: admin
ob>
```

Starting obtool as a Specific User

You can force obtool to use different credentials when starting, destroying any existing login token. To do so, use the `-u` option with `obtool`, specifying the name of the user for the session. For example:

```
[root@osblin1 ~]# obtool -u admin
Password:
ob>
```

Using Oracle Secure Backup through Recovery Manager (RMAN)

Oracle Secure Backup, through the System Backup to Tape (SBT) interface, serves as a media management layer for RMAN. You can use RMAN to directly backup Oracle Databases to tape.

You can access RMAN through one of the following interfaces: RMAN executable or Oracle Enterprise Manager Cloud Control. RMAN communicates with Oracle Secure Backup through the SBT interface.

It is recommended that you use RMAN to perform online backups of your Oracle Database. Before you use RMAN to perform tape backups, you must configure RMAN as described in "Configuring Oracle Secure Backup for Use with RMAN".

Configuring Oracle Secure Backup for Use with RMAN

This section describes the configuration steps required in order to enable RMAN to backup Oracle Databases to tape through Oracle Secure Backup. Before you perform the

configuration steps, ensure that you install the Oracle Database software and Oracle Secure Backup.

To configure Oracle Secure Backup for use with RMAN:

1. Create a preauthorized user that the RMAN server session can use to access Oracle Secure Backup.
2. Create a database backup storage selector that contains details about the databases you want to backup or restore using the SBT interface. The storage selector contains details about the Oracle Database backup or restore operation.

Setting Up User Preauthorization in Oracle Secure Backup

User preauthorization enables you to use Oracle Secure Backup without going through the normal Oracle Secure Backup login requirements. In the case of RMAN, preauthorization is used to determine the Oracle Secure Backup user under which a specific RMAN operation, such as backup or restore, is performed.

You can preauthorize access to Oracle Secure Backup services and data from specific hosts and UNIX users or Windows accounts. For each host within an Oracle Secure Backup administrative domain, you can create one or more one-to-one mappings between the operating system and Oracle Secure Backup user. If a preauthorization mapping is not found for a particular backup or restore request, the request fails.

> **See Also:**
>
> *Oracle Secure Backup Administrator's* Guide for more information on the steps for setting preauthorized users.

Defining Backup Storage Selectors Using Oracle Secure Backup

Database backup storage selectors enable you to provide detailed information about the backup or restore operation that needs to be performed. A storage selector is an Oracle Secure Backup object that associates an RMAN operation with storage media that is managed using Oracle Secure Backup.

A storage selector typically contains information such as the following:

- Oracle Databases that must be backed up or restored
- Hosts to which the database storage selector applies
- Devices and media families that must be used for the backup or restore operation

> **See Also:**
>
> “Configuring Database Backup Storage Selectors" in *Oracle Secure Backup Administrator's Guide* for information about defining database backup storage selectors

4

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 contains the following sections:

Prerequisites for Installing on Linux or UNIX

Before starting Oracle Secure Backup installation on a Linux host, check the following prerequisites.

- Complete the planning tasks described in Preparing to Install Oracle Secure Backup.
- Preconfigure the required attach points for your tape drives and libraries on your media server systems.

  > **See Also:**
  >
  > Configuring Platform-Specific Media Server Devices

- Before adding Oracle Secure Backup tape libraries and drives to an administrative domain, disable or stop any system software that scans and opens arbitrary SCSI targets (for example, tape library monitoring software).
- You have the `root` privileges on each host to perform the installation.
- Ensure that the host has the packages `sg3_utils` and the `sg3_utils-libs` installed. To run the `sg_map` command, the host requires these packages.

  > **Note:**
  >
  > To install Oracle Secure Backup on a host with Oracle Linux 8, ensure that the host has the packages `csh` and `libnsl` installed.

For more information, contact your system administrator or Linux operating system documentation.

- For installing the administrative server or media server role, verify the physical and network requirements for the host as discussed in Choosing Secure Hosts for the Administrative and Media Servers.
- Oracle Secure Backup requires NDMP port 10000 for installing on your host. If this port is not available on your host, for example other applications are using this port, then the installation cannot complete successfully. Therefore, Oracle Secure Backup provides an option to manually specify the NDMP Port for installation.

  For more information, see Table 4-2.

Obtain the Oracle Secure Backup software distribution and store it in a secure directory that all hosts can access.

> **See Also:**
>
> Acquiring Oracle Secure Backup Installation Media

Secure Location Check

The installation process checks whether the directory has the correct privileges. For the installation to complete successfully, the secure directory must have the owner and group privileges as indicated in Table 3-1. However, you can disable the secure location check using the following command:

```
setup --securepath
```

> **Note:**
>
> Use this option only after you confirm that the installation location is fully protected.

Table 4-1 Secure Directory Owner and Group Privileges

Platform	Required Owner and Group
Linux	`root:root`
Solaris SPARC	`root:root` or `root:sys`
Solarix X86	`root:root` or `root:sys`
IBM AIX	`root:system` or `bin:bin`
HPUX	`root:root` or `bin:bin`

> **Note:**
>
> Oracle recommends that you store the Oracle Secure Backup software package on a network accessible share or in a local temporary directory.
>
> For example, if you store the software package in an NFS shared path `/net/myfiler/export/vol0/home/osb_media_dir/`*`OSB-OS-package`*, then you can run the install utility setup on all hosts in your network that have access to this location. This not only prevents duplicate copies of the software package but also saves space on your network.

Options for Installing on Linux or UNIX

For installing Oracle Secure Backup on Linux or UNIX, you can use the following parameters.

Table 4-2 Installation Parameters for Linux or UNIX

Parameter	Description	Required for Unattended Installation
`--addinghostid` *`hostname`*	Specifies the adding host ID.	Yes, if `--noaddinghostid` is not specified
`--install_role Client`	Disables user prompts for advanced settings and automatically selects the client host role.	Yes
`--noaddinghostid`	Disables administrative host identification check while adding a client to the administrative domain.	Yes, if `--addinghostid` *`hostname`* is not spedified
`--securepath`	Disables secure directory check for the installation location. Use this option only after you confirm that the installation location is fully protected.	No
`-t` *`path-to-alternate-temp-directory`*	Specifies an alternative install temp directory, if the default temp directory (`/usr/tmp`) is not available or has insufficient space.	No
`--ndmp_port`	Specifies the port used by Oracle Secure Backup for NDMP communication.	Yes, if the default port 10000 is not available
`--disable_web_tool`	Installs the Oracle Secure Backup administrative server with the web server disabled.	No

Interactive Installation on Linux or UNIX

Follow these steps to perform an interactive installation of Oracle Secure Backup on Linux or UNIX operating system.

1. Log in to your host as `root`.
2. Open a terminal window and go to the Oracle Secure Backup home directory, `$OSB_HOME`, where the software package is stored.

Oracle recommends that you use the standard install location `/usr/local/oracle/backup` as the home directory. However, you can specify a different directory for the installation. The setup utility prompts you to confirm the nonstandard location.

If the Oracle Secure Backup software package is stored in a different directory, for example `/net/myfiler/export/vol0/home/osb_media_dir/`*`OSB-OS-package`*, and you want to install in the `$OSB_HOME` location, then you can do this. Create the `$OSB_HOME` directory if it does not exist, go to the `$OSB_HOME` directory, and enter the full path of the setup utility for the version of Oracle Secure Backup.

```
# mkdir -p /usr/local/oracle/backup
# cd /usr/local/oracle/backup
# /net/myfiler/export/vol0/home/osb_media_dir/OSB-OS-package/setup
```

The setup utility uses as a default temporary directory, `/usr/tmp`, for the installation. If this directory is not available or has insufficient space, then you can specify an alternate location for the temporary directory using the `-t` option.

```
# /net/myfiler/export/vol0/home/osb_media_dir/OSB-OS-package/setup -t path-
to-alternate-temp-directory
```

To install Oracle Secure Backup on another NDMP Port if the default port 10000 is not available, run the setup utility with the option `--ndmp_port`.

```
# /net/myfiler/export/vol0/home/osb_media_dir/OSB-OS-package/setup --
ndmp_port 12345
```

To install the Oracle Secure Backup administrative server with the web server disabled, run the setup utility with the option `--disable_web_tool`.

```
# /net/myfiler/export/vol0/home/osb_media_dir/OSB-OS-package/setup --
disable_web_tool
```

3. Run the setup utility to start the installation process.

   The window displays details about the installation, such as the Oracle Secure Backup version, platform details, and progress information of the packages.

   > **Note:**
   >
   > The setup utility, if interrupted, may generate some files, namely `OBnnnn` or `OBnnnn.Z`, in the temporary directory. It is safe to delete these temporary files.

4. Specify the host role from the following options:

   - **A**: to install the administrative server and client. For detailed information, see Installing Administrative Server on Linux or UNIX
   - **B**: to install only client role. For detailed information, see Installing Client Role on Linux or UNIX

For both options, the setup utility installs the media server packages on the host. An administrative user can add the media server role to clients while configuring the administrative domain.

> **Note:**
>
> - Although the *software* required for a media server is installed, the host does not have the media server role until the `admin` user grants that role with the `chhost` command after Oracle Secure Backup is installed.
> - To add the media server role to an administrative server or client after initial installation, you must use the `chdev` command with the `--addrole` option.

The setup utility completes the installation and displays a confirmation message: `Oracle Secure Backup was installed.`

The installation generates a log file, namely `osb_install.log`, and stores it in either the default temporary directory, `/usr/tmp`, or a user-specified temporary directory.

Similarly, you can install Oracle Secure Backup in silent mode on your Linux or UNIX host. For more information, see Noninteractive or Unattended Installation on Linux or UNIX.

> **Note:**
>
> For installing in an Oracle Real Application Clusters (Oracle RAC) environment, install Oracle Secure Backup on each node in the cluster.

Installing Administrative Server on Linux or UNIX

While running the Oracle Secure Backup setup utility on a Linux or UNIX host, you can install the administrative server.

1. Specify the host role in the setup utility. Select **Option A** to install the host as the administrative server.
2. Specify an e-mail address for the administrative user, if you want to receive notifications about jobs, operations, status, and so on from the administrative server. Leave this blank if you do not want to receive notifications.
3. Select whether you want to customize configuration parameters for the installation.
   - Enter **y** to configure the parameters.

> **See Also:**
>
> Overview of Customizing Configuration Parameters During Installation to know the configuration parameters that you can modify
>
> Specifying Advanced Settings for Linux/UNIX to understand how to modify the configuration parameters

- Enter **n** to use the default values.

4. Create a password to encrypt the Oracle Secure Backup keystore.

> **Important:**
>
> Ensure to note the keystore password and keep it safe. In case of a failure, you require this password to recover your administrative server.

Oracle Secure Backup stores the password in the Cloud Wallet.

5. Create a password for the Oracle Secure Backup administrative server.

   For both, keystore password and administrative server password, Oracle recommends that you select a password of minimum eight characters with a combination of alphabetic and numeric values. You can also customize the minimum length of the password as a part of Specifying Advanced Settings for Linux/UNIX.

Now, continue the installation of Oracle Secure Backup on your Linux or UNIX host.

When you install the Oracle Secure Backup administrative server, it also installs the web server. However, while installing the administrative server Oracle Secure Backup provides an option to disable the web server using the following command:

```
setup --disable_web_tool
```

Installing Client Role on Linux or UNIX

While running the Oracle Secure Backup setup utility on a Linux or UNIX host, you can install the client role.

1. Specify the host role in the setup utility. Select **Option B** to install the client role.
2. Select whether you want to customize configuration parameters for the installation.
   - Enter **y** to configure advanced settings.

   > **See Also:**
   >
   > Specifying Advanced Settings for Linux/UNIX to learn how to modify these parameters

   For a client, you can modify the Oracle Secure Backup temporary directory and the option to start Oracle Secure Backup daemons when the host restarts.

   - Enter **n** to use the default values for the parameters.
3. Enter the host ID of the administrative server that adds the client to its domain.

   You can enter either the Fully Qualified Domain Name (FQDN) or the IP address of the administrative server. Specifying the IP address avoids connectivity failures during problems with nameservice.

   The client stores the specified IP address or FQDN in `/etc/obconfig` file. This information is essential for authentication purpose and for establishing the initial connection between the client and the administrative server.

While installing the client, you can disable adding IP address using the following command:

```
# setup --noaddinghostid
```

Now, continue the installation of Oracle Secure Backup on your Linux or UNIX host.

Specifying Advanced Settings for Linux/UNIX

Oracle Secure Backup uses default values for most configuration parameters that are required during the installation process. This includes parameters such as the identify certificate key size, minimum length for user passwords, and so on. In most cases, the default values are sufficient. However, you can provide new values for the parameters by configuring advanced settings during the installation.

To configure advanced settings, the `setup` script displays a numbered list containing the parameters that can be configured. To modify a particular parameter, enter the number adjacent to that parameter and provide the required values. For example, to modify the minimum length for user passwords, type 2. The default setting is displayed in brackets beside the option name. Enter the new minimum password length that you wish to use.

Only one advanced parameter can be modified at a time. If you want to make multiple changes, you need to enter them separately.

> **See Also:**
>
> "Overview of Customizing Configuration Parameters During Installation" for information about the installation parameters that can be modified

Noninteractive or Unattended Installation on Linux or UNIX

Oracle Secure Backup supports noninteractive or unattended installation of client role on a Linux or UNIX host.

For Oracle Secure Backup unattended installation , the prerequisites and the installation steps are similar to interactive installation. See Prerequisites for Installing on Linux or UNIX.

For unattended installation of client role on Linux or UNIX:

1. Log in to your host as `root`.
2. Open a terminal window and go to the Oracle Secure Backup home directory, `$OSB_HOME`, where the software package is stored.

   The default home directory is `/usr/local/oracle/backup`.
3. Run the setup utility with an additional parameter, `--install_role Client`.

   ```
   setup --install_role Client
   ```

   The `--install_role Client` parameter automatically selects the client role on your host. Using this parameter, the setup utility proceeds with the installation without providing any options for advanced settings.

   Moreover, the setup utility supports additional parameters for unattended installation.

- **With adding host ID**: to specify an adding host ID, for example `myhost.oracle.com`

  ```
  setup --install_role Client --addinghostid myhost.oracle.com
  ```

- **Without adding host ID**: to disable the secure registration feature and install Oracle Secure Backup without specifying an adding host ID

  ```
  setup --install_role Client --noaddinghostid
  ```

- **Specify NDMP Port**: to use another NDMP Port for installation, if the default port 10000 is not available

  ```
  setup --install_role Client --ndmp_port 12345
  ```

The setup utility completes the installation and displays a confirmation message: `Oracle Secure Backup was installed.`

Configuring Platform-Specific Media Server Devices

This section explains how to configure tape drives and libraries for Oracle Secure Backup to communicate with them. In versions 10.4.0.3 and earlier, the Oracle Secure Backup utility `discoverdev` worked only with NDMP filers. As of Oracle Secure Backup 12.1 the `discoverdev` utility works on all media server platforms (with the exception of HP-UX). In Oracle Secure Backup 12.1 and later `discoverdev` is the preferred method of configuring devices because it is faster and it removes the possibility of user error when variables are manually entered in `mkdev`.

> **Note:**
>
> In the past, `makedev` was used on all platforms in Oracle Secure Backup to generate system attach points. The current practice is to use native SGEN device drivers whenever possible (Solaris and Linux), but system attach points must still be created manually using `makedev` on HP-UX. Instructions for running `makedev` on AIX are only included in this document for situations where there might be a reason for doing it manually, but using `discoverdev` is the preferred procedure.

Device attach points must exist prior to running `discoverdev` in order for it to function correctly. Table 4-3 lists the requirements to access device attach points, for each platform.

Table 4-3 Platform-Specific Requirements for Accessing Attach Points

Platform	Requirements
Linux	`sg_map` must be operational for use by `discoverdev`
Solaris	sgen driver must be installed for use by `discoverdev`
AIX	(Optional) `makedev` can be used to manually create system attach point
HP-UX	`makedev` must be used to create attach points prior to running `mkdev` as `discoverdev` is not yet available on this platform

> **Note:**
>
> The Oracle Secure Backup `makedev` command should not be confused with `obtool mkdev`. `makedev` use is required on HP-UX and it can be used on AIX to create Oracle Secure Backup custom system attach points. `makedev` is not used on Solaris or Linux where Native SCSI Generic operating system based attach points are used. `obtool discoverdev` automates the `obtool mkdev` command which detects and utilizes existing attach points but `discoverdev` itself does not create system attach points. `obtool mkdev` is the manual device configuration command which utilizes attach points to configure devices for use in Oracle Secure Backup.

This section contains the following topics:

Configuring Devices on Linux Media Servers

Configuring a Linux host as an Oracle Secure Backup media server requires that the SCSI Generic driver be installed on that host. The driver enables Oracle Secure Backup to interact with tape and library devices. The host must be configured to automatically reload the driver after a restart. It is also recommended that persistent bindings be configured. By using persistent bindings, the Host Bus Adapter pairs the SCSI targets and LUNs for each device with their WWNs, thus preventing the attach points from being shuffled among devices during a reboot. Without persistent bindings, devices can become inaccessible by Oracle Secure Backup until their attach points are updated to reflect their new values. Please consult your system administrator or operating system documentation for information on how to configure persistent bindings on your Linux media server systems.

To identify the `/dev/sg` that corresponds to the specific tape device you are interested in, obtain the `sg_map` output by executing the following Linux command:

```
# sg_map -i -x

/dev/sg0 5 0 0 0 8 STK SL3000 4.00

/dev/sg1 5 0 0 1 8 STK SL3000 4.00

/dev/sg2 5 0 1 0 8 STK SL500 1466

/dev/sg3 5 0 3 0 1 /dev/nst2 HP Ultrium 5-SCSI I11V

/dev/sg4 5 0 4 0 1 /dev/nst3 STK T10000C 1.57

/dev/sg5 5 0 5 0 1 /dev/nst4 HP Ultrium 5-SCSI I3AS

/dev/sg6 5 0 6 0 1 /dev/nst5 HP Ultrium 5-SCSI I3AS

/dev/sg7 5 0 7 0 1 /dev/nst6 STK T10000C 1.57
```

Once these attach points are present on the system, Oracle Secure Backup's `discoverdev` will be able to use them in creating devices.

Here is an example showing the use of `discoverdev` to create devices:

```
ob> lsh
storabck06       admin,mediaserver,client          (via OB)   in service

ob> discoverdev -ic -h storabck06
   Device-Type   Device-Model            Serial-Number        Attachpoint
   Library       STK     SL3000           464970G+1333SY1401   storabck06:/dev/sg0
create device object storabck06_lib_1? (a, n, q, y, ?) [y]:
   Tape          HP      Ultrium 5-SCSI  HU1328WGF6           storabck06:/dev/sg3
create device object storabck06_tape_1? (a, n, q, y, ?) [y]:
   Tape          STK     T10000C HU1327WEYJ           storabck06:/dev/sg4
create device object storabck06_tape_2? (a, n, q, y, ?) [y]:
Checking each library to associate discovered drive(s) with DTE...
    Assigning DTE 1 in library storabck06_lib_1 for drive storabck06_tape_1 with serial
number: HU1328WGF6
    Assigning DTE 2 in library storabck06_lib_1 for drive storabck06_tape_2 with serial
number: HU1327WEYJ
ob>

ob> lsd -l
storabck06_lib_1:
    Device type:            library
    Model:                  STK     SL3000
    Serial number:          464970G+1333SY1401
    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
    Ejection type:          ??
    Min writable volumes:   0
    UUID:                   9a9c2982-1b34-1032-9c3e-aad50196aa4f
    Attachment 1:
        Host:               storabck06
        Raw device:         /dev/sg0

storabck06_tape_1:
    Device type:            tape
    Model:                  HP      Ultrium 5-SCSI
    Serial number:          HU1328WGF6
    In service:             yes
    Automount:              yes
    Position interval:      [undetermined]
    Debug mode:             no
    Blocking factor:        (default)
    Max blocking factor:    (default)
    UUID:                   9aa59b5c-1b34-1032-9c3e-aad50196aa4f
    Attachment 1:
        Host:               storabck06
        Raw device:         /dev/sg3

storabck06_tape_2:
    Device type:            tape
    Model:                  STK     T10000C
    Serial number:          HU1327WEYJ
    In service:             yes
    Automount:              yes
    Position interval:      [undetermined]
    Debug mode:             no
```

```
Blocking factor:        (default)
Max blocking factor:    (default)
UUID:                   9aa59f4e-1b34-1032-9c3e-aad50196aa4f
Attachment 1:
    Host:               storabck06
    Raw device:         /dev/sg4
```

Manually creating devices using `mkdev` in Linux

In Oracle Secure Backup 12.1 and later, `obtool discoverdev` is the preferred method of configuring devices in Linux, but in some cases it may still be necessary to create devices manually using `obtool mkdev`. This section explains how to run `mkdev` in Linux.

Oracle Secure Backup's `discoverdev` uses thee `sg_map -i -x` output as attach points. The link names themselves can be used as Oracle Secure Backup device attach points in `mkdev`.

```
# sg_map -i -x
/dev/sg0  5 0 0 0  8  STK       SL3000            4.00
/dev/sg1  5 0 0 1  8  STK       SL3000            4.00
/dev/sg2  5 0 1 0  8  STK       SL500             1466
/dev/sg3  5 0 3 0  1  /dev/nst2  HP        Ultrium 5-SCSI    I11V
/dev/sg4  5 0 4 0  1  /dev/nst3  STK       T10000C           1.57
/dev/sg5  5 0 5 0  1  /dev/nst4  HP        Ultrium 5-SCSI    I3AS
/dev/sg6  5 0 6 0  1  /dev/nst5  HP        Ultrium 5-SCSI    I3AS
/dev/sg7  5 0 7 0  1  /dev/nst6  STK       T10000C           1.57
```

The following example shows how this is done:

`/dev/sg0` translates to a library attachment in `obtool mkdev` of:

```
# obtool mkdev --type lib --attach <hostname>:/dev/sg0 lib
```

`/dev/scsi/sg3` translates to a drive attachment in `obtool mkdev` of:

```
# obtool mkdev --type tape --attach <hostname>:/dev/sg3 -l lib -d 1 drv
```

It is also possible to create links in `/dev` that point to the attach points. For example, if you wish to create `/dev/obl<n>` or `/dev/obt<n>` links for use as attachments in Oracle Secure Backup, you would do the following:

```
# ln -s /dev/sg0 /dev/obl0 for the library (the "l" stands for library)

# ln -s /dev/sg3 /dev/obt0 for the drive (the "t" stands for tape drive)
```

If you choose to do this, there must be a unique `/dev/obl<n>` or `/dev/obt<n>` entry where `n` starts at 0 and increments by 1 for each device that Oracle Secure Backup will utilize.

The same device configurations shown earlier would now look like this:

```
# obtool mkdev --type lib --attach <hostname>:/dev/obl0 lib

# obtool mkdev --type tape --attach <hostname>:/dev/obt0 -l lib -d 1 drv
```

Configuring Devices on Solaris Media Servers

You must enable the Solaris sgen driver for changer (library) and sequential (tape) devices before a host can access SCSI & Fibre Channel attached devices and be configured as an Oracle Secure Backup media server.

To enable sgen drivers

1. If you have `sgen.conf` file in `/kernel/drv/` then, copy `/kernel/drv/sgen.conf` to `/etc/driver/drv/sgen.conf` by issuing the following:
   `cp /kernel/drv/sgen.conf /etc/driver/drv/sgen.conf`
2. Enable sequential (01) and changer (01) devices by adding the following line to the `/kernel/drv/sgen.conf` file:

   ```
   device-type-config-list="sequential","changer";
   ```

   > **Note:**
   >
   > If `device-type-config-list` is already defined for other devices, add `sequential` and `changer` to the existing list in the `sgen.conf` file.

3. Verify that an entry for an sgen file exists in the `/etc/minor_perm`. For example:
   `sgen * 0600 root sys`
4. Verify that an entry for an sgen file exists in the `/etc/name_to_major`. For example:
   `sgen 151`
5. Remove any old sgen drivers by using the following commands:

   ```
   rm -r /dev/scsi/changer
   ```

   ```
   rm -r /dev/scsi/sequential
   ```

6. In the `/kernel/drv/sgen.conf` file, add a line for each device's target and LUN parameters.

   You can obtain these details from the output of the `prtconf -Dv` and `dmseg` commands. An example is shown here.

   ```
   name="sgen" class="scsi" target=0 lun=0; name="sgen" class="scsi" target=1
   lun=0; name="sgen" class="scsi" target=2 lun=0; name="sgen" class="scsi"
   target=3 lun=0;
   .....
   name="sgen" class="scsi" target=13 lun=0; name="sgen" class="scsi"
   target=14 lun=0; name="sgen" class="scsi" target=15 lun=0;
   ```

7. Run the following to remove any existing active sgen device configuration.

   ```
   rem_drv sgen
   rem_drv st
   rem_drv sas
   ```

8. Use the following command, typed all on one line, to configure the sgen drivers:

   ```
   add_drv -m '* 0666 bin bin' -i '"scsiclass,01" "scsiclass,08" "scsa,01.bmpt"
   "scsa,08.bmpt"' sgen
   ```

9. To check whether the sgen attachments are created, run the following commands as the root user:

   ```
   # ls -latr /dev/scsi/seq*
   total 10
   drwxr-xr-x 5 root sys 512 Jan 29 17:01 ..
   ```

```
lrwxrwxrwx 1 root sys 57 Jan 29 17:01 c1t1d0 -> ../../../devices/pci@1f,4000/
scsi@3,1/sgen@1,0:sequential
lrwxrwxrwx 1 root sys 57 Jan 29 17:01 c1t2d0 -> ../../../devices/pci@1f,4000/
scsi@3,1/sgen@2,0:sequential
lrwxrwxrwx 1 root sys 57 Jan 29 17:01 c1t5d0 -> ../../../devices/pci@1f,4000/
scsi@3,1/sgen@5,0:sequential
drwxr-xr-x 2 root sys 512 Jan 29 17:01 .

# ls -latr /dev/scsi/cha*
total 8
lrwxrwxrwx 1 root sys 54 Jan 29 17:01 c1t0d0 -> ../../../devices/pci@1f,4000/
scsi@3,1/sgen@0,0:changer
drwxr-xr-x 5 root sys 512 Jan 29 17:01 ..
lrwxrwxrwx 1 root sys 54 Jan 29 17:01 c1t4d0 -> ../../../devices/pci@1f,4000/
scsi@3,1/sgen@4,0:changer
drwxr-xr-x 2 root sys 512 Jan 29 17:01 .
```

10. If you do not find the sgen driver entries, reboot your system using the following commands:

```
# touch /reconfigure

# reboot
```

11. Create devices in Solaris using the sgen drivers by running `discoverdev`:

```
ob> lsh
storabck18       admin,mediaserver,client          (via OB)    in service
ob> discoverdev -ic -h storabck18
   Device-Type   Device-Model            Serial-Number        Attachpoint
   Library       STK     SL150          464970G+1333SY1401   storabck18:/dev/scsi/
changer/c2t500104F000D14F89d1
create device object storabck18_lib_1? (a, n, q, y, ?) [y]: y
   Tape          HP      Ultrium 5-SCSI  HU1328WGF6           storabck18:/dev/scsi/
sequential/c2t500104F000D14F89d0
create device object storabck18_tape_1? (a, n, q, y, ?) [y]: y
   Tape          HP      Ultrium 5-SCSI  HU1327WEYJ           storabck18:/dev/scsi/
sequential/c2t500104F000D14F8Cd0
create device object storabck18_tape_2? (a, n, q, y, ?) [y]: y

Checking each library to associate discovered drive(s) with DTE...
    Assigning DTE 1 in library storabck18_lib_1 for drive storabck18_tape_1 with
serial number: HU1328WGF6
    Assigning DTE 2 in library storabck18_lib_1 for drive storabck18_tape_2 with
serial number: HU1327WEYJ
ob>

ob> lsd -l
storabck18_lib_1:
    Device type:            library
    Model:                  STK     SL150
    Serial number:          464970G+1333SY1401
    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
    Ejection type:          ??
    Min writable volumes:   0
    UUID:                   9a9c2982-1b34-1032-9c3e-aad50196aa4f
    Attachment 1:
        Host:               storabck18
```

```
        Raw device:         /dev/scsi/changer/c2t500104F000D14F89d1

storabck18_tape_1:
    Device type:            tape
    Model:                  HP      Ultrium 5-SCSI
    Serial number:          HU1328WGF6
    In service:             yes
    Automount:              yes
    Position interval:      [undetermined]
    Debug mode:             no
    Blocking factor:        (default)
    Max blocking factor:    (default)
    UUID:                   9aa59b5c-1b34-1032-9c3e-aad50196aa4f
    Attachment 1:
        Host:               storabck18
        Raw device:         /dev/scsi/sequential/c2t500104F000D14F89d0

storabck18_tape_2:
    Device type:            tape
    Model:                  HP      Ultrium 5-SCSI
    Serial number:          HU1327WEYJ
    In service:             yes
    Automount:              yes
    Position interval:      [undetermined]
    Debug mode:             no
    Blocking factor:        (default)
    Max blocking factor:    (default)
    UUID:                   9aa59f4e-1b34-1032-9c3e-aad50196aa4f
    Attachment 1:
        Host:               storabck18
        Raw device:         /dev/scsi/sequential/c2t500104F000D14F8Cd0
ob>
```

Configuring Partitioned Libraries

To configure Oracle Storagetek partitioned library, obtain WWPN (HBA port number) in the Partitions Summary details page of the console.

To configure partitioned libraries

:

1. Install Oracle Secure Backup on the media server and add the Media Server role:

   ```
   chhost --addrole mediaserver <media server>
   ```

2. Use the `fcinfo` command to identify the WWPN of the HBA initiator port that is online:

   ```
   sudo /bin/csh
   fcinfo hba-port
   ```

   Locate the `HBA Port WWN` that is in `State: online` and note it for using in zoning and partition configuration.

3. Configure the zoning of the Oracle Secure Backup Solaris host and the libraries on your switch:

a. Login into your switch:

```
ssh admin@<switch_hostname>
```

b. Create an alias for the Media Server host using the WWPNs and verify by viewing the alias.

```
alicreate storabck68,"21:00:00:24:ff:8d:0b:be;21:00:00:24:ff:8d:0b:bf"
alishow storabck68
```

c. Create a zone that pairs the Media Server host with the library and verify by viewing the zone:

```
zonecreate STORABCK68-
TEST,"storabck68;storabcktape08_dte1_partition1;storabcktape08_dte2_part
ition1;SL500-robot-stape08"
zoneshow STORABCK68-TEST


zone:  STORABCK68-TEST
                storabck68-test; storabcktape08_dte1_partition1;
                storabcktape08_dte2_partition1; SL500-robot-stape08
```

d. Save the configuration:

```
cfgsave
```

If you are configuring for traffic isolation zones, run the `cfgenable` command for the changes to take effect.

A confirmation message displays:

```
Do you want to save the Defined zoning configuration only?  (yes, y,
no, n):
    [no] y
Updating flash ...
```

Enter `yes` to confirm the changes.

e. Enable the new fabric configuration.

```
cfgadd OSB_TEST_1,STORABCK68-TEST
```

Enter `yes` to confirm the changes.

```
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes.
Do you want to enable 'OSB_TEST_1' configuration  (yes, y, no, n): [no]
y
zone config "OSB_TEST_1" is in effect
Updating flash ...
```

4. Configure partitioned libraries with FC-SCSI connections by adding an FC-SCSI host connection in SLConsole
   a. Navigate to **Tools**, then **Partitions**, and **Summary**.
   b. Select the partition and click **Add Connection**.
   c. Enter the Initiator (WWPN) and LUN (`default: LUN 0`)
   d. Click **OK**.

   Each partition can have up to nine host connections, and each host can connect to multiple partitions. To get the right WWN's for hosts, look for the port that is `State: online` on the HBA.
5. Prepare Solaris Media Server for newly configured devices by logging back in the media server and clean up the system.
6. Follow the steps 4 through the end in Configuring Devices on Solaris Media Servers for newly configured devices.

Manually creating devices using `mkdev` in Solaris

In Oracle Secure Backup 12.1 and later, `obtool discoverdev` is the preferred method for configuring devices on Solaris systems. However, in some cases it may be necessary to create devices manually using `obtool mkdev`. This section explains how to run `mkdev` on Solaris systems.

The entries created in the `/dev/scsi/changer` and `/dev/scsi/sequential` directories when you enable the Solaris sgen driver are used as Oracle Secure Backup device attachments. The link names themselves can be used as Oracle Secure Backup device attach points.

`/dev/scsi/changer/c1t0d0` translates to a library attachment in `obtool mkdev` of:

```
# obtool mkdev --attach <hostname>:/dev/scsi/changer/c1t0d0 lib
```

`/dev/scsi/sequential/c1t2d0` translates to a drive attachment in `obtool mkdev` of:

```
# obtool mkdev --attach <hostname>:/dev/scsi/sequential/c1t2d0 drv -d 1 -l lib
```

In other cases, you may prefer to create links in `/dev` that point to the attach points. For example, if you wish to create `/dev/obl<n>` or `/dev/obt<n>` links for use as attachments in Oracle Secure Backup, do the following:

```
# ln -s /dev/scsi/changer/c1t0d0 /dev/obl0 for the library (the "l" stands for
library)
```

```
# ln -s /dev/scsi/sequential/c1t2d0 /dev/obt0 for the drive (the "t" stands for
tape drive)
```

If you choose to do this, each device that Oracle Secure Backup will utilize must have its own unique name in the format `/dev/obl<n>` or `/dev/obt<n>`.

The same device configurations shown earlier would now look like this:

```
# obtool mkdev --attach <hostname>:/dev/obl0 lib
```

```
# obtool mkdev --attach <hostname>:/dev/obt0 drv -d 1 -l lib
```

Configuring Devices on AIX Media Servers

Oracle Secure Backup no longer requires that AIX attach points be pre-configured using `makedev` before obtool `discoverdev` can find and utilize them.

To configure devices on AIX:

1. Complete the steps in
2. Add the mediaserver role to the host

   ```
   ob> chhost --addrole mediaserver osblp01
   ```

3. Run `discoverdev`:

```
ob> discoverdev -ic -h osblp01
   Device-Type   Device-Model            Serial-Number        Attachpoint
   Library       STK     SL150           464970G+1333SY1401   osblp01:/dev/obl0
create device object osblp01_lib_1? (a, n, q, y, ?) [y]: y
   Tape          HP      Ultrium 5-SCSI  HU1327WEYJ           osblp01:/dev/obt0
create device object osblp01_tape_1? (a, n, q, y, ?) [y]: y
   Tape          HP      Ultrium 5-SCSI  HU1328WGF6           osblp01:/dev/obt1
create device object osblp01_tape_2? (a, n, q, y, ?) [y]: y

Checking each library to associate discovered drive(s) with DTE...
    Assigning DTE 1 in library osblp01_lib_1 for drive osblp01_tape_2 with serial
number: HU1328WGF6
    Assigning DTE 2 in library osblp01_lib_1 for drive osblp01_tape_1 with serial
number: HU1327WEYJ

ob> lsd -l
osblp01_lib_1:
    Device type:            library
    Model:                  STK     SL150
    Serial number:          464970G+1333SY1401
    In service:             no
    Debug mode:             no
    Barcode reader:         default (hardware-selected)
    Barcodes required:      no
    Auto clean:             no
    Clean interval:         (not set)
    Clean using emptiest:   no
    Ejection type:          ??
    Min writable volumes:   0
    UUID:                   eed24e34-15e2-1032-bdb8-000000000000
    Attachment 1:
        Host:               osblp01
        Raw device:         /dev/obl0

osblp01_tape_2:
    Device type:            tape
    Model:                  HP      Ultrium 5-SCSI
    Serial number:          HU1328WGF6
    In service:             no
    Library:                osblp01_lib_1
    DTE:                    1
    Automount:              yes
    Position interval:      [undetermined]
    Debug mode:             no
    Blocking factor:        (default)
    Max blocking factor:    (default)
```

```
        Current tape:           [unknown]
        Use list:               [not set]
        Drive usage:            [not set]
        Cleaning required:      [unknown]
        UUID:                   01832346-15e3-1032-bdb8-000000000000
        Attachment 1:
            Host:               osblp01
            Raw device:         /dev/obt1

    osblp01_tape_1:
        Device type:            tape
        Model:                  HP      Ultrium 5-SCSI
        Serial number:          HU1327WEYJ
        In service:             no
        Library:                osblp01_lib_1
        DTE:                    2
        Automount:              yes
        Position interval:      [undetermined]
        Debug mode:             no
        Blocking factor:        (default)
        Max blocking factor:    (default)
        Current tape:           [unknown]
        Use list:               [not set]
        Drive usage:            [not set]
        Cleaning required:      [unknown]
        UUID:                   0183170c-15e3-1032-bdb8-000000000000
        Attachment 1:
            Host:               osblp01
            Raw device:         /dev/obt0
    ob>
```

Manually Creating Devices in AIX

Preconfiguration of system device attach points is not necessary for running `discoverdev` to configure Oracle Secure Backup devices on an AIX media server. This section explains how to create and configure attach points using obtool commands.

The standalone tool `obscan` can be used to assist with gathering device information for SCSI attached or Fibre Channel tape and media changer devices in a switched environment on AIX. The SCSI ID and LUN are required to create system device attach points using makedev for use by Oracle Secure Backup. The `obscan` utility is located in the `OSB_HOME/tools` directory of the Oracle Secure Backup admin server. The syntax is as follows, where `dname` is the device file name of the SCSI bus or Fibre Channel fabric to scan:

```
# obscan -f dname

# obscan -f /dev/scsi0

# obscan -f /dev/fscsi0
```

> **Note:**
>
> Note: when creating OSB attach points using makedev you will be asked to
>
> Enter logical unit number 0-31 [0]: 0
>
> This is the number that will be associated with the attach point name makedev creates to differentiate it from other devices. Although these values are arbitrary, It is customary to start at zero and increment by one for each library or drive attachment being created.
>
> (see 3.3.5.0 Assigning Oracle Secure Backup Logical Unit Numbers to Devices)

In the following steps, `obscan` gathers information needed by `makedev` to create Oracle Secure Backup system attachments for devices attached to the Fibre Channel fabric identified by `/dev/fscsi1`:

1. Login to the system as a `root` user.
2. Run obscan to identify the SCSI ID & LUN for the tape drives and media changers attached to the system:

```
./obscan -f /dev/fscsi1
 obscan version 18.1.0.0.0 (AIX)

 DEVICE information for /dev/fscsi1

 Connection Type = 2, Switch

    Target-id : 658982, Lun : 0
       Vendor   : HP          Product  : Ultrium 6-SCSI  Device type : Tape  World
Wide Name : 500104F000CC6412

    Target-id : 658983, Lun : 0
       Vendor   : HP          Product  : Ultrium 5-SCSI  Device type : Tape  World
Wide Name : 500104F000CC640F

    Target-id : 658983, Lun : 1
       Vendor   : STK         Product  : SL150           Device type : Library
World Wide Name : 500104F000CC640F

    Target-id : 659008, Lun : 0
       Vendor   : HP          Product  : Ultrium 5-SCSI  Device type : Tape World
Wide Name : 500104F000D14F8C

    Target-id : 659009, Lun : 0
       Vendor   : HP          Product  : Ultrium 5-SCSI  Device type : Tape World
Wide Name : 500104F000D14F89

    Target-id : 659009, Lun : 1
       Vendor   : STK         Product  : SL150           Device type : Library World
Wide Name : 500104F000D14F89
Total count of Media Changers and/or Tape devices found : 6
```

3. To reconfigure all devices, remove all existing Oracle Secure Backup system attach points using `rm /dev/ob*`. If you wish to add devices while retaining the existing attach points, check to see which `/dev/ob*` attach points are present and then proceed to specify Oracle Secure Backup logical unit numbers that are not already in use.

Here is an example of running `makedev` to create new Oracle Secure Backup system attach points where none exist already:

```
# install/makedev
Enter logical unit number 0-31 [0]: 0
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable  tape
library [d]: l
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [3]: 658983
Enter SCSI logical unit number (lun) 0-7 [0]: 1
/dev/obl0 created

# install/makedev
Enter logical unit number 0-31 [0]: 1
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
    tape library [d]: l
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [2]: 659009
Enter SCSI logical unit number (lun) 0-7 [0]: 1
/dev/obl1 created

# install/makedev
Enter logical unit number 0-31 [0]: 0
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
    tape library [d]: d
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [4]: 658983
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obt0 created

# install/makedev
Enter logical unit number 0-31 [0]: 1
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable  tape
library [d]: d
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [5]: 658982
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obt1 created

# install/makedev
Enter logical unit number 0-31 [0]: 2
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable  tape
library [d]: d
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [3]: 659008
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obt2 created

# install/makedev
Enter logical unit number 0-31 [0]: 3
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable  tape
library [d]: d
Enter SCSI bus name [scsi0]: fscsi1
Enter SCSI target id 0-16777215 [2]: 659009
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obt3 created

# ls /dev/ob*
/dev/obl0  /dev/obl1  /dev/obt0  /dev/obt1  /dev/obt2  /dev/obt3

# obtool
Oracle Secure Backup 18.1.0.0.0
```

```
Warning: auto-login failed - login token has expired
login: admin
Password:
ob> lsh
osblp01          admin,mediaserver,client          (via OB)    in service
ob> lsd
ob> mkdev -t lib -a osblp01:/dev/obl1 lib
ob> mkdev -t tape -a osblp01:/dev/obt2 -d 1 -l lib drv1
ob> mkdev -t tape -a osblp01:/dev/obt3 -d 2 -l lib drv2

ob> mkdev -t lib -a osblp01:/dev/obl0 lib1
ob> mkdev -t tape -a osblp01:/dev/obt0 -d 1 -l lib1 drva
ob> mkdev -t tape -a osblp01:/dev/obt1 -d 2 -l lib1 drvb
ob>
```

Identifying and Configuring AIX Devices in a Point-to-Point or FC-AL Configuration

In a point-to-point or FC-AL configuration, no tool is provided to help you determine the SCSI ID and LUN . However, for IBM-supported devices in these configurations, you can use the `lsattr` command.

To identify and configure AIX devices with lsattr and makedev:

1. Log on as `root`.

   You must have operating system privileges to access devices, which is often root access, to run `lsattr`.

2. Run `lsattr` for each SCSI and Fibre Channel adapter with tape devices to be used by Oracle Secure Backup.

   The following `lsattr` example displays the attribute names, current values, descriptions, and user-settable flag values for the `rmt0` device:

```
user: lsattr -El rmt0
block_size     512                Block size (0=variable length)           True
delay          45                 Set delay after a FAILED command         True
density_set_1  0                  DENSITY setting #1                       True
density_set_2  0                  DENSITY setting #2                       True
extfm          yes                Use EXTENDED file marks                  True
location                          Location Label                           True
lun_id         0x1000000000000    Logical Unit Number ID                  False
mode           yes                Use DEVICE BUFFERS during writes         True
node_name      0x1000006045175222 FC Node Name                            False
res_support    no                 RESERVE/RELEASE support                  True
ret_error      no                 RETURN error on tape change or reset     True
rwtimeout      144                Set timeout for the READ or WRITE commandTrue
scsi_id        0x2                SCSI ID                                 False
var_block_size 0                  BLOCK SIZE for variable length support   True
ww_name        0x2001006045175222 FC World Wide Name                      False
```

   You can convert the hexadecimal values of `lun_id` and `scsi_id` (shown in bold) to decimal so that they are usable by the Oracle Secure Backup `makdev` command. After conversion, the SCSI LUN ID is 281474976710656 and the SCSI ID is 2.

3. Navigate to the `install` directory in your Oracle Secure Backup home. For example:

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

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

```
# makedev
```

5. At the prompts, enter the information required to create attach points used within Oracle Secure Backup to identify devices for backup and restore operations.

   The `makedev` script creates the attach point, displaying messages indicating its progress.

Configuring Devices on HP-UX Media Servers

To access SCSI or Fibre Channel tape devices on HP-UX using the `makedev` script, Oracle Secure Backup requires the following identifying information about how the devices are attached to their hosts:

- SCSI bus number instance
- Target ID
- LUN

To gather device information in HP-UX, you can use the `ioscan` utility located in `/usr/sbin` on the HP-UX operating system. The `ioscan` command searches the system and lists any devices that it finds. You must have root access to run `ioscan`.

> **Note:**
>
> The `ioscan` tool, which may be included as part of the HP-UX operating system, is an optional tool for device identification.

To identify and configure HP-UX devices:

1. Log on as `root`.
2. Execute the following command:

   ```
   /usr/sbin/ioscan -f
   ```

   Running the command with the `-f` option displays full information about the system configuration including device class, instance number, device or interface driver, software state, and hardware type.

   Example 4-1 shows sample output for `ioscan -f`. The bus number instance, target ID, SCSI LUN, and device description for each device are shown in bold.
3. Using the `ioscan` output, make a note of the bus number, target ID, and SCSI LUN for the tape devices.

   Table 4-4 shows the relevant information from Example 4-1.

Table 4-4 Information Required by makedev

Device	Type	Name	Bus Number Instance	Target ID	SCSI LUN
Tape library (autoch)	SCSI	ADIC FastStor 2	3	1	0
Tape drive (tape)	SCSI	HP Ultrium 2	3	2	0
Tape library (autoch)	FC	ADIC Scalar 24	9	3	0
Tape drive (tape)	FC	IBM ULTRIUM-TD3	9	3	1

Table 4-4 (Cont.) Information Required by makedev

Device	Type	Name	Bus Number Instance	Target ID	SCSI LUN
Tape drive (tape)	FC	IBM ULTRIUM-TD3	9	3	2

4. Use `makedev` to create attach points so that Oracle Secure Backup can identify devices for backup and restore operations.

   The following example runs `makedev` using the information in Table 4-4. The example creates the attach point `/dev/obl/8` for the ADIC FastStor 2 library on SCSI bus instance 3 with the target ID 1 and SCSI LUN 0.

```
% makedev
Enter logical unit number 0-31 [0]: 8
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
    tape library [d]: l
Enter SCSI bus instance: 3
Enter SCSI target id 0-16777215: 1
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obl/8 created
```

   The following example runs `makedev` using the information in Table 4-4. The example creates the attach point `/dev/obt/9m` for the HP Ultrium 2 tape drive on SCSI bus instance 3 with the target ID 2 and SCSI LUN 0.

```
% makedev
Enter logical unit number 0-31 [0]: 9
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
    tape library [d]: d
Enter SCSI bus instance: 3
Enter SCSI target id 0-16777215: 2
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obt/9m created
```

Example 4-1 ioscan -f

```
$ /usr/sbin/ioscan -f

Class      I  H/W Path                Driver   S/W State  H/W Type   Description
...
ext_bus    3  0/1/1/1                 mpt      CLAIMED    INTERFACE  SCSI Ultra320
target    11  0/1/1/1.1               tgt      CLAIMED    DEVICE
autoch     4  0/1/1/1.1.0             schgr    CLAIMED    DEVICE     ADIC FastStor 2
target    10  0/1/1/1.2               tgt      CLAIMED    DEVICE
tape       8  0/1/1/1.2.0             stape    CLAIMED    DEVICE     HP  Ultrium 2-SCSI
...
fcp        2  0/2/1/0.99              fcp      CLAIMED    INTERFACE  FCP Domain
ext_bus    9  0/2/1/0.99.15.255.1     fcpdev   CLAIMED    INTERFACE  FCP Device Interface
target     1  0/2/1/0.99.15.255.1.3   tgt      CLAIMED    DEVICE
autoch     8  0/2/1/0.99.15.255.1.3.0 schgr    CLAIMED    DEVICE     ADIC Scalar 24
tape      19  0/2/1/0.99.15.255.1.3.1 stape    CLAIMED    DEVICE     IBM ULTRIUM-TD3
tape      20  0/2/1/0.99.15.255.1.3.2 stape    CLAIMED    DEVICE     IBM ULTRIUM-TD3
```

Assigning Oracle Secure Backup Logical Unit Numbers to Devices

Each tape drive and tape library must be assigned an Oracle Secure Backup LUN during the configuration process. This number is used to generate unique device names during device configuration. Oracle Secure Backup logical unit numbers are assigned as needed automatically on Windows. For each UNIX or Linux media server, however, you must select Oracle Secure Backup logical unit numbers for each device as part of planning your administrative domain.

There is no required order for assigning Oracle Secure Backup logical unit numbers. They are typically assigned sequentially, starting at 0, for each tape device of a given type, whether tape library or tape drive. That is, tape 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 UNIX, the resulting device special file names for tape libraries are `/dev/obl1`, `/dev/obl2`, `/dev/obl3` and so on, and the names for tape drives are `/dev/obt1`, `/dev/obt2`, `/dev/obt3` and so on. On Windows, the resulting tape library names are `//./obl1`, `//./obl2`, `//./obl3` 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.

> **See Also:**
>
> "Configuring Devices on Linux Media Servers"

> **Note:**
>
> The Oracle Secure Backup logical unit number should not be confused with the SCSI LUN. The latter is part of the hardware address of the tape device, while the Oracle Secure Backup logical unit number is part of the device special filename.

Additional Information for Installation of Oracle Secure Backup on Linux

For each Linux media server, ensure that the SCSI Generic (SG) driver is installed. This driver is required for Oracle Secure Backup to interact with a tape device.

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 start time.

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

> **Note:**
>
> The `rc.modules` file is necessary, and not `rc.local`, because `rc.modules` runs earlier in the start process.

On RedHat Enterprise Linux, you can use the following commands to add the `sg` module to the list of modules configured to load as `root` at start time:

```
# echo modprobe sg >> /etc/rc.modules
# chmod +x /etc/rc.modules
```

An Oracle Secure Backup user must be mapped to a Linux or UNIX user that has read/write permissions to the `/dev/sg` devices. One way to accomplish this goal is to set the permissions to `666` for the `/dev/sg` devices.

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 a tape device. The host must also be configured to automatically reload the driver after a restart.

Installing Oracle Secure Backup on AIX

The steps for installing and uninstalling Oracle Secure Backup on AIX is similar to a Linux or UNIX host.

To successfully install Oracle Secure Backup on AIX, ensure that the Input/Output Completion Port (IOCP) is configured on your system. To configure IOCP, complete the steps explained in Configuring IOCP on AIX Systems.

You can install Oracle Secure Backup 18.1 and earlier versions on AIX hosts up to version 7.1. If you are installing Oracle Secure Backup from a C shell and the installation stops responding, then do a `/bin/sh` before running the setup. If the installation still does not respond, then run this command:

```
/net/myfiler/export/vol0/home/osb_media_dir/OSB-OS-package/setup --securepath
```

During Oracle Secure Backup installation, the Oracle Secure Backup `admin` user is mapped by default to UNIX user `root` and UNIX group `root`. In this configuration, Oracle Secure Backup requires that the user `root` be a member of the group `root` to back up the file system successfully. AIX does not define a group `root` by default. If the group `root` does not exist on your AIX system, then you must create it and make user `root` a member of it.

> **Note:**
>
> You can change this mapping of the Oracle Secure Backup `admin` after installation.

> **See Also:**
>
> - "Interactive Installation on Linux or UNIX" and "Uninstalling Oracle Secure Backup on Linux or UNIX"
> - "Configuring Devices on AIX Media Servers"

Configuring IOCP on AIX Systems

It is mandatory to enable IOCP on your AIX systems to be able to perform Oracle Secure Backup operations successfully.

To configure IOCP:

1. Run the `lslpp` command to ensure that IOCP module was installed on your system during the database install.

   ```
   $ lslpp -l bos.iocp.rte
   ```

   The output should look similar to this:

   ```
   Fileset                      Level     State       Description
   ----------------------------------------------------------------------------
   Path: /usr/lib/objrepos
     bos.iocp.rte               5.3.9.0   APPLIED     I/O Completion Ports API

   Path: /etc/objrepos
     bos.iocp.rte               5.3.0.50  COMMITTED   I/O Completion Ports API
   ```

2. Run the `lsdev` command to check the status of the IOCP port.

   ```
   $ lsdev -Cc iocp
   ```

   The required IOCP port status is `Available`.

   If the IOCP port status is `Defined`, change this to `Available` by completing the following steps:

   a. Log on as `root`.

   b. Run the following command:

      ```
      # smitty iocp
      ```

   c. Select **Change/Show characteristics of the I/O Completion Ports**.

   d. Change the configured state from `Defined` to `Available`.

   e. Restart the system for this change to reflect.

5

Installing Oracle Secure Backup on Windows

Follow these steps to learn how to install Oracle Secure Backup on hosts that run the Windows operating system.

This chapter contains these sections:

- Prerequisites for Installing on Windows
- Options for Installing on Windows
- Interactive Installation on Windows
- Noninteractive or Unattended Installation on Windows
- Configuring Firewalls for Oracle Secure Backup on Windows

Prerequisites for Installing on Windows

Before starting Oracle Secure Backup installation on Windows, check the following prerequisites.

- Complete the planning tasks described in Preparing to Install Oracle Secure Backup.
- While installing Oracle Secure Backup on a host, if you want to use the host as a media server, then physically attach each tape library and tape drive to the host. Restart the system if required.
- Before adding Oracle Secure Backup tape libraries and drives to an administrative domain, disable or stop any system software that scans and opens arbitrary SCSI targets (for example, tape library monitoring software).
- For installing the administrative server or media server role, verify the physical and network requirements for the host as discussed in Choosing Secure Hosts for the Administrative and Media Servers.
- Oracle Secure Backup requires NDMP port 10000 for installing on your host. If this port is not available on your host, for example other applications are using this port, then the installation cannot complete successfully. Therefore, Oracle Secure Backup provides an option to manually specify the NDMP Port for installation.

  For more information, see Table 5-1.

Obtain the Oracle Secure Backup installation media and store it in a directory that all hosts can access. You can download the installation media from Oracle Technology Network (OTN) and extract the contents of the archive file.

> **See Also:**
>
> Acquiring Oracle Secure Backup Installation Media

Options for Installing on Windows

For installing Oracle Secure Backup on Windows, you can use the following parameters.

Table 5-1 Installation Parameters for Windows

Parameter	Description	Required for Unattended Installation
`ADD_HOST_INITIATOR_VALUE="myhostname.com"`	Specifies the adding host ID.	Yes, if `ADD_HOST_INITIATOR_ENABLE` is not specified
`INSTALL_ROLE="Client"`	Disables user prompts for advanced settings and automatically selects the client host role.	Yes
`ADD_HOST_INITIATOR_ENABLE="No"`	Disables administrative host identification check while adding a client to the administrative domain.	Yes, if `ADD_HOST_INITIATOR_VALUE` is not specified
`NDMP_PORT="12345"`	Specifies the port used by Oracle Secure Backup for NDMP communication.	Yes, if the default port 10000 is not available
`DISABLE_WEB_TOOL="Yes"`	Installs only the Oracle Secure Backup administrative server with the web server disabled.	No

Interactive Installation on Windows

Follow these steps to perform an interactive installation of Oracle Secure Backup on Windows.

1. Log in to your host as an administrator user.
2. Go to the directory where the installation software is stored and run the `setup.exe` program to open Oracle Secure Backup setup wizard.

   > **Note:**
   >
   > To install Oracle Secure Backup on an alternate NDMP Port if the default port 10000 is not available, run the setup wizard with an additional option `NDMP_PORT`.
   >
   > `setup.exe NDMP_PORT="12345"`

   On this host, if you have uninstalled Oracle Secure Backup earlier or if this is a fresh installation, then the Clean Install window appears. Click **Next** to continue.

   Along with the install options, you can also use the following buttons in the setup wizard:

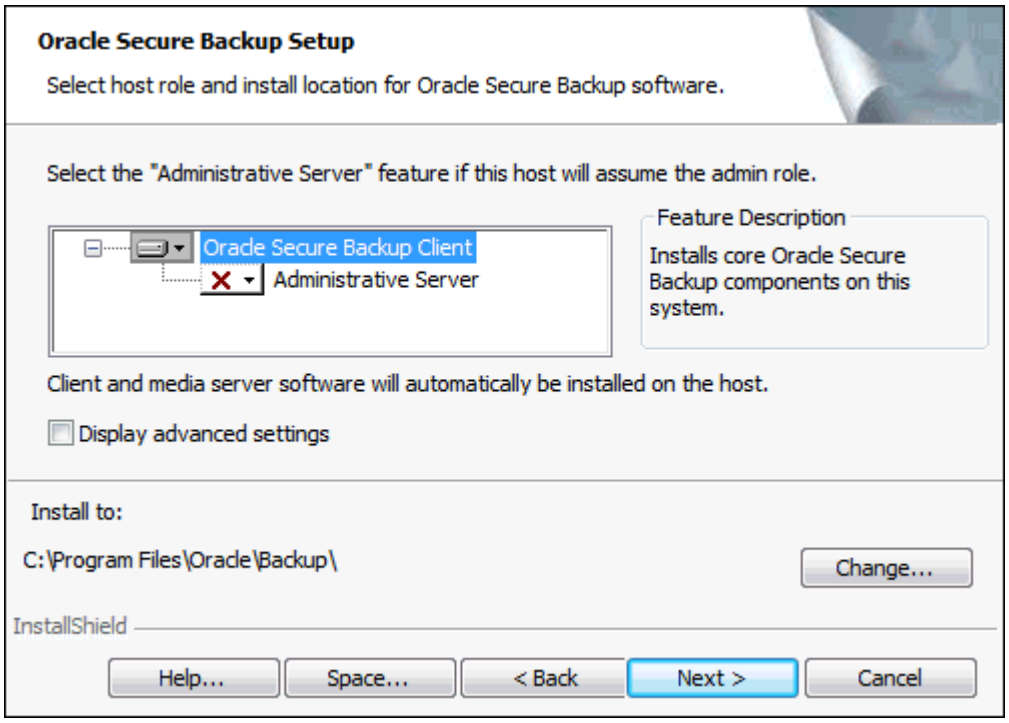
   - **Help**: to view detailed description for installation
   - **Space**: to check disk space for installation
3. Specify user information as follows:

- **User Name**: Enter a user name
- **Organization**: Enter the name of your company
- Select who can use Oracle Secure Backup on this host.
  - **Anyone who uses this computer**: Provides access to all users
  - **Only for me**: Restricts using Oracle Secure Backup only to you

Click **Next** to continue.

4. Select the host role as displayed in Figure 5-1.

Figure 5-1 Oracle Secure Backup Setup Window



You can select from the following:

- **Administrator Server**: Click the **Administrative Server** option and install. For more information, see Installing Administrative Server on Windows
- **Client role**: Leave the defaults and click next. For more information, see Installing Client Role on Windows

> **Note:**
>
> Installation of Oracle Secure Backup on Windows also includes the client and media server packages.
>
> By default, a Windows host assumes the client role unless you specifically select the administrative role.

A single host can have multiple roles, which are additive rather than exclusive.

5. Verify that Oracle Secure Backup installs in the default directory, `C:\Program Files\Oracle\Backup`. If you want to select a different directory for the installation, then click **Change** and specify the location.

   Click **Next** to continue. The setup wizard displays the Ready to Install the Program window.

6. Click **Install** to start the Oracle Secure Backup installation.

   The setup wizard displays a confirmation message that the installation is complete. Click **Finish** to close the setup wizard.

The installation generates a log file, namely `osb_install.log`, and stores it in the Windows temporary directory.

If you have enabled Windows Installer logging, then the installation also creates an additional Windows log in the same directory. For more information, see Enabling Installer Logging on Windows.

Similarly, you can install Oracle Secure Backup in unattended mode on your Windows host. For more information, see Noninteractive or Unattended Installation on Windows.

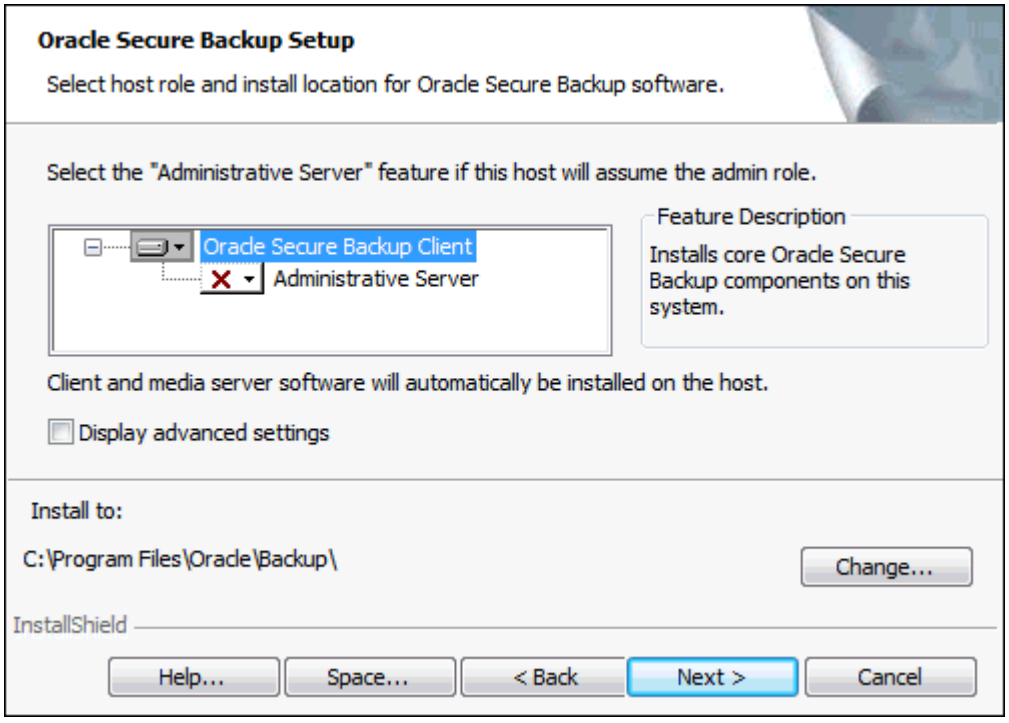
> **Note:**
>
> For installing in an Oracle Real Application Clusters (Oracle RAC) environment, install Oracle Secure Backup on each node in the cluster.

Installing Administrative Server on Windows

While running the Oracle Secure Backup setup wizard on a Windows host, you can install the administrative server .

1. Select the host role as displayed in Figure 5-1.

Figure 5-2 Oracle Secure Backup Setup Window



Under Oracle Secure Backup Client, select **Administrative Server** then select **This feature will be installed on local hard drive**.

> **Note:**
>
> By default, a Windows host assumes the client role unless you specifically select the administrative role.

2. Select whether you want to customize configuration parameters for the installation.
   - To configure the parameters, select **Display advanced settings**.

     > **See Also:**
     >
     > Overview of Customizing Configuration Parameters During Installation to know the configuration parameters that you can modify
     >
     > Configuring Advanced Settings for Windows to understand how to modify the configuration parameters

   - Leave the advanced settings options if you want to use the default values for configuration parameters.

   Click **Next** to continue.
3. Create a password for the Oracle Secure Backup Encryption Wallet. Enter the password in the given fields.

> **Important:**
>
> Ensure to note the Encryption Wallet password and keep it safe. In case of a failure, you require this password to recover your administrative server.

Click **Next** to continue. Oracle Secure Backup stores the password in the Cloud Wallet.

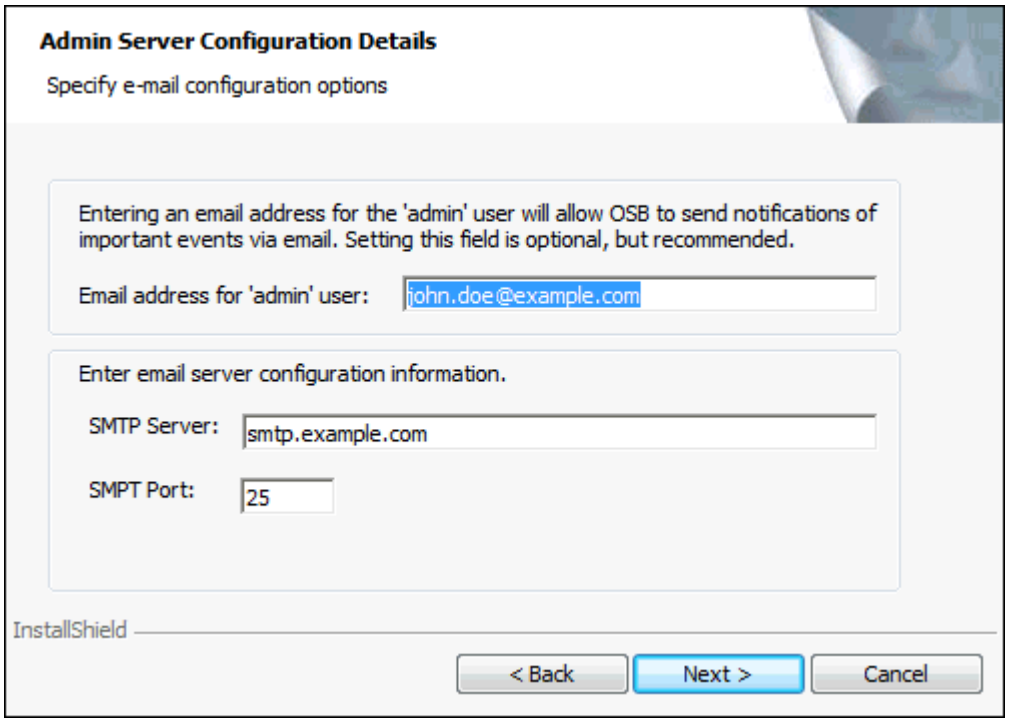
4. Create a password for the Oracle Secure Backup administrative server. Enter the password in the given fields and click **Next** to continue.

   For both, Encryption Wallet password and administrative server password, Oracle recommends that you select a password of minimum eight characters with a combination of alphabetic and numeric values. You can also customize the minimum length of the password as a part of Configuring Advanced Settings for Windows.

5. On the Admin Server Configuration Details window, you can enter configuration information for your email server.

   These fields are optional. If you do not want to specify these, then leave them blank and click **Next** to continue.

Figure 5-3 Admin Server Configuration Details Page



- **Email address for admin user**: Specify an email address, if you want to receive notifications about jobs, operations, status, and so on from the administrative server. Leave this blank if you do not want to receive notifications.
- **SMTP Server**: Enter details of your email server
- **SMTP Port**: Enter the TCP/IP port number of your email server

> **Note:**
>
> By default, Oracle Secure Backup sends email notifications from *SYSTEM@FQDN* address, where FQDN is the Fully Qualified Domain Name of the administrative server. You can change the default sender while configuring the installation parameters. For more information, see Oracle Secure Backup Reference.

6. In the Web Server Account Details Window, enter the credentials for your Apache Web user account.

> **Note:**
>
> Failure to log in to your Apache Web server account displays an error message and stops the Oracle Secure Backup installation.
>
> If you do not want to use your Web server account or do not have a Web server account, then use the Local System Account credentials for the installation.

   - Enter your Windows user account in the format `domain\user`. This user can run the Apache daemon.
   - Create a password for the Apache Web user account. Enter the password in the given fields.

Now, continue the installation of Oracle Secure Backup on your Windows host.

When you install the Oracle Secure Backup administrative server, it also installs the web server. However, while installing the administrative server Oracle Secure Backup provides an option to disable the web server using the following command:

```
msiexec /i "Oracle Secure Backup.msi" /qn /L*V "msi_install.log"
DISABLE_WEB_TOOL="Yes"
```

Installing Client Role on Windows

While running the Oracle Secure Backup setup wizard on a Windows host, you can install the client or media server role.

1. Select the host role as displayed in Figure 5-1.

> **Note:**
>
> By default, a Windows host assumes the client role unless you specifically select the administrative role.

2. Select whether you want to customize configuration parameters for the installation.
   - To configure the parameters, select **Display advanced settings**. You can specify configuration parameters in the Client Advanced Settings window.

> **See Also:**
>
> Overview of Customizing Configuration Parameters During Installation to know the configuration parameters that you can modify
>
> Configuring Advanced Settings for Windows to understand how to modify the configuration parameters

- Leave the advanced settings options if you want to use the default values for configuration parameters.

Click **Next** to continue. The setup wizard displays the Adding Host Initiator Name window.

3. Enter the host ID of the administrative server that adds the client to its domain.

   You can enter either the Fully Qualified Domain Name (FQDN) or the IP address of the administrative server. Specifying the IP address avoids connectivity failures during problems with nameservice.

   The client stores the specified IP address or FQDN in `C:\Program Files\Oracle\Backup\db\obconfig.txt` file. This information is essential for authentication purpose and for establishing the initial connection between the client and the administrative server.

   For more information, see Configuring and Managing the Administrative Domain.

Now, continue the installation of Oracle Secure Backup on your Windows host.

Enabling Installer Logging on Windows

The Windows Installer logging helps in troubleshooting issues while installing Oracle Secure Backup.

To enable Windows Installer logging

1. Open the Windows registry with `Regedit.exe` and create the following path and keys:

   `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer`

   `Reg_SZ: Logging`

   `Value: voicewarmupx`

2. Select the required logging mode. Table 5-2 displays the letters you can enter in the value field to enable the corresponding logging options.

   These letters are not in a sequence, that is, you can enter them in any order.

Table 5-2 Windows Installer Logging Values

Value	Description
v	Verbose output
o	Out-of-disk-space messages
i	Status messages
c	Initial UI parameters
e	All error messages
w	Non-fatal warnings

Table 5-2 (Cont.) Windows Installer Logging Values

Value	Description
a	Start up of actions
r	Action-specific records
m	Out-of-memory or fatal exit information
u	User requests
p	Terminal properties
+	Append to existing file
!	Flush each line to the log
x	Extra debugging information
*	Wildcard, log all information except for the `v` and the `x` options. To include the `v` and the `x` option, specify `/l*vx`.

> **Note:**
>
> Use Windows Installer logging for troubleshooting purposes only. If you leave it running for a longer period, then it might affect the system performance and occupy more disk space.
>
> Each time you use the **Add/Remove Programs** tool in Windows Control Panel, it creates a new `Msi*.log` file.

Configuring Advanced Settings for Windows

Oracle Secure Backup provides default values for configuration parameters during installation unless you modify them and specify a different value.

While running the setup wizard on Windows, you can use the **Display advanced settings** option to view and modify the configuration parameters. Depending on the host role, whether it is an administrative server or a client, the setup wizard displays the Admin Host Advanced Settings or Client Host Advanced Settings window respectively.

You can modify the following parameters for both administrative server and client role.

- **Temporary directory**: Specify the location to store transient files used while performing various operations. For more information, see Oracle Secure Backup Temporary Directory.
- **Start Oracle Secure Backup Services automatically**: Select this option to automatically start all services after the system restarts.

Configuration Parameters for Administrative Server

You can modify the following parameters in the Admin Host Advanced Settings, that is, only for an administrative server.

- **Minimum User Password Length**: Specify the minimum length for Oracle Secure Backup user passwords. For more information, see Length of Oracle Secure Backup User Passwords.
- **Security Certificate Keysize**: Specify the key size for identity certificates. For more information, see Identity Key Certificate Length.

Using Oracle Secure Backup with RMAN
To perform Oracle Database backup and restore operations with Recovery Manager (RMAN), Oracle Secure Backup requires a preauthorized Oracle Secure Backup user on the administrative server. This preauthorized user with the rights of the `oracle` class can perform backup and restore operations with RMAN.

1. In the Admin Host Advanced Settings window, select the **Create "oracle" user** option to create the preauthorized user.

   The setup wizard automatically generates a password for the `oracle` user. Generally, you do not change this password because you do not log in to Oracle Secure Backup as the `oracle` user.

2. In the Preauthorized User Details window, enter the account information for the preauthorized user.

   By default, the setup wizard provides the name `oracle` for the preauthorized user, which you can modify. You can perform backup of Oracle Database on both Linux or UNIX and on Windows client.

   To backup a database on a Linux or UNIX client, enter the following:

   - **Preauthorized user account**: The user name on Linux or UNIX associated with the preauthorized user.
   - **Preauthorized Group**: Name of the group on Linux or UNIX associated with the preauthorized user.

   To backup a database on a Windows client, in the **Preauthorized Account** field, enter the domain user account associated with the preauthorized user.

> **Note:**
>
> - Create the `oracle` user only for using Oracle Secure Backup with RMAN.
> - To perform unprivileged backup operations on Windows clients using RMAN, you must modify the Oracle Secure Backup `admin` and `oracle` users and assign Windows credentials (a domain, user name, and password) to them. This is applicable to any platform that acts as the administrative server.
> - Creating an `oracle` user provides convenience but can also affect the security.

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

Noninteractive or Unattended Installation on Windows

Oracle Secure Backup supports noninteractive or unattended installation of client role on a Windows host.

You can perform unattended installation of Oracle Secure Backup client host role on Windows from the command-line interface (CLI).

For unattended installation of client role on Windows:

1. Log in to your host as an administrator user.
2. Open a CLI window, such as Windows Command Prompt or PowerShell, and go to the directory where the software package is stored.
3. For unattended installation of client role, run the installer with an additional parameter, `INSTALL_ROLE="Client"`.

   The `INSTALL_ROLE="Client"` parameter automatically selects the client host role. Using this parameter, the installer proceeds with the installation without displaying any prompts for advanced settings.

   Moreover, you have additional options for unattended installation.

   - **With adding host ID**: to specify an adding host ID, for example `myhost.oracle.com`

     ```
     msiexec /i "Oracle Secure Backup.msi" /qn /L*V "C:\msi_install.log"
     INSTALL_ROLE="Client" ADD_HOST_INITIATOR_VALUE="myhostname.com"
     ```

   - **Without adding host ID**: to disable the secure registration feature and install Oracle Secure Backup without specifying an adding host ID

     ```
     msiexec /i "Oracle Secure Backup.msi" /qn /L*V "msi_install.log"
     INSTALL_ROLE="Client" ADD_HOST_INITIATOR_ENABLE="No"
     ```

   - **Specify NDMP Port**: to use another NDMP Port for installation, if the default port 10000 is not available

     ```
     msiexec /i "Oracle Secure Backup.msi" /qn /L*V "msi_install.log"
     INSTALL_ROLE="Client" ADD_HOST_INITIATOR_ENABLE="No" NDMP_PORT="12345"
     ```

The setup wizard completes the installation and displays a confirmation message: `Oracle Secure Backup was installed.`

Configuring Firewalls for Oracle Secure Backup on Windows

Windows contains a built-in Windows Firewall which, in the default configuration, blocks inbound traffic on ports used by Oracle Secure Backup.

If your Windows host is protected by a firewall, then 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 port 400, port 10000, and other dynamically assigned ports.

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.

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, the built-in firewall released with Windows. Review the script to determine whether it is suitable for your environment. You can run the script after the installation completes.

Local Policy for tcpkeepalive

As Oracle Secure Backup performs a backup, several network connections are opened across the nodes in the Oracle Secure Backup domain. For large backups, some of these connections

may be idle for a long time. Your firewall or other network devices may be configured to terminate idle connections after a specific time. If a backup exceeds this time, the firewall terminates the idle connections, resulting in a failed backup.

The firewall terminates a connection in the following scenarios:

- The firewall is configured to terminate network connections which are idle for a specified time, for example, 7200 seconds or 2 hours.
- Oracle Secure Backup is performing large backups, which takes longer than the firewall setting for terminating connections.

Enable the local policy for `tcpkeepalive` to maintain the network connections and prevent idle socket timeouts, which causes failure of the backup jobs.

> **See Also:**
>
> See "Enable tcpkeepalive on local host" for more information about how to enable `tcpkeepalive` for network connections.

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.

> **See Also:**
>
> My Oracle Support note `727528.1` for more information on how to configure firewall ports for use with Oracle Secure Backup. My Oracle Support is available at `http://support.oracle.com/`.

6
Uninstalling Oracle Secure Backup

This chapter explains how to uninstall Oracle Secure Backup software from Linux, UNIX, and Windows hosts.

This chapter contains the following sections:

- Uninstalling Oracle Secure Backup on Linux or UNIX
- Uninstalling Oracle Secure Backup on Windows

Uninstalling Oracle Secure Backup on Linux or UNIX

This section explains how to uninstall Oracle Secure Backup from a Linux or UNIX host. In this procedure 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. Change directory to the Oracle Secure Backup home directory.

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

   > **Note:**
   >
   > If you uninstall Oracle Secure Backup from the administrative server, then the `uninstallob` script removes the Oracle Secure Backup home directory at the end of the uninstall process.

3. Run the `uninstallob` script:

   ```
   # ./install/uninstallob
   ```

4. If the host on which Oracle Secure Backup is being uninstalled was configured as a client, then the `uninstallob` script asks you the following question:

   ```
   Do you want to remove this system's identity as a member of the administrative
   domain? (y or n) [n]? :
   ```

   Select one of the following options:

   - `y`

     Select this option to remove the system's identity as a member of the administrative domain.

   - `n`

     Select this option to keep the system's identity as a member of the administrative domain. This is the default option.

   The `uninstallob` script continues with Step 6.

5. If the host from which Oracle Secure Backup is being uninstalled was configured as an administrative server, the `uninstallob` script asks to save the Oracle Secure Backup `admin` directory. Select one of these options:

   - `no`

     Select this option to remove the admin directory.

   - `yes`

     Select this option to save the admin directory. If you keep the admin directory, then you can reinstall the Oracle Secure Backup software later without destroying your administrative domain.

   This procedure assumes you are saving the Oracle Secure Backup `admin` directory.

6. The `uninstallob` scripts asks if you want to continue. Enter **y** to continue with the uninstallation. Enter **n** to stop the uninstall process.

   If you choose **y**, then a message is displayed informing you that the uninstall was completed successfully.

Uninstalling Oracle Secure Backup on Windows

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

1. Select **Start** > **All Programs** > **Oracle Secure Backup** > **Uninstall Oracle Secure Backup**.

   A confirmation dialog appears.

2. Click **Yes** to remove Oracle Secure Backup from your computer.

3. An additional window opens asking whether you want to preserve the files specific to your backup domain. Select one of these options:

   - Click **Delete** if you do not want to retain the backup domain files.
   - Click **Keep** to retain the backup domain files.

     If you click **Keep** to retain the backup domain files, then the configuration of your backup domain is preserved. This is useful for reinstallation of the Oracle Secure Backup software later.

Oracle Secure Backup is now uninstalled from your host.

7

Configuring and Managing the Administrative Domain

This chapter explains the basic steps involved in setting up an Oracle Secure Backup administrative domain after initial installation of the product on all of your hosts. Some steps, such as "Adding a Host to the Administrative Domain", are also useful when managing an existing administrative domain.

This chapter contains the following sections:

Overview of Configuring the Administrative Domain

The administrative domain consists of a set of hosts and backup containers that are managed as a single unit by Oracle Secure Backup. The administrative domain enables you to manage backup and restore operations among diverse hosts, devices, and databases.

After you install the Oracle Secure Backup software on all the hosts, except NDMP hosts and NAS filers, in the administrative domain, you must configure the administrative domain. Configuring the administrative domain sets up the environment that is required to create and manage backups.

The instructions in this chapter describe how to configure the administrative domain with host and backup container information using the Web tool. It is assumed that you have installed the Oracle Secure Backup software on each host in the domain, as described in Installing Oracle Secure Backup on Linux or UNIX or Installing Oracle Secure Backup on Windows.

> **See Also:**
>
> *Oracle Secure Backup Reference* for information about the obtool commands used to configure the administrative domain

The administrative domain is set up using a default security configuration that should be adequate for most users. Further configuration of users, user classes, security options, and the

Oracle Secure Backup media management layer for use with Recovery Manager (RMAN) in backing up Oracle databases might be required in some cases.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for information about additional security configuration

Network Load Balancing in Oracle Secure Backup

Network load balancing ensures that multiple network connections on a client are utilized optimally and no single connection carries the data load of all the concurrent backup and restore jobs. The transfer load of multiple backup and restore jobs is distributed across the network connections available on the client and media server. Load balancing is available starting with Oracle Secure Backup 10.4 and is supported for both file-system and Oracle Database backup and restore operations. Load balancing is turned off by default.

> **Note:**
>
> Load balancing is not supported for NDMP clients.

Oracle Secure Backup sets up a data connection between the client and the media server over which the data transfer occurs. If a host contains more than one network interface of a particular type, Oracle Secure Backup uses all the available interfaces of that type for the data connections between the client and the media server. The type of network interface can be IPv4, IPv6, or RDS/RDMA (Reliable Datagram Socket over Remote Direct Memory Access) over Infiniband. Load balancing requires connectivity between the client and the media server on all the interfaces of the selected connection type.

Oracle Secure Backup selects a connection type only if both the client and the media server support that connection type. Therefore, if both the client and the media server support RDS/RDMA over Infiniband and the IPv6 connection types, then Oracle Secure Backup selects RDS/RDMA over Infiniband as the connection type.

If a Preferred Network Interface (PNI) is configured, then load balancing is disabled on the media server and PNI takes precedence. Load balancing will still be performed on the client.

Order of Precedence for Network Connection Types

When multiple network connections are available between a client and media server, Oracle Secure Backup decides which connection type to use based on the following order of precedence:

- RDS/RDMA over Infiniband
- IPv6
- IPv4 (includes TCP/IP over Infiniband)

Steps to Configure the Administrative Domain

1. Configure all the hosts in your administrative domain. Hosts include the administrative server, media servers, and clients.

   While configuring a host, specify the role that is assigned to the host in the administrative domain.

   > **See Also:**
   >
   > "Steps to Configure Hosts in the Administrative Domain" for information about configuring hosts

2. Add the tape devices in your network to the administrative domain. Tape devices include tape libraries and tape devices.

   You can automatically discover tape devices that are attached to media servers in the administrative domain or manually configure each tape device.

   > **See Also:**
   >
   > - "Overview of Automatic Device Discovery" for information about discovering tape devices
   > - "Adding Tape Devices to an Administrative Domain" for information about adding tape devices

3. Verify the configuration of tape devices that were added to the administrative domain.

   > **See Also:**
   >
   > "Verifying and Configuring Added Tape Devices" for information about verifying tape devices

4. Configure disk pools in your administrative domain.

   > **See Also:**
   >
   > "Configuring Disk Pools" for information about configuring disk pools

The initial configuration of your administrative domain is complete.

Network communication among hosts in the administrative domain is configured with the default security configuration described in "Default Security Configuration".

> **Note:**
>
> You must still identify files to be backed up in a dataset, configure at least one backup schedule, and set up users, classes, and security policies. These tasks are described in the *Oracle Secure Backup Administrator's Guide*.

Configuring the Administrative Domain with Hosts

After installing Oracle Secure Backup, configure the administrative domain with client hosts.

You can add hosts to your administrative domain either during the initial administrative domain configuration or when you subsequently define new hosts in your domain.

After the initial configuration, you can manage your hosts and perform tasks such as editing host properties, updating hosts, and removing hosts from the administrative domain.

This section contains these topics:

About Administrative Domain Host Configuration

The host configuration process makes the administrative server aware of a media server or client to be included in the administrative domain. You must perform this process for every host in the administrative domain, including each host running Oracle Secure Backup natively and each network-attached storage device managed by Network Data Management Protocol (NDMP).

For any host to be added to the administrative domain, you must provide the following attributes:

- Host name
- IP address
- Assigned roles: client, media server or both
- Whether the host is in service or not in service at the moment

After adding a host to the administrative domain, Oracle recommends that you ping the host to confirm that it can be accessed by the administrative server.

> **See Also:**
>
> "Pinging Hosts in the Administrative Domain"

For hosts that use NDMP access mode, such as network-attached storage devices, you must configure the following additional attributes:

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

> **See Also:**
>
> *Oracle Secure Backup Reference* for a complete account of host attributes

Steps to Configure Hosts in the Administrative Domain

After you install the Oracle Secure Backup software on hosts, use the steps in this section to configure the administrative domain with hosts.

To configure your hosts in the administrative domain:

1. Open the Oracle Secure Backup Web tool running on the administrative server and log in as the `admin` user.

   > **See Also:**
   >
   > "Starting a Web Tool Session" for information about accessing the Web tool

2. For each host in your administrative domain that must be set up for the role of media server, perform the following steps:

   a. Add the host to the administrative domain by selecting the media server role for the host as described in "Adding a Host to the Administrative Domain".

      > **Note:**
      >
      > If the administrative server is also assigned the media server role, then it is part of the administrative domain. See "Adding the Media Server Role to an Administrative Server" for information about assigning the media server role to the administrative server.

   b. Configure the administrative domain to include each tape device attached to this host as described in "Adding Tape Devices to an Administrative Domain" describes this task.

c. Configure the administrative domain to include disk pools as described in "Configuring Disk Pools".

3. (Optional) For certain NDMP hosts, you may need to define backup and restore environment variables before the host can function with Oracle Secure Backup.

> **See Also:**
>
> "Adding Backup and Restore Environment Variables to an NDMP Host" for information about defining backup and restore environment variables for NDMP hosts

4. (Optional) For hosts that have multiple physical data paths with the administrative server or media server, you can define a Preferred Network Interface (PNI) that will be used while exchanging backup or restore data with another host.

> **See Also:**
>
> "Configuring Preferred Network Interfaces (PNI)" for information about defining a PNI for your host

5. For each host that is to be set up only for the client role, add the host to the administrative domain by selecting the client role as described in "Adding a Host to the Administrative Domain".
6. Verify that all the hosts that you added to your administrative domain are accessible using the IP address that was configured for the host.

> **See Also:**
>
> "Pinging Hosts in the Administrative Domain" for information about pinging hosts

After you complete the initial configuration of the hosts, you can manage hosts by performing tasks such as editing host properties, updating hosts, and removing hosts from the administrative domain as described in "Managing Hosts in the Administrative Domain".

Adding a Host to the Administrative Domain

You can add a host (media server or client) to the administrative domain either at the time of initial domain configuration or subsequently, when you want to configure additional hosts in your administrative domain.

To add a host to an administrative domain:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Click **Hosts** in the Basic section to display the Hosts page.
3. Click **Add** to add a host.

   The Configure: Hosts > New Hosts page appears.
4. In the **Host** field, enter the unique name of the host in the Oracle Secure Backup administrative domain.

In most cases, this name is the host name resolvable to an IP address using the host name resolution system (such as DNS or NIS) on your network. However, you can assign a different host name purely for use with Oracle Secure Backup.

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

5. You must enter a value in the **IP Interface name(s)** field in the following situations:
   - The name of this host cannot be resolved to an IP address using a mechanism such as DNS or NIS
   - The resolvable name of your host is different from the value entered in the **Host** field.
   - Your host has multiple IP interface names or IP addresses to use with Oracle Secure Backup

   If any of the preceding conditions apply to this host, then enter one or more IP interface names in this field. Valid values are either resolvable host names or IP addresses. Separate multiple values with a comma.

   For example, you can use `myhost.oracle.com` for a host name or `141.146.8.66` for an IP address.

   If a value is specified for this field, then Oracle Secure Backup tries the host names or IP addresses in the order specified when it must contact this host, rather than using the name specified in the **Host** field.

   > **Note:**
   >
   > If some hosts should contact this host using a particular network interface, then you can use the Preferred Network Interface (PNI) capability to override this order for those hosts, after completing the initial configuration of the administrative domain. See "Configuring Preferred Network Interfaces (PNI)" for details.

6. In the **Status** list, select one of these:
   - **in service**

     Select this option to indicate that the host is available to perform backup and restore operations.
   - **not in service**

     Select this option to indicate that the host is unavailable to perform backup and restore operations.
7. In the **Roles** list, select the roles for this host: **admin**, **client** or **mediaserver**.
8. In the **Encryption** field, specify the encryption settings for backup operations performed for this host. Select one of the following values:
   - required
   - allowed

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for information about the encryption settings

9. In the **Algorithm** field, select one of the following options to specify the algorithm that must be used to encrypt backups created for this host: aes128, aes192, or aes256.
10. In the **Access method** field, select one of these:
    - **OB**

      Select this option for Windows, Linux and UNIX hosts that have Oracle Secure Backup installed.
    - **NDMP**

      Select this option for devices that support NDMP without an Oracle Secure Backup installation, such as a network-attached storage device.

> **Note:**
>
> OB access mode is a synonym for primary access mode. See "Oracle Secure Backup Host Access Modes" for a discussion of access modes.

11. In the Disable RDS field, select one of the following:
    - **yes**

      Select this option to disable the use of Reliable Datagram Socket (RDS) over Infiniband for communication between the client and media server. The default protocol, TCP/IP, is used for communication.
    - **no**

      Select this option to enable the use of Reliable Datagram Socket (RDS) over Infiniband for communication between the client and media server.
    - **systemdefault**

      Select this option to specify that the administrative domain level setting, by using the operations policy `disablerds`, is used to decide of RDS is enabled for the host. For example, if you set `systemdefault` at the host level and the `disablerds` policy is set to `no`, the host uses RDS for data transfer.

> **See Also:**
>
> Oracle Secure Backup and Reliable Datagram Socket (RDS) for more information about RDS

12. In **Public and private key sizes**, select the size for the public/private key associated with the identity certificate for this host.

    For hosts using the **ob** access mode, skip to Step 20. For hosts such as Network Attached Storage (NAS) devices that must use **NDMP** mode, continue to Step 13. Steps 13 through 18 apply only to hosts in NDMP mode.

13. In the **NDMP authorization type** list, select an authorization type. The authorization type defines the way Oracle Secure Backup authenticates itself to the NDMP server. Typically, you should use the default setting.

    Your choices are the following:

    - **default**

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

    - **none**

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

    - **negotiated**

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

    - **text**

      Select this option to use unencrypted text to authenticate.

    - **md5**

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

    > **See Also:**
    >
    > *Oracle Secure Backup Administrator's Guide* to learn about NDMP-related policies

14. In the **Username** field, enter the name used to authenticate Oracle Secure Backup to this NDMP server. If left blank, then Oracle Secure Backup uses the name in the NDMP policy.
15. In the **Password** list, select one of these options:

    - **Use default password**

      Select this option to use the default NDMP password.

    - **Use text password**

      Select this option to enter a password.

    - **Set to NULL**

      Check this to use a NULL password.

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

    > **Note:**
    >
    > The practice of supplying a password in clear text on a command line or in a command script is not recommended by Oracle. It is a security vulnerability. The recommended procedure is to have the user be prompted for the password.

16. In the **Backup type** field, enter an NDMP backup type. A backup type is the name of a backup method supported by the NDMP data service running on a host. Backup types are defined by each data service provider.

17. In the **Protocol Version** list, select **2**, **3**, **4**, or **as proposed by server**. See "Oracle Secure Backup Host Access Modes" for details on NDMP protocol versions.
18. In the **Port** field, enter a port number. Typically, the TCP port (10000) in the NDMP policy is used. You can specify another port if this server uses a port other than the default.
19. If required, add backup and restore environment variables as described in "Adding Backup and Restore Environment Variables to an NDMP Host".
20. In the **TCP/IP buffer size** field, enter the value of the buffer size in bytes.
21. If the host you are adding to the administrative domain is not currently accessible on the network, then select the **Suppress communication with host** option.
22. Click **OK** to save your changes.

Adding the Media Server Role to an Administrative Server

If you choose both the administrative server and media server roles when installing Oracle Secure Backup on a host, then that host is automatically part of the administrative domain. But it is not recognized as a media server until that role is explicitly granted to it using the `chhost` command in `obtool` or the Oracle Secure Backup Web tool.

> **See Also:**
>
> *Oracle Secure Backup Reference* for complete syntax and semantics for the `chhost` command

To add the media server role to an administrative server using the Oracle Secure Backup Web tool:

1. On the Configure page of the Oracle Secure Backup Web tool, click **Hosts**.

   The Configure: Hosts page appears.
2. Select the administrative server and click **Edit**.

   The Configure: Hosts > *host_name* page appears.
3. In the Roles list, shift-click to add the media server role and then click **OK**.

   The Configure: Hosts page reappears with the media server role added to the administrative server host under the Roles column.

Adding Backup and Restore Environment Variables to an NDMP Host

Some NDMP hosts might require that you add backup and restore environment variables before they function with Oracle Secure Backup.

To add backup and restore environment variables:

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

   If an environment variable name or value includes spaces, then you must use quotes around the name or value to ensure correct processing of the name or value. For example, enter **A=B** or **"Name A"="Value B"** (if the name or value includes spaces).

3. Select an existing environment variable pair and click **Remove** to remove the pair.

Configuring Preferred Network Interfaces (PNI)

This section contains the following topics:

> **Note:**
>
> PNI configuration settings for a host are applicable only to Oracle Secure Backup services. These settings have no impact on the network selection or usage of other applications running on the same host.

About PNI

PNI (Preferred Network Interface) enables you to configure the network or interface that must be used for communication between two hosts in the administrative domain.

Multiple physical data paths can exist between a client, which contains primary storage to be backed up or restored, a media server, which controls at least one secondary storage device that writes and reads the backup media, and the administrative server. For example, a host might have multiple network interfaces connected to the network containing the hosts in the administrative domain. Typically, clients transfer huge amounts of backup data over the network. Therefore, specifying the network/interface over which data must be sent prevents performance issues that may be caused when production networks are used for backup data.

For each host, you can configure PNI to instruct Oracle Secure Backup services to use a specific network or interface for sending backup data or for requesting a remote Oracle Secure Backup service to send inbound data. PNI applies to both control connections and data connections. Data connections are used to transfer backup data. Backup data is large in size and consumes considerable network bandwidth. Control connections are used to manage the administrative domain. The messages sent over control connections are small and consume minimal bandwidth.

> **See Also:**
>
> Network Load Balancing in Oracle Secure Backup for information about network load balancing and PNI

About PNI for Inbound Connections

Configuring a PNI for inbound connections specifies the interface that will be used when a remote host (media server or client) establishes a connection with the host.

See Also:

- Configuring PNI for Inbound Connections
- Removing a PNI for Inbound Connections

About PNI for Outbound Connections

Configuring a PNI for outbound connections from a host specifies the network and interface that must be used when this host connects to a remote host (media server or client). The configured PNI is used for both data and control connections.

You can create one of the following to specify a PNI for outbound connections:

- Single interface only

  Limits the outgoing backup and control data transfer to the interface specified in the configured PNI. The interface must exist in the remote host to which a connection is being established. You can configure one network/interface for each address family (one for IPv4 and another for IPv6). You must not use the single interface for RDS connections. When you chose this type of connection, you cannot configure other networks as PNI for outbound connections for this host.

- One or more specified networks

  Uses the specified network when connecting to a remote host. You can specify one or more networks. Optionally, a bind address for each outgoing network can be specified. If no bind address is specified, then the operating system decides which address to bind to. When multiple networks are specified, a connection is attempted based on the order of remote host IP names specified.

  If the specified networks are not available, then you can configure Oracle Secure Backup to use any available network and interface to connect to a remote host. The following IP values are used to configure any network as PNI:

  0.0.0.0/0: any IPv4 network

  0::0/0: any IPv6 network

  0/0: any of IPv4 or IPv6 network

See Also:

- Configuring PNI for Outbound Connections
- Removing a PNI for Outbound Connections

PNI and Network Connection Types

A host can have different types of networks. Oracle Secure Backup supports IPv4 and IPv6 for control connections and IPv4, IPv6, RDS/RDMA over Infiniband for data connections. When multiple network connections exist between a client and the media server, Oracle Secure Backup uses the following criteria to determine which connection type is used:

- If a PNI is configured, the network interface specified in the PNI is used to transfer backup and restore data between the client and media server. The connection type chosen is the same as the connection type of the network interface specified in PNI.
- If a PNI is not configured, Oracle Secure Backup selects the connection type as follows:
  - For control connections, the order of precedence is based on the ordering of IP addresses in the host object. Each client has a host object. The host object contains the list of IP addresses that can be used to access that host.
  - For data connections, the default connection used depends on the type of connection. The order of precedence is described in "Order of Precedence for Network Connection Types".

    For a particular connection type to be used, both the client and media server must support that connection type.

Configuring PNI for Inbound Connections

When you configure a PNI for inbound connections for a host, remote hosts specified in inbound PNI use the interface specified in PNI to send data to the host.

To configure a PNI for inbound connections:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the host for which you want to configure a PNI and click **Edit**.

   The Configure Hosts > *host_name* page appears.
3. Click **Preferred Network Interfaces**.

   The Configure Hosts > *host_name* > Preferred Network Interface page appears.

   Ensure that **Inbound** is selected in the list at the top-right of the page. This is the default selection.
4. Select an IP address or DNS name from the **Interface** list.

   This list shows a list of interfaces using which this host can be referenced. The IP address or name is used by the remote host to connect to this host.
5. From the Clients list, select one or more clients that will use this IP address or DNS name when creating a connection to this host.
6. Click **Add**.

Configuring PNI for Outbound Connections

When multiple network paths exist between hosts in the administrative domain, you can configure a PNI to define the network/interface that must be used when creating connections from this host to another remote host.

To configure a PNI for outbound connections from a host:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the host for which you want to configure a PNI and click **Edit**.

   The Configure Hosts > *host_name* page appears.
3. Click **Preferred Network Interfaces**.

   The Configure Hosts > *host_name* > Preferred Network Interface page appears.
4. From the list at the top-right of the page, select **Outbound**.

The Outbound Interfaces section is displayed.

5. Depending on the type of outbound connection that you want to configure as the PNI, perform one of the following steps:
   a. To configure a single interface for all outbound connections:
      i. Select **useonly**.
      ii. In the Interface column corresponding to the useonly option, select the interface that must be used as the PNI.

      > **Note:**
      >
      > Once you configure a useonly interface, you cannot configure other networks as PNI for this host.

   b. To configure a specified network for outbound connections:
      i. Select **network**.
      ii. In the Network column corresponding to the Network option, specify the network that must be used as the PNI.
      iii. (Optional) In the Interface column, corresponding to the Network option selected, select the bind address that must be used.
   c. To configure any network for outbound connections:
      i. Select **network**.
      ii. In the Network column corresponding to the Network option, specify one of the following in the network:

      0.0.0.0/0: any IPv4 network

      0::0/0: any IPv6 network

      0/0: any of IPv4 or IPv6 network
6. Click **Add** to add the details provided as a PNI for outbound connections.

   The specified details are added and displayed at the top the page.
7. (Optional) If you did not configure a useonly interface, configure another network as PNI by clicking **Add**and performing the steps listed in Step 5.

Removing a PNI for Inbound Connections

To remove a PNI for inbound connections:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the host for which you want to remove a PNI and click **Edit**.

   The Configure Hosts > *host_name* page appears.
3. Click **Preferred Network Interfaces**.

   The Configure Hosts > *host_name* > Preferred Network Interface page appears.
4. Under Inbound Interfaces, click **Select** corresponding to the interface and client that you want to remove as a PNI configuration.
5. Click **Remove**.

Removing a PNI for Outbound Connections

To remove a PNI configuration for outbound connections from a host:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the host for which you want to remove a PNI and click **Edit**.

   The Configure Hosts > *host_name* page appears.
3. Click **Preferred Network Interfaces**.

   The Configure Hosts > *host_name* > Preferred Network Interface page appears.
4. Select **Outbound** at the top-right of the page.

   The list of configured PNIs for outbound connections is displayed.
5. In the **Outbound Interfaces** section, click **Select** corresponding to the PNI configuration that you want to remove.
6. Click **Remove**.

Pinging Hosts in the Administrative Domain

You can use the Oracle Secure Backup ping operation to determine whether a host responds to requests from Oracle Secure Backup on each of its configured IP addresses.

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

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

To ping a host in the administrative domain:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. From the Hosts page, select a host to ping.
3. Click **Ping**.

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

Enable tcpkeepalive on local host

Enable `tcpkeepalive` in the local policy to prevent idle Oracle Secure Backup network connections from being terminated by a proxy or firewall due to inactivity.

You can set the local policy for `tcpkeepalive` and configure the control connections to remain open so that the backup operations, for both file system and Recovery Manager (RMAN), complete successfully.

About tcpkeeplive

Oracle Secure Backup provides a local policy for `tcpkeepalive`.

The `tcpkeepalive` policy helps maintain idle TCP connections by periodically exchanging packets between hosts in the Oracle Secure Backup domain that have the local policy enabled. By default, Oracle Secure Backup has the `tcpkeepalive` policy disabled.

However, you can change the local policy and enable `tcpkeepalive` from the obtool interface. Since `tcpkeepalive` is set on the local host, you must enable it individually on all media servers and administrative servers in the administrative domain.

To enable the `tcpkeepalive` policy:

- Run the `obtool` commands for `tcpkeepalive` on the local host.
- Configure the system parameters depending on your operating system.

The Web tool does not support changing or viewing the local policies.

> **See Also:**
>
> Configuring Firewalls for Oracle Secure Backup on Windows for information about the role of Windows firewall on network connections.

Steps to enable tcpkeepalive

Log in to the `obtool` command-line interface and enable `tcpkeepalive` in the local policy.

Here are the `obtool` commands to view the local policies and to enable `tcpkeepalive`.

To enable tcpkeepalive:

1. Open a terminal window and enter into the `obtool` command-line interface.

   ```
   obtool
   ```

   See "obtool Login" for more details on how to log in to `obtool`.
2. View all defaults and policies in the administrative domain.

   ```
   lsp
   ```

   See "lsp" for more details on the `lsp` command.
3. View the policies local to the host.

   ```
   lsp local
   ```

   Observe that the default setting for `tcpkeepalive` is no.
4. Change the local policy on your host and enable the setting for `tcpkeepalive`.

   ```
   setp local/tcpkeepalive yes
   ```
5. Optionally, run the `lsp local` command once again and view the new setting for `tcpkeepalive`.

   ```
   lsp local
   ```

   Verify that you have enabled `tcpkeepalive` on the local host.

   ```
   tcpkeepalive                    yes
   ```

The system parameters to set the timers associated with `tcpkeepalive` vary for each operating system. After a restart, the system parameters may reset to their default values.

> **Tip:**
>
> Consult with your system administrators or network administrators to define the system parameters and control the behavior of the connection timeouts.

Configure Character Encoding (Windows)

Character encoding actively translates human-readable characters, including those in foreign languages, into binary code for internal processing and representation by Oracle Secure Backup software.

This policy determines the character encoding used by Oracle Secure Backup internally to represent file names and directory paths on the current Windows host. It's important to note that this policy only applies to Windows hosts and has no effect on non-Windows systems. For new Oracle Secure Backup installations on Windows, the default encoding is `utf8`. Upgraded Oracle Secure Backup installations on non-English Windows systems will keep their existing encoding, which is referred to as `legacy` in this context. To view the current character encoding setting, you can run the following command:

```
ob> lsp local/charencoding
charencoding utf8 [default]
```

The valid values for this policy are `utf8` or `legacy`. The values can be changed using the following command:

```
ob> setp local/charencoding utf8
```

Overview of Automatic Device Discovery

Oracle Secure Backup allows you to discover and configure libraries and tape drives that are attached to media servers in the administrative domain.

If you choose not to discover devices automatically, then you can manually configure attached tape devices as described in "Adding Tape Devices to an Administrative Domain".

About Automatic Device Discovery

You can automatically discover and then configure libraries and tape drives that are attached to media servers in the administrative domain. This includes NDMP servers and media servers that have Oracle Secure Backup software installed. Automated device discovery makes the process of configuring attached libraries and drives automatic so that you can quickly add attached tape drives to the administrative domain. Its options allow you to configure all attached libraries and drives, or devices attached to specific hosts.

In addition to the initial configuration, automatic device discovery can also detect changes in the configuration of libraries and tape drives. When automatic device discovery is performed for a media server that has existing tape devices configured, devices that have already been configured in Oracle Secure Backup will not be reconfigured. This information can be used to

update the configuration information of existing tape devices. By default, Oracle Secure Backup discovers Solaris, Linux, and AIX attached libraries and tape devices that have their attachments located in the `/dev` directory.

> **Note:**
>
> It is recommended that you use the automatic device discovery feature to rediscover devices only when the existing devices in the current domain are not in use.

Tape Device Configuration Changes Oracle Secure Backup Detects

During automatic device discovery, the following media changers and tape drives can be detected:

- Media changers and tape drives that were not previously part of the current administrative domain.

  For each such device discovered, Oracle Secure Backup can create a device with an internally-assigned name and then configure its device attachment.
- Previously configured libraries and/or tape devices that have new attachments.

  In this case, Oracle Secure Backup can add new attachments to an existing device configuration.

  Libraries and tape devices are detected by Oracle Secure Backup by reading the serial number reported for the device by the media server's operating system. Devices having multiple attachments are detected based on their having the same serial number reported by multiple media servers. Oracle Secure Backup will configure devices based on the serial number associated with its attachments rather than any logical name assigned by the operating system.
- Previously configured devices which have lost an attachment

  Oracle Secure Backup displays information about the lost device attachment.

About Persistent Binding for SCSI Tape Devices

Oracle Secure Backup uses device file names, such as `/dev/sg3`, to refer to the actual physical tape devices. These device file names are specified during device configuration as part of the attach point specification. Hardware configuration changes or a system reboot may sometimes cause an existing device file name to point to a different tape device instead of the originally-configured tape device. To ensure that SCSI tape device configuration remains constant across hardware configuration changes and system reboots, the system administrator can use persistent binding to set up the tape devices. When persistent binding is used, the operating system uses symbolic links to manage the mapping of device files to the configured SCSI tape devices. Therefore, Oracle Secure Backup device files will always map to the correct tape devices. Tape devices that use persistent binding can also be automatically discovered and configured as described in "Overview of Automatic Device Discovery".

> **Note:**
>
> Persistent binding is supported only for the Linux 64-bit platform.

By default, Oracle Secure Backup discovers Solaris, Linux, and AIX attached libraries and tape drives that have their attachments located in the `/dev` directory. However, when persistent binding is used, the tape device files may be located in a different directory. You can specify the directory from which SCSI persistent devices must be discovered by using the `OB_DEVICE_SEARCH_PATH` environment variable.

> **See Also:**
>
> `discoverdev` in the *Oracle Secure Backup Reference* for information about the `OB_DEVICE_SEARCH_PATH` environment variable

Steps to Discover and Configure Tape Devices in the Administrative Domain

Depending on the requirement, you can either discover tape devices attached to media servers in the administrative domain or you can also configure the discovered devices.

> **See Also:**
>
> `discovereddevicestate` policy in the *Oracle Secure Backup Reference* for more information on the policy setting for managing the availability of discovered tape devices

To automatically discover and configure tape devices:

1. Open the Oracle Secure Backup Web tool running on the administrative server and log in as the `admin` user.

   > **See Also:**
   >
   > "Starting a Web Tool Session" for information about accessing the Web tool

2. Click the **Configure** tab.

   The Configure page is displayed.

3. Click **Discover Devices**.

   The Configure: Device Discovery > Discover page appears.

4. In the **Media Servers** field, select one of the following options:

   - **Specific type**

     Discover all tape devices or tape devices attached to hosts of a specific type. Select one of the following:

     - **All:** Discovers tape devices attached to all hosts in the administrative domain.
     - **OSB:** Discovers tape devices attached to hosts that have the Oracle Secure Backup software installed.
     - **NDMP:** Discovers tape devices attached to all NDMP devices in the administrative domain.

- **Specific host**

  Discovers tape devices attached to specific hosts. Multiple hosts can be specified by holding down the Shift key while selecting the hosts.

5. If the tape devices are being set up using SCSI persistent binding, then you must specify the path in which Oracle Secure Backup searches for device files by using the `OB_DEVICE_SEARCH_PATH` parameter.

> **See Also:**
>
> *Oracle Secure Backup Reference* for information about the `OB_DEVICE_SEARCH_PATH` parameter

6. In the **Options** field, select one of the following options:

   - **Display Discovered Devices**

     Displays information about the attached tape devices that was discovered by Oracle Secure Backup. The discovered devices are not configured in the domain.

   - **Automatically Configure Discovered Devices**

     Discovers tape devices attached to media servers and then configures them as devices in the administrative domain.

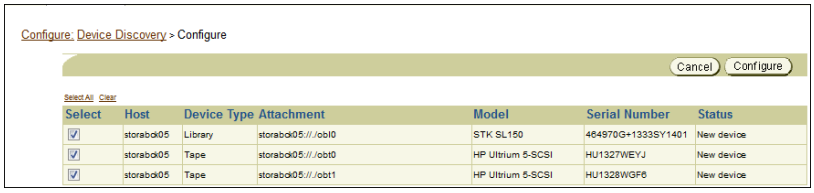
   - **Only Show Missing Devices**

     Displays information about tape devices that were previously configured but whose attachments are not discovered during the device discovery process.

7. Click **Discover**.

   If changed tape devices are discovered, then the Oracle Secure Backup Web tool displays a message similar to the following:

Figure 7-1 Device Discovery Page



Steps to Detect Missing Tape Devices

Automatic device discovery can detect tape devices that were previously configured but are now missing from the administrative domain.

To detect missing devices in the administrative domain:

1. Open the Oracle Secure Backup Web tool running on the administrative server and log in as the `admin` user.

> **See Also:**
>
> "Starting a Web Tool Session" for information about accessing the Web tool

2. Click the **Configure** tab.

   The Configure page is displayed.

3. Click **Discover Devices**.

   The Configure: Device Discovery > Discover page appears.

4. In the **Media Servers** field, select one of the following options:

   - **Specific type**

     Discovers all tape devices or tape devices attached to hosts of a specific type. Select one of the following:

     – **All:** Discovers tape devices attached to all hosts in the administrative domain.

     – **OSB:** Discovers tape devices attached to hosts that have the Oracle Secure Backup software installed.

     – **NDMP:** Discovers tape devices attached to all NDMP devices in the administrative domain.

   - **Specific host**

     Discovers tape devices attached to the specified hosts. Multiple hosts can be specified by holding down the Shift key while selecting the hosts.

5. In the Options field, select **Only Show Missing Devices**.

6. Click **Discover**.

Adding Tape Devices to an Administrative Domain

This section explains how to configure tape drives and tape libraries for use with Oracle Secure Backup. During initial configuration of the administration domain, you must add all tape devices in your environment to the domain. Subsequently, when you add new devices to your domain, you must configure the new tape devices using the steps described in this section.

This section contains the following topics:

About Tape Device Names

A tape device can be assigned a logical name by the host operating system (such as `nrst0a`), but it also can have a worldwide name, such as `nr.WWN[2:000:0090a5:0003f7]L1.a`. On some platforms, such as a Fibre Channel tape drive or tape library connected to a Network Appliance filer, the logical name might vary at each operating system restart. Oracle Secure Backup supports such tape devices, but they must be referred to by their worldwide name, which does not change across operating system restarts.

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

The WWN is usually automatically discovered by the device discovery function in Oracle Secure Backup. However, you can enter it manually if necessary.

About Manually Configuring Tape Drives and Libraries

For both tape drives and tape libraries, you can configure the following attributes:

- The name of the tape device
- The attachment, which is the description of a physical or logical connection of a tape device to a host
- Whether the tape device is in service

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

- The tape library in which the tape drive is housed, if the tape drive is not standalone
- A storage element range that the tape device can use, if the tape drive is in a tape library

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

For tape libraries, you can configure the following additional attributes:

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

> **See Also:**
>
> *Oracle Secure Backup Reference* for a complete account of tape device attributes.

Methods of Configuring Tape Devices

You can configure a tape drive or tape library for use with Oracle Secure Backup using one of the following methods:

- Automatic discovery

  Oracle Secure Backup can automatically discover and configure each secondary storage device connected to media servers.

  > **See Also:**
  >
  > "Overview of Automatic Device Discovery"

- Manually

  A tape device connected to a media server on which Oracle Secure Backup is installed must be added to the administrative domain manually.

  > **See Also:**
  >
  > "Adding Tape Devices to an Administrative Domain"

> **Note:**
>
> You must add the media server role to a host before adding any tape devices whose attachment point references that host. Oracle Secure Backup does not do this automatically.

Steps to Configure Tape Devices in the Administrative Domain

This section provides an overview of the steps used to configure tape devices, with each step containing links to the sections that describe how to perform each device configuration task.

To configure your administrative domain to include tape devices:

1. Perform one of the following steps to add tape devices to the administrative domain:
   - Manually configure tape libraries and tape devices.
     a. Configure tape libraries locally attached to your media servers as described in "Manually Configuring Tape Libraries".
     b. Configure tape drives locally attached to your media servers as described in "Configuring Tape Drives"
     c. Create an attachment between the tape device to the host to which the tape device is connected as described in "Adding Tape Device Attachments".

        A tape device can have more than one attachment.

If your tape library is shared by multiple hosts in the administrative domain, see "Configuring Multihosted Device Objects" for details about handling shared devices.

- Use automatic device discovery to add every tape device attached to hosts as described in "Overview of Automatic Device Discovery" describes this task.

2. Configure tape devices that are network-accessible but are not locally attached.

   You must decide which media servers should control the tape devices and, for each media server, specify an attachment between the media server and the tape device. The procedure is identical to configuring a tape device attached locally to a media server.

3. Verify each device attachment as described in "Verifying Tape Device Configuration".

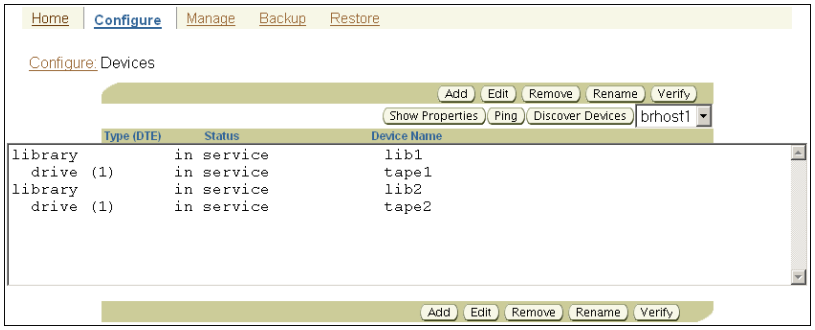
4. Inventory each tape library, and then list its volumes as described in "Updating Tape Library Inventory".

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

Displaying the Devices Page

The Devices page, illustrated in Figure 7-2, lists each tape library and tape drive that is currently in the administrative domain. The page lists the type, status, and name of every tape device.

Figure 7-2 Devices Page



To display the Devices page:

1. Open the Oracle Secure Backup Web tool running on the administrative server and log in as the `admin` user.

> **See Also:**
>
> "Starting a Web Tool Session" for information about accessing the Web tool

2. Click the **Configure** tab.
3. Click **Devices** in the Basic section.

   The Configure: Devices page appears.

Manually Configuring Tape Libraries

Automatic Device Discovery is the recommended method for configuring a tape library for use with Oracle Secure Backup. This section explains how to manually configure a tape library.

> **See Also:**
>
> "Overview of Automatic Device Discovery"

To configure a tape library:

1. Disable any system software that scans and opens arbitrary SCSI targets before adding a tape device to an administrative domain. If Oracle Secure Backup has to contend with other system software (such as monitoring software) for access to a tape library or tape drive, then unexpected behavior can result.
2. Display the Devices page as described in "Displaying the Devices Page".
3. Click **Add** to add a tape device.
4. In the **Device** field, enter a name for the tape device.

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

   The tape device name is of your choosing. It must be unique among all Oracle Secure Backup device names. It is unrelated to any other name used in your computing environment or the Oracle Secure Backup administrative domain.
5. In the **Type** list, select **library**.
6. In the **ACSLS** field, select `yes` if the tape library is an ACSLS library.
7. In the **Status** list, select one of these options:
   - **in service**

     Select this option to indicate that the tape device is available to perform Oracle Secure Backup backup and restore operations.
   - **not in service**

     Select this option to indicate that the tape device is unavailable to perform backup or restore operations.
   - **auto not in service**

     This option indicates that the tape device is unavailable to perform backup or restore operation and is set automatically for a failed operation.
8. In the **Debug mode** list, select **yes** or **no**. The default is **yes**.
9. In the **World Wide Name** field, enter a worldwide name for the tape device, if required.

> **See Also:**
>
> "About Tape Device Names" for more information on World Wide Names

10. In the **Barcode reader** list, select one of these options to indicate whether a barcode reader is present:

    - **yes**

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

    - **no**

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

    - **default**

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

11. In the **Barcode required** list, select **yes** or **no**. If you specify **yes**, then Oracle Secure Backup refuses to use any tape that lacks a readable barcode.

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

12. Set whether the tape library should use automatic cleaning.

    > **See Also:**
    >
    > "Configuring Automatic Tape Drive Cleaning for a Library"

13. In the **Unload required** list, select **yes** or **no** to specify if an unload operation is required before moving a tape from a tape drive to a storage element.

    The default value is **no**.

14. Select an **ejection type**. Your choices are:

    - `auto`

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

    - `ondemand`

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

    - `manual`

      No automation is used to eject volumes from the tape library. The backup operator determines which storage elements contain volumes ready to be ejected and manually removes them. This option can be useful when the tape library has no import/export slots.

15. Enter a value in the **Minimum writable volumes** field.

    When Oracle Secure Backup scans tape devices for volumes to be moved, it looks at this minimum writable volume threshold. If the minimum writable volume threshold is nonzero, and if the number of writable volumes in that tape library is less than this threshold, then

Oracle Secure Backup creates a media movement job for the full volumes even if their rotation policy does not require it. When this happens, Oracle Secure Backup notes in the media movement job transcript that volumes have been moved early.

16. Click **OK** to save your changes.

> **See Also:**
>
> "Adding Tape Device Attachments"

Configuring Automatic Tape Drive Cleaning for a Library

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

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

To configure automatic cleaning for a tape library:

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

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

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

2. In the **Clean using emptiest** field, select one of these options:

   - **yes**

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

   - **no**

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

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

3. Click **OK** to save your changes.

> **See Also:**
>
> "Adding Tape Device Attachments"

Configuring Tape Drives

The preferred method of configuring devices is by using automated device discovery. The following procedure describes the steps to configure tape drives manually.

This section explains how to configure a tape drive for use with Oracle Secure Backup. If the tape drive you want to configure is attached to a tape library, then you must configure the tape library first, as described in "Manually Configuring Tape Libraries".

To configure tape drives for use with Oracle Secure Backup:

1. Disable any system software that scans and opens arbitrary SCSI targets before adding a tape device to an administrative domain. If Oracle Secure Backup has to contend with other system software (such as monitoring software) for access to tape libraries and tape drives, then unexpected behavior can result.
2. Display the Devices page as described in "Displaying the Devices Page".
3. Click **Add** to add a tape device.
4. In the **Device** field, enter a name for the tape device.

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

   The tape device name is of your choosing. It must be unique among all Oracle Secure Backup device names. It is unrelated to any other name used in your computing environment or the Oracle Secure Backup administrative domain.
5. Optionally, enter the serial number of the tape drive in the **Serial Number** field.

   If you do not enter a serial number, then Oracle Secure Backup reads and stores the tape drive serial number the first time it opens the tape drive.

   The `checkserialnumbers` policy is enabled by default. If you change the tape drive hardware, then you must update the serial number of the tape drive before using it.

   > **See Also:**
   >
   > - "Editing Device Properties"
   > - *Oracle Secure Backup Reference* for more information on the `checkserialnumbers` policy
6. In the **Type** list, select **tape**.
7. In the **ACSLS** field, select `yes` if the tape library is an ACSLS library.
8. In the **Status** list, select one of these options:
   - **in service**

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

- **not in service**

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

- **auto not in service**

  This option indicates that the tape device is unavailable to perform backup or restore operation and is set automatically for a failed operation.

9. In the **Debug mode** list, select **yes** or **no**. The default is **no**.
10. Optionally, in the **World Wide Name** field, enter a worldwide name for the tape device.

> **See Also:**
>
> "About Tape Device Names" for more information on World Wide Names

11. If the tape drive is located in a tape library, then select the tape library by name from the **Library** list.
12. In the **DTE** field, enter the data transfer element (DTE) number, only if it hasn't been automatically discovered using automated device discovery.

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

13. In the **Automount** field, select **yes** (default) or **no** to specify whether automount mode is on or off. Enable the automount mode if you want Oracle Secure Backup to mount tapes for backup and restore operations without operator intervention.
14. In the **Error rate** field, enter an error rate percentage or leave this field blank to accept the default setting. The default is **8**.

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

    Oracle Secure Backup also issues a warning if it encounters a SCSI error when trying to read or reset the tape drive error counters. Some tape drives do not support the SCSI commands necessary to perform these operations. To avoid these warnings, error rate checking can be disabled by selecting **None**.
15. In the **Blocking factor** field, enter the blocking factor or leave this field blank to accept the default setting. The default is 128 bytes.

    The blocking factor value specifies how many 512-byte records to include in each block of data written to tape. The default value is 128, which means that Oracle Secure Backup writes 64K blocks to tape.

> **See Also:**
>
> "Tape Drives" for more information on blocking factors and maximum blocking factors

16. In the **Max Blocking factor** field, enter the maximum blocking factor.

    The largest value supported for the maximum blocking factor is 4096. This represents a maximum tape block size of 2MB.

    > **Note:**
    >
    > Device and operating system limitations might reduce this maximum block size.

17. In the **Drive usage since last clear** field, enter the amount of time the tape drive has been in use since it was last cleaned and then select the time unit from the adjacent list.
18. Leave the **Current tape** field empty during initial configuration. Update the tape drive inventory after configuration, as described in "Updating Tape Library Inventory".
19. Oracle Secure Backup allows all tapes to be accessed by all tape drives. The use list enables you to divide the use of the tapes for tape libraries in which you are using multiple tape drives to perform backups. For example, you might want the tapes in half the storage elements to be available to the first tape drive, and those in the second half to be available to the second tape drive.

    In the **Use list** group, select one of these options to configure the use list:

    - **Storage element range or list**

      Select this option for a numeric range of storage element addresses. Enter a range in the field, for example, **1-20**.

    - **All**

      Select this option to specify all storage elements. For tape libraries with single tape drives, you can select this option to use all tapes. This is the default setting.

    - **None**

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

20. In the **Enable Checksum** field, select one of the following options:

    - **system default**

      Uses the setting specified by the **Enable tape checksum** device policy to determine if a checksum must be computed for backup image instances stored on this tape device. This is the default setting.

    - **yes**

      Computes a checksum for the all backup image instances that are stored on this tape device. The checksum is stored as part of the backup metadata.

    - **no**

      Does not compute or store a checksum for the backup image instances that are stored on this tape device.

21. Click **OK** to save your changes.

Configuring an NDMP Copy-Enabled Virtual Tape Library

An NDMP copy-enabled virtual tape library (VTL) is a virtual tape library with an embedded NDMP server and multiple access paths. The embedded NDMP server allows offloading the

I/O associated with volume duplication from the application running on the media server to the VTL.

An NDMP copy-enabled virtual tape library (VTL) must be represented in Oracle Secure Backup as a group of tape devices with multiple attach specifications. This ensures that the inventory data coming through the multiple access paths is identical.

Two Oracle Secure Backup host objects must be created to represent the VTL. One object must be associated with the media server to which the VTL is attached. The other host object must be associated with the VTL's embedded NDMP server. Both host objects must be assigned the media server role in Oracle Secure Backup.

One Oracle Secure Backup library device object with two attach specifications must be created for the virtual library. One access path is through the media server to which the VTL is attached. The other access path is through the embedded NDMP server.

An Oracle Secure Backup tape device object with two access paths must also be created for each virtual drive contained within the virtual library. As in the virtual library case, one access path is through the media server, and the other is through the embedded NDMP server.

One Oracle Secure Backup library device object with a single attach specification must be created for the physical library. The access path is through the VTL's embedded NDMP server. An Oracle Secure Backup tape device object with a single attach specification must also be created for each physical drive contained within the physical library. As in the physical library case, the access path is through the VTL's embedded NDMP server.

> **Note:**
>
> Multiple media servers may be able to access the physical library and its drives if they are all connected to a shared SAN. In this case, the Oracle Secure Backup device objects for the physical library and its drives must be created with multiple attach points.

Here is an example of the `obtool` commands that would be used to configure an NDMP copy-enabled VTL. Many of the options that would be specified in a real environment have been omitted for clarity. Also, the device names shown are simply placeholders that may differ from the actual names in a real environment.

1. This command creates the Oracle Secure Backup host object associated with the media server to which the VTL is attached.

   ```
   mkhost --access ob --ip ipname osb_media_server
   ```

2. This command creates the Oracle Secure Backup host object associated with the embedded NDMP server contained within the VTL.

   ```
   mkhost --access ndmp --ip ipname ndmp_server
   ```

3. This command configures an Oracle Secure Backup device object that is associated with the virtual library *vlib*.

   ```
   mkdev --type library --class vtl
   --attach osb_media_server:/dev/obl0,ndmp_media_server:/dev/sg0 vlib
   ```

   This library and its drives are accessible through the Oracle Secure Backup media server and the embedded NDMP server.

4. This command configures an Oracle Secure Backup device object that is associated with virtual tape drive *vdrive1*, which is contained in the virtual library *vlib*.

   ```
   mkdev --type tape --library vlib --dte 1
   --attach osb_media_server:/dev/obt0,ndmp_media_server:/dev/nst0 vdrive1
   ```

   This command must be repeated for each tape drive in the virtual tape library.

5. This command configures an Oracle Secure Backup device object that is associated with the physical library *plib*.

   ```
   mkdev --type library --attach ndmp_media_server:/dev/sg1 plib
   ```

   This library and its drives are accessible only through the embedded NDMP server.

6. This command configures an Oracle Secure Backup device object that is associated with tape drive *pdrive1*, which is contained in the physical library *plib*.

   ```
   mkdev --type tape --library plib --dte 1
   --attach ndmp_media_server:/dev/nst1 pdrive1
   ```

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information on NDMP copy-enabled virtual tape libraries

Adding Tape Device Attachments

Oracle Secure Backup distinguishes between a tape device and a device attachment. Automated Device Discovery makes it so that it is no longer necessary to manually configure device attachments in Oracle Secure Backup. This section is added as a reference for situations where detailed understanding of the process of manually configuring device attachments in Oracle Secure Backup is needed. A device attachment is the means by which that tape device is connected to a host and Oracle Secure Backup uses this attachment as a data path to communicate with the device. Each drive or library accessed by Oracle Secure Backup has one or more attachments.

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

To configure device attachments:

1. After adding or editing a device, click **Attachments**.
2. Select a host in the **Host** list.
3. In the **Raw device** field, enter the raw device name. This is the operating system's name for the device, such as a Linux or UNIX attach point or a Windows device file. For example, a tape library name might be `/dev/obl0` on Linux and `//./obl0` on Windows.
4. Click **Add** to add the attachment.

Pinging Device Attachments

You can ping a device attachment to determine whether the tape device is accessible to Oracle Secure Backup using that attachment. Pinging device attachments is a good way to test whether you set up the attachment properly.

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

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

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

To ping an attachment from the Attachments page:

1. From the Oracle Secure Backup Web Tool Home Page, click **Configure**.
2. On the **Configure** page, under Basics, click **Devices**.
3. Select an attachment to ping.
4. Click **Ping**.

   The Oracle Secure Backup: Devices page displays the accessibility status of the attachment.
5. Click **Close** to exit the page.

Displaying Device Attachment Properties

You can display device attachment properties from the Devices page.

To display attachment properties:

1. Select the name of the tape device whose attachment properties you want to view.
2. Click **Show Properties**.

   The Oracle Secure Backup Web tool displays device attachments and other properties for the tape device you selected.
3. Click **Close** to exit the page.

Multiple Attachments for SAN-Attached Tape Devices

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

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

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

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

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

> **See Also:**
>
> The description of the `mkdev` command *`aspec`* placeholder in *Oracle Secure Backup Reference*, which describes the syntax and naming conventions for device attachments

Configuring Multihosted Device Objects

A **multihosted device**, also known as a **shared device**, is a tape library shared by multiple hosts within a single administrative domain. Shared devices are common in environments that deploy SAN or *i*SCSI-based tape equipment. These technologies give the user the flexibility to have multiple direct connections from hosts to tape devices, which enables all hosts to act as media servers.

When a device is shared by multiple hosts, a single device object is used to ensure that it is known by its serial number across all members of the Oracle Secure Backup administrative domain. The configuration is done behind the scenes using automated device discovery and multiple attachments will be created, one for each device on each media server by which the device will be accessed.

Table 7-1 shows the correct configuration of a single tape library and tape drive shared by two hosts: `host_a` and `host_b`. After the devices are configured, Oracle Secure Backup is aware of the devices and handles device reservation properly.

Table 7-1 Correct Configuration for Tape Library and Tape Drive

Tape Device Object	Attach Point 1	Attach Point 2
`SAN_library_1`	`host_a:/dev/sg1`	`host_b:/dev/sg5`
`SAN_tape_1`	`host_a:/dev/sg2`	`host_b:/dev/sg6`

If the device is configured as two separate device objects that point to the same physical device, then there is potential for contention. In this case, simultaneous backups to the these devices fail. Table 7-2 shows the *incorrect* configuration of a single tape library and tape drive shared by two hosts: `host_a` and `host_b`.

Table 7-2 Incorrect Configuration for Tape Library and Tape Drive

Tape Device Object	Attach Point
`SAN_library_1a`	`host_a:/dev/sg1`

Table 7-2 (Cont.) Incorrect Configuration for Tape Library and Tape Drive

Tape Device Object	Attach Point
SAN_library_1b	host_b:/dev/sg5
SAN_tape_1a	host_a:/dev/sg2
SAN_tape_1b	host_b:/dev/sg6

Updating Tape Library Inventory

An initial inventory of the storage element contents should be taken immediately after adding a new tape library to your Oracle Secure Backup administrative domain. This is necessary before Oracle Secure Backup will be able to use the library.

To update a tape library or tape drive inventory using the Oracle Secure Backup Web tool:

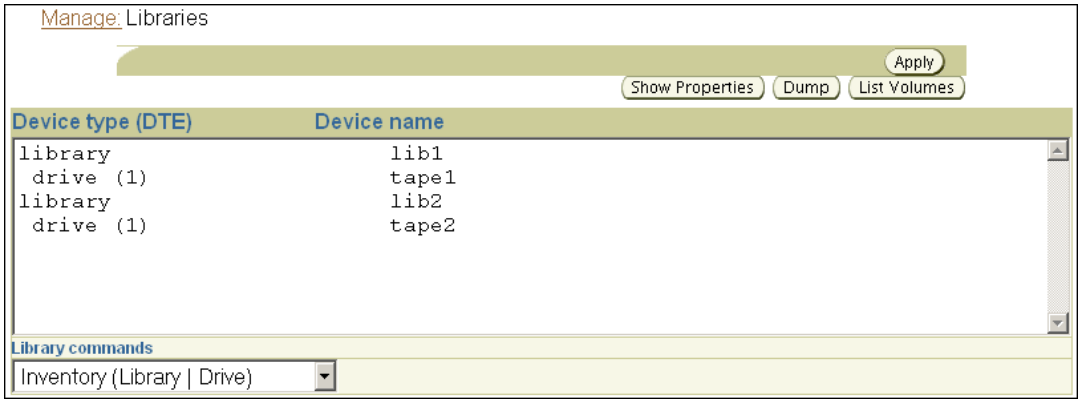
1. From the Oracle Secure Backup Web tool Home page, click **Manage**.

   The Manage page appears.

2. In the Devices section, click **Libraries**.

   The Manage: Libraries page appears as shown in Figure 7-3.

Figure 7-3 Manage: Libraries Page



3. Select the tape drive or tape library you want to inventory in the **Devices** table.
4. Select Inventory (Library | Drive) in the **Library commands** list.

   In this example, `lib1` is selected.

5. Click **Apply**.

   The Manage: Libraries page appears.

6. Ensure that the **Library** list is set to the device you want to inventory.
7. Select the **Force** option.

   Instead of reading from its cache, the tape library updates the inventory by physically scanning all tape library elements.

8. Click **OK**.

When the inventory is complete, the Manage: Libraries page reappears and displays a success message.

To see the results of the inventory, select the tape drive or tape library again and click **List Volumes**.

Verifying and Configuring Added Tape Devices

This section explains how to verify that tape devices are reachable, display information about these devices, and configure serial number checking.

This section contains the following topics:

Displaying Device Properties

The Oracle Secure Backup Web tool can display tape device properties including:

- Whether a tape device is in service
- Which host or hosts the tape device is connected to
- The tape device type

When a tape device is in service, then Oracle Secure Backup can use it; when it is not in service, then Oracle Secure Backup cannot use it. When a tape device is taken out of service, no more backups are dispatched to it.

To display tape device properties:

1. Display the Devices page as described in "Displaying the Devices Page".
2. Select the name of the tape device whose properties you want to display.
3. Click **Show Properties**.

   The Oracle Secure Backup Web tool displays a page with the properties for the tape device you selected.

Pinging Tape Devices

To determine whether a tape device is reachable by Oracle Secure Backup through any available attachment, ping the tape device. You should ping each tape device after it is configured or discovered, to check it's accessibility status.

To ping a tape device:

1. Perform the steps in "Verifying Tape Device Configuration" to ensure that the device has been configured correctly.
2. Display the Devices page as described in "Displaying the Devices Page".
3. Select a tape device to ping.

4. Click the **Ping** button.

   The Oracle Secure Backup Web tool displays the status of the operation.

> **Note:**
>
> Pinging a tape library causes each service member tape drive in the tape library to be pinged as well.

Editing Device Properties

If you make an error during installation, such as not configuring every attachment for a tape device or incorrectly configuring its properties, then you can edit its properties.

To edit the properties of an existing tape device:

1. Display the Devices page as described in "Displaying the Devices Page".
2. Select the name of the tape device.
3. Click **Edit**.

   The Oracle Secure Backup Web tool displays a page with details for the tape device you selected.
4. Make any required changes.

> **See Also:**
>
> For information about the device properties, refer to the following sections:
>
> - "Manually Configuring Tape Libraries"
> - "Configuring Tape Drives"

5. Click **OK** to save your changes.

Verifying Tape Device Configuration

Oracle Secure Backup provides the following method for confirming that libraries and tape devices are configured correctly.

To verify tape device configuration:

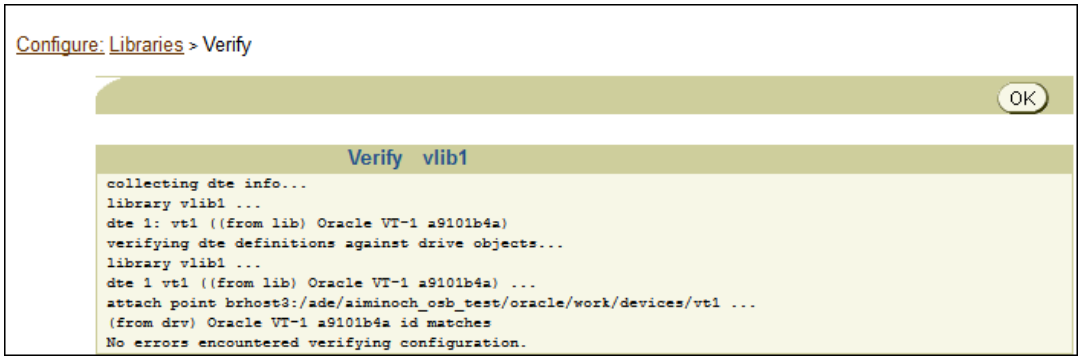
1. From the Oracle Secure Backup Web tool home page, click **Configure**.

   The Configure page appears
2. In the Basic section click **Devices**.

   The Configure Devices page appears.
3. Select the library whose configuration you want to check and click **Verify**.

   The Configure: Libraries > Verify *device_name* page appears as shown in Figure 7-4.

Figure 7-4 Configure: Libraries Verification Page



In this example, library vlib1 is verified. No errors are found.

Setting Serial Number Checking

You can use the Oracle Secure Backup Web tool to enable or disable tape device serial number checking. If serial number checking is enabled, then whenever Oracle Secure Backup opens a tape device, it checks the serial number of that device. If the tape device does not support serial number reporting, then Oracle Secure Backup simply opens the tape device. If the tape device does support serial number checking, then Oracle Secure Backup compares the reported serial number to the serial number stored in the device object. Three results are possible:

- There is no serial number in the device object.

  If Oracle Secure Backup has never opened this tape drive since the device was created or the serial number policy was enabled, then it cannot have stored a serial number in the device object. In this case, the serial number is stored in the device object, and the open succeeds.
- There is a serial number in the device object, and it matches the serial number just read from the device.

  In this case, Oracle Secure Backup opens the tape device.
- There is a serial number in the device object, and it does not match the serial number just read from the device.

  In this case, Oracle Secure Backup returns an error message and does not open the tape device.

> **Note:**
>
> Oracle Secure Backup also performs serial number checking as part of the `--geometry/-g` option to the `lsdev` command in `obtool`. This option causes an Inquiry command to be sent to the specified device, and `lsdev` displays its vendor, product ID, firmware version, and serial number.

To enable or disable tape device serial number checking:

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

The Configure page appears.

2. In the Advanced section, click **Defaults and Policies**.

   The Configure: Defaults and Policies page appears as shown in Figure 7-5.

Figure 7-5 Configure Details and Policies Page

Policy	Description
Backup compression	policies for backup compression operations
Backup encryption	policies for backup encryption operations
Cloud	cloud related policies
Copy instance	copy instance policies
Daemons	daemon and service control policies
Devices	device management policies
Duplication	duplication-related policies
Index	index catalog generation and management policies
Logs	log and history management policies
Media	general media management policies
Naming	WINS host name resolution server identification
NDMP	NDMP Data Management Agent (DMA) defaults
Operations	policies for backup, restore and related operations
Scheduler	backup scheduler policies
Security	security-related policies
Staging	staging-related policies
Testing	controls for test and debug tools
Vaulting	policies for media life cycle management operations

3. In the Policy column, click **devices**.

   The Configure: Defaults and Policies > Devices page appears as shown in Figure 7-6.

Figure 7-6 Defaults and Policies for Devices

Apply OK Cancel

Name	Current Value	Reset to Default Value
Check serial numbers	yes	
Disable Async IO	no	
Discovered device state	not in service	
Disk Pool free space goal	10	
Error rate percentage	8	
Max ACSLS Eject Wait Time	5 minutes	
Max Drive Idle Time	5 minutes	
Return to service check	no	

Apply OK Cancel

4. Do one of the following:

   a. Select **Yes** from the **Check serial numbers** list to enable tape device serial number checking. This is the default setting.

   b. Select **No** from the **Check serial numbers** list to disable tape device serial number checking.

5. Click **OK**.

   The Configure: Defaults and Policies page appears with a success message.

Configuring Disk Pools

Before you can store backups on a disk pool, you must configure the disk pool as a device in your administrative domain. Unlike tape devices, disk pools can be accessed concurrently by independent backup and restore jobs.

This section contains the following topics:

- Displaying the Defined Disk Pools
- Creating Disk Pools
- Editing Disk Pool Properties
- Renaming Disk Pools
- Removing Disk Pools

Displaying the Defined Disk Pools

You must have the `query and display information about devices` right to display disk pools.

To display the list of currently defined disk pools using the Web tool:

1. On the Oracle Secure Backup Web tool Home page, click **Configure**.
2. In the Basic section, click **Devices**.
3. The Configure: Devices page is displayed. It lists all the currently-defined backup containers (disk pools, tape libraries, and tape drives). The details displayed for each backup container are the device name, status, and type of device.

Creating Disk Pools

To store backups to a file system on disk, configure a device that corresponds to this file system directory.

You must have the `manage devices and change device state` right to create disk pools.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for an overview of disk pools

To create a disk pool using the Web tool:

1. Perform the steps in Displaying the Defined Disk Pools.

   The Configure: Devices page appears.
2. Click **Add**.

   The Configure: Devices > New Device page appears.
3. In the **Device** field, enter a name for the disk pool.

The name must start with an alphanumeric character and be unique across the administrative domain. It can contain letters, numerals, dashes, underscores, or periods. It cannot contain spaces. The maximum character length is 127 characters.

4. In the Type field, select **disk**.
5. In the **Status** field, specify if the disk pool is available for backup or restore operations by selecting one of the following options:
   - **in service**

     Indicates that the disk pool is available to perform backup and restore operations.
   - **not in service**

     Indicates that the disk pool is unavailable to perform backup and restore operations.
   - **auto not in service**

     Indicates that the disk pool is unavailable to perform backup or restore operation and is set automatically for a failed operation.
6. In the **Debug mode** field, select yes or no. The default is yes.
7. In the **Capacity** field, specify a value that represents the space allocated to the disk pool. Select one of the following to specify the unit of storage space: KB, MB, GB, TB, PB, or EB. Leave the default value of **(not set)** to indicate that no maximum capacity is specified for this disk pool. In this case, the capacity of the disk pool is limited only by the underlying file system that hosts the disk pool.

   If the space occupied by backups on the disk pool exceeds the capacity specified, then Oracle Secure Backup does not schedule new jobs for this disk pool until the space usage is less than the specified capacity.
8. In the **Concurrent Jobs** field, specify the number of jobs that can be run concurrently for this disk pool. Select **unlimited** to indicate that no limit is set for the number of concurrent jobs.

   This property enables you to control the concurrent usage of disk pools. The jobs include backup jobs, restore jobs, and media management jobs.
9. In the **Free space goal percentage** field, select `system default` or any value between 1-100.

   The free space goal percentage is the percentage of free space that Oracle Secure Backup maintains in a disk pool. Before scheduling a backup or restore job for a disk pool, the Oracle Secure Backup scheduler checks the disk pool usage. If the amount of free space is less than the specified free space goal percentage, then expired backup image instances are deleted.
10. In the **Blocking factor** field, enter a value that specifies the blocking factor for the disk pool or leave the field blank to accept the default setting. The default is 128 bytes.

    > **See Also:**
    >
    > *Oracle Secure Backup Administrator's Guide* for information about blocking factor and maximum blocking factor
11. In the **Max blocking factor** field, enter a value for the maximum blocking factor for the disk pool.

    The largest value supported for the maximum blocking factor is 4096. This represents a maximum block size of 2 MB.

12. In the **Attachment** field, specify the host and file system directory that stores backup image instances for this disk pool. Provide information in the following fields:
    - **Host: Base path:** Enter the host name of the Oracle Secure Backup client that stores the backups.
    - **Directory:** Enter the name of the file system directory that stores the backups for this disk pool.

      > **Note:**
      >
      > Ensure the NFS-mounted file system for disk pool attachments is hard-mounted with read/write permissions. This prevents timeouts during backups of large files and reduces the risk of data loss. Configure the NFS mount with the `root_squash` option, allowing root user `write` access for Oracle Secure Backup operations. Adherence to these configurations ensures efficient and secure data management.

    - **Initialize:** Select **yes** or **no**.

      > **See Also:**
      >
      > *Oracle Secure Backup Administrator's Guide* for more on managing disk pools.

13. In the **Enable Checksum** field, select one of the following options:
    - **system default**

      Uses the setting specified by the **Enable disk checksum** device policy to determine if a checksum must be computed for backup image instances. This is the default setting.
    - **yes**

      Computes a checksum for the all backup image instances that are written to this disk pool. The checksum is stored as part of the backup metadata.
    - **no**

      Does not compute or store a checksum for the backup image instances that are written to this disk pool.
14. Click **OK** to create the disk pool.

> **Caution:**
>
> In a dedup file system, the amount of disk space occupied by a disk pool (as reported by OS commands, such as "df -h") is less than the standard storage. If you create a disk pool on a dedup file system and overfill the file system, Oracle Secure Backup utilities for managing disk space will not report accurate sizes for disk pools on dedup file systems.

Editing Disk Pool Properties

You can use the Web tool to edit disk pool properties. You must have the `manage devices and change device state` right to edit disk pool properties.

To edit the properties of a disk pool:

1. Perform the steps in "Displaying the Defined Disk Pools".

   The Configure: Devices page appears. The currently configured devices, tape devices and disk pools, are listed on this page.

2. Select the disk pool whose properties need to be edited and click **Edit**.

   The Configure: Device > *disk_pool_name* page is displayed.

3. Modify the required disk pool properties.

   You can edit any of the following properties: Status, Debug mode, Capacity, Concurrent jobs, Free space goal percentage, Blocking factor, Max blocking factor.

   See "Creating Disk Pools" for more details about each of these properties.

4. Click **Save** to commit the changes to disk pool properties.

Renaming Disk Pools

You must have the `manage devices and change device state` right to edit disk pool properties.

To rename a disk pool:

1. Perform the steps in "Displaying the Defined Disk Pools".

   The Configure: Devices page appears. The currently configured devices, tape devices and disk pools, are listed on this page.

2. Select the disk pool that you want to rename and click **Rename**.

3. In the **Rename *device_name* to** field, enter the new name of the disk pool.

Removing Disk Pools

You need the manage devices and change device state right to remove a disk pool.

To remove a disk pool:

1. Perform the steps in "Displaying the Defined Disk Pools".

   The Configure: Devices page appears. The currently configured devices, tape devices and disk pools, are listed on this page.

2. Select the disk pool to be removed and click **Remove**.

   A prompt is displayed asking if you want to delete all backup image instances for the disk pool that is being removed.

3. Totalled the backup image instances stored on the selected disk pool, select **Yes**.

   To retain the backup image instances stored on the selected disk pool, select **No**.

   A prompt is displayed asking if you want to force a delete of backup image instances even if they are unexpired.

4. Click **Yes** to force a delete of backup image instances on the selected disk pool. Click **No** to retain unexpired backup image instances.
5. On the Configure: Device Remove Summary page, a confirmation is displayed asking if you want to remove the disk pool. Click **Yes**.

Managing Hosts in the Administrative Domain

After you configure hosts in the administrative domain, you can manage the hosts by performing any of the following tasks:

- Viewing the Hosts in the Administrative Domain
- Viewing or Editing Host Properties
- Updating Hosts in the Administrative Domain
- Removing Hosts from an Administrative Domain

Viewing the Hosts in the Administrative Domain

To view hosts in the administrative domain:

1. Open the Oracle Secure Backup Web tool running on the administrative server and log in as the `admin` user.

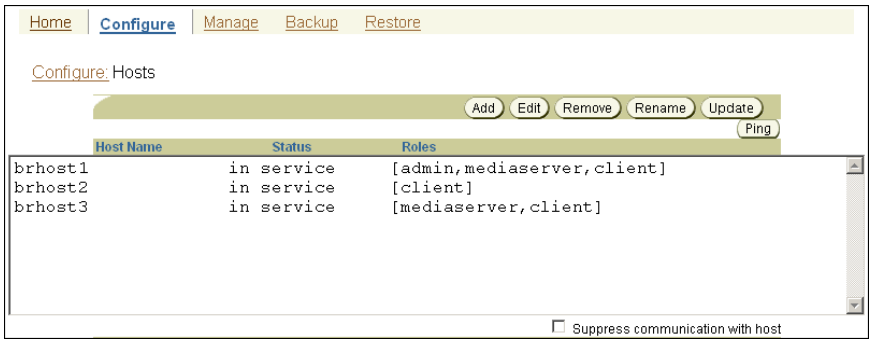
> **See Also:**
>
> "Starting a Web Tool Session" for information about accessing the Web tool

2. Click the **Configure** tab.

   The Configure page is displayed.
3. Select **Hosts** in the Basic section.

   The Configure: Hosts page appears as displayed as displayed in Figure 7-7. The Hosts page lists the host name, configured host roles, and the current status of the host.

Figure 7-7 Oracle Secure Backup Web Tool: Hosts Page



> **Note:**
>
> You can also view the current list of hosts with the obtool `lshost` command.

Viewing or Editing Host Properties

If you are having difficulties configuring Oracle Secure Backup, you might be required to view and/or edit hosts that are members of the domain.

To display or edit host properties:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the name of the host whose properties require editing.

   Select the **Suppress communication with host** option to edit a host that is currently not accessible through the network.
3. Click **Edit**.

   The Oracle Secure Backup Web tool displays a page with details for the host you selected.
4. Make any desired changes to the host properties.
5. Click **OK** to save your changes.

Updating Hosts in the Administrative Domain

When you add or modify a host in an Oracle Secure Backup administrative domain, Oracle Secure Backup exchanges messages with that host to inform it of its changed state. If you make changes to your administrative host, your client will likely contain outdated configuration information. Update Host can be used to send fresh state information to the client.

Updating is useful only for hosts running Oracle Secure Backup natively. Hosts accessed in NDMP mode, such as NAS devices, do not maintain any Oracle Secure Backup state data and therefore it is not necessary to update their state information.

To update a host:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the name of the host to be updated.
3. Click **Update**.

Removing Hosts from an Administrative Domain

This section explains how to remove a host from an Oracle Secure Backup administrative domain. When you remove a host, Oracle Secure Backup destroys all information pertinent to that host, including:

- Configuration data
- Incremental backup state information
- Metadata in the backup catalog for this host
- Each device attachment
- PNI references

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

To remove a host:

1. Display the Hosts page as described in "Viewing the Hosts in the Administrative Domain".
2. Select the name of the host to remove.

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

   Oracle Secure Backup prompts you to confirm the removal of the host.
4. Click **Yes** to remove the host or **No** to leave the host undisturbed.

   Oracle Secure Backup removes the host and returns you to the **Host** page.

Configuring Cloud Storage Devices

Before you can store backups on a cloud storage device, you must configure it as a device in your administrative domain.

This section contains the following topics:

- Prerequisites for Configuring Storage Devices for OCI Classic
- Configuring an Authentication Object for Oracle Cloud Infrastructure
- Creating Cloud Storage Devices for Oracle Cloud Infrastructure
- Creating Cloud Storage Devices for Oracle Cloud Infrastructure Classic
- Displaying the Defined Cloud Storage Devices
- Editing Cloud Storage Device Properties
- Renaming Cloud Storage Devices
- Removing Cloud Storage Devices
- About Cloud Certificates

Prerequisites for Configuring Storage Devices for OCI Classic

You must complete the following tasks before you can configure an Oracle Secure Backup cloud storage device for Oracle Cloud Infrastructure Classic:

1. Subscribe to Oracle Cloud Infrastructure Object Storage Classic.
2. Acquire your login credentials and identity domain.

The information provided in this topic explains how to perform each of these tasks.

Subscribing to Oracle Cloud

Oracle Cloud Infrastructure Object Storage Classic offers different storage options with and without replication. In addition to object storage, Oracle provides Oracle Cloud Infrastructure Archive Storage Classic which provides storage for long term retention. To access these services, you must first acquire a subscription.

> **See Also:**
>
> - Storage Classic for further details about these services
> - Get Started with Oracle Cloud for information about free trials and subscriptions

Acquiring Login Credentials and an Identity Domain

When you subscribe to Oracle Cloud services, a unique identifier, called an identity domain, is created for all of your services. It is recommended that you create an identity domain administrator user to manage your cloud services. You must have the `Storage_Administrator` and `Storage_ReadWriteGroup` roles in order to do so.

After you receive your identity domain and user credentials, you can use them to create login accounts for other users who need to access the services. To access storage services from Oracle Secure Backup, it is recommended that you create another user that has the `Storage_Administrator` role.

> **See Also:**
>
> - Adding Users and Assigning Roles for more information about Oracle Cloud Storage roles and users

Configuring an Authentication Object for Oracle Cloud Infrastructure

You must create an authentication object for Oracle Cloud Infrastructure before you can configure a cloud storage device that stores backups in Oracle Cloud Infrastructure Object Storage. The authentication object contains information such as the public key fingerprint, private key file, identity domain, and tenancy information that is required to authenticate Oracle Secure Backup with Oracle Cloud Infrastructure.

Before configuring an authentication object for Oracle Cloud Infrastructure:

- You must have the `modify domain configuration` right.
- You must have an Oracle Cloud account with access to Oracle Cloud Infrastructure Object Storage. See Object Storage.
- You must generate a key pair file that contains a public key and a private key used to authenticate with Oracle Cloud Infrastructure, as described in How to Generate an API Signing Key. Both keys must be in `PEM` format. The private key is stored on the media server, not in Oracle Cloud.
- You must configure the key pair in the Oracle Cloud Infrastructure Console as described in How to Upload the Public Key. This generates a fingerprint for the key.

To create an authentication object for Oracle Cloud Infrastructure:

1. On the Oracle Secure Backup Web tool Home page, click **Configure**.
2. In the Basic section, click **Authetications**.

   The Configure: Authentications page appears.
3. Click **Add**.

The Configure: Authentications > New Authentications page appears.

4. In the Authentication field, enter a name for the authentication object.

   The name must start with an alphanumeric character and be unique across the administrative domain. It can contain letters, numerals, dashes, underscores, or periods. It cannot contain spaces. The maximum character length is 127 characters.

5. In the **Type** field, select **OCI** to create an Oracle Cloud Infrastructure authentication object.
6. In the **Tenancy ocid** field, specify the tenancy OCID for your Oracle Cloud Infrastructure account. The tenancy contains all your Oracle Cloud Infrastructure resources and is assigned a unique ID.
7. In the **User ocid** field, specify the user ID for your Oracle Cloud Infrastructure account.
8. In the **Key** field, click **Browse** and select the file that contains the private key that you generated to authenticate Oracle Secure Backup with Oracle Cloud Infrastructure.
9. In the **Fingerprint** field, specify the public key that you generated in the key pair file.
10. In the **Identity Domain** field, specify the identity domain. The identity domain is a construct for managing certain features of Oracle Cloud Infrastructure.
11. In the **URL** field, specify the endpoint URL provided by Oracle Cloud Infrastructure Object Storage.

    The endpoint URL depends on the region. For example:

    ```
    https://objectstorage.us-phoenix-1.oraclecloud.com
    ```

12. In the **Comments** field, enter a description of this authentication object.

    This step is optional.

13. Click **Apply**.

Creating Cloud Storage Devices for Oracle Cloud Infrastructure

Use the `mkdev` command or the Oracle Secure Backup Web tool to create a new cloud storage device for Oracle Cloud Infrastructure.

You must have the `manage devices` and `change device state` rights to create cloud storage devices for Oracle Cloud Infrastructure. An authentication object for Oracle Cloud Infrastructure must also be configured.

To create a cloud storage device for Oracle Cloud Infrastructure using the Web tool:

1. Perform the steps in "Displaying the Defined Cloud Storage Devices".

   The Configure: Devices page appears.

2. Click **Add**.

   The Configure: Devices > New Device page appears.

3. In the **Device** field, enter a name for the cloud storage device.

   The name must start with an alphanumeric character and be unique across the administrative domain. It can contain letters, numerals, dashes, underscores, or periods. It cannot contain spaces. The maximum character length is 127 characters.

4. In the **Type** field, select **cloudstorage**.
5. In the **Status** field, specify if the cloud storage device is available for backup or restore operations by selecting one of the following options:

- **in service**

  Indicates that the cloud storage device is available to perform Oracle Secure Backup backup and restore operations.

- **not in service**

  Indicates that the cloud storage device is unavailable to perform Oracle Secure Backup backup and restore operations.

- **auto not in service**

  Indicates an error in the cloud storage device. Do not select this option during configuration.

6. In the **Debug mode** field, select yes or no. The default is no.
7. In the **Service Type** field, select **oci**.
8. In the **Authentication Object** field, select the authentication object that contains the information required to authenticate Oracle Secure Backup with Oracle Cloud Infrastructure.

   The authentication object is created as described in Configuring an Authentication Object for Oracle Cloud Infrastructure.
9. In the **Compartment** field, enter the name of the compartment that contains the bucket in which the backed up data will be stored.
10. In the **Mediaserver** field, specify the name of the attached media server to which this cloud device must be attached.
11. In the **Storage class** field, select archive, object, or infrequent access.
12. In the **Capacity** field, specify a value that represents the space allocated to the cloud storage device. Select one of the following to specify the unit of storage space: KB, MB, GB, TB, PB, or EB. Leave the default value of **(not set)** to indicate that no maximum capacity is specified for this cloud storage device. In this case, the capacity of the cloud storage device is limited by the storage capacity you purchased or that was assigned by the account administrator.

    If the space occupied by backups on the cloud storage device exceeds the capacity specified, then Oracle Secure Backup does not schedule new jobs for this cloud storage device until the space utilization drops to below the specified capacity.
13. In the **Segment size** field, enter the size of the object. (Oracle Secure Backup stores each backup image by splitting it into multiple segments and storing each segment as a single object in the container.)
14. In the **Streams per job** field, enter the number of connections to Oracle Cloud Infrastructure that Oracle Secure Backup can make per job. Alternatively, you can check the box for streams per job system default, which is 4.
15. In the **Concurrent Jobs** field, specify the number of jobs that can be run concurrently for this cloud storage device.

    This property enables you to control the concurrent usage of cloud storage devices. The jobs include backup jobs, restore jobs, and media management jobs.
16. In the **Blocking factor** field, the value you enter defines the block transfer size from the client to the media server. Increasing this value may improve backup performance. The default value is 128.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for information about blocking factor and maximum blocking factor

17. In the **Max blocking factor** field, enter a value for the maximum blocking factor for the cloud storage device.

    The largest value supported for the maximum blocking factor is 4096. This represents a maximum block size of 2MB.

18. In the **Free space goal percentage** field, select `system default` or any value between 1-100.

    The free space goal percentage is the percentage of free space that Oracle Secure Backup maintains in a cloud storage device. Before scheduling a backup or restore job for a cloud storage device, the Oracle Secure Backup scheduler checks the cloud storage device utilization. If the amount of free space is lower than the specified free space goal percentage, then expired backup image instances are deleted.

19. In the **Force** field, check the box to force association of the device with an existing container created by Oracle Secure Backup.

20. In the **Enable Checksum** field, select one of the following options:

    - **system default**

      Uses the setting specified by the **Enable cloud checksum** device policy to determine if a checksum must be computed for backup image instances. This is the default setting.

    - **yes**

      Computes a checksum for the all backup image instances that are written to this Cloud storage device. The checksum is stored as part of the backup metadata.

    - **no**

      Does not compute or store a checksum for the backup image instances that are written to this Cloud storage device.

21. Click **OK** to create the cloud storage device.

22. After the cloud storage device is created, it should be pinged. To do so, select the device from the Configure: Devices page and click on **ping**.

Creating Cloud Storage Devices for Oracle Cloud Infrastructure Classic

Use the `mkdev` command or the Oracle Secure Backup web tool to create a new cloud storage device for Oracle Cloud Infrastructure Classic. You must have the `manage devices` and `change device state` rights to create cloud storage devices.

To create a cloud storage device using the Web tool:

1. Perform the steps in "Displaying the Defined Cloud Storage Devices".

   The Configure: Devices page appears.

2. Click **Add**.

   The Configure: Devices > New Device page appears.

3. In the **Device** field, enter a name for the cloud storage device.

   The name must start with an alphanumeric character and be unique across the administrative domain. It can contain letters, numerals, dashes, underscores, or periods. It cannot contain spaces. The maximum character length is 127 characters.

4. In the Type field, select **cloudstorage**.

5. In the **Status** field, specify if the cloud storage device is available for backup or restore operations by selecting one of the following options:

   - **in service**

     Indicates that the cloud storage device is available to perform Oracle Secure Backup backup and restore operations.

   - **not in service**

     Indicates that the cloud storage device is unavailable to perform Oracle Secure Backup backup and restore operations.

6. In the **Debug mode** field, select yes or no. The default is no.

7. In the Service Type field, select **oci-classic**.

8. In the **Authentication Object** field, select the authentication object that contains the information required to authenticate Oracle Secure Backup with Oracle Cloud Infrastructure Classic.

   The authentication object is created as described in Configuring an Authentication Object for Oracle Cloud Infrastructure.

9. In the **Mediaserver** field, specify the name of the attached media server.

10. In the **Storage class** field, select archive or object.

11. In the **Capacity** field, specify a value that represents the space allocated to the cloud storage device. Select one of the following to specify the unit of storage space: KB, MB, GB, TB, PB, or EB. Leave the default value of **(not set)** to indicate that no maximum capacity is specified for this cloud storage device. In this case, the capacity of the cloud storage device is limited by the storage capacity you purchased or that was assigned by the account administrator.

    If the space occupied by backups on the cloud storage device exceeds the capacity specified, then Oracle Secure Backup does not schedule new jobs for this cloud storage device until the space utilization drops to below the specified capacity.

12. In the **Username** field, enter the user name of the cloud account. Specifying a user name is not required if you selected an authentication object.

13. In the **Password** field, enter the password. In the **Verify password** field, enter the password again. Specifying a password is not required if you selected an authentication object.

14. In the **Container** field, enter the name of the container. Oracle Secure Backup creates a new container in Oracle Cloud Infrastructure Object Storage Classic with the name you specify. You cannot specify an already existing name unless you also specify the `--force` option. Oracle Secure Backup does not support the use of existing containers that were not created by Oracle Secure Backup.

15. In the Segment size field, enter the size of the object. (Oracle Secure Backup stores each backup image by splitting it into multiple segments and storing each segment as a single object in the container.)

16. In the **Streams per job** field, enter the number of connections to Oracle Cloud Infrastructure that Oracle Secure Backup can make per job. Alternatively, you can check the box for streams per job system default, which is 4.
17. In the **Concurrent Jobs** field, specify the number of jobs that can be run concurrently for this cloud storage device.

    This property enables you to control the concurrent usage of cloud storage devices. The jobs include backup jobs, restore jobs, and media management jobs.
18. In the **Blocking factor** field, the value you enter defines the block transfer size from the client to the media server. Increasing this value may improve backup performance. The default value is 128.

    > **See Also:**
    >
    > *Oracle Secure Backup Administrator's Guide* for information about blocking factor and maximum blocking factor
19. In the **Max blocking factor** field, enter a value for the maximum blocking factor for the cloud storage device.

    The largest value supported for the maximum blocking factor is 4096. This represents a maximum block size of 2MB.
20. In the **Free space goal percentage** field, select `system default` or any value between 1-100.

    The free space goal percentage is the percentage of free space that Oracle Secure Backup maintains in a cloud storage device. Before scheduling a backup or restore job for a cloud storage device, the Oracle Secure Backup scheduler checks the cloud storage device utilization. If the amount of free space is lower than the specified free space goal percentage, then expired backup image instances are deleted.
21. In the **URL** field, specify the endpoint URL provided by Oracle Cloud Storage Service. This step is optional if you specified an authentication object. The endpoint URL is usually the following, where *`identity_domain_name`* is replaced with the name of an actual identity domain:

    `identity_domain_name``.storage.oraclecloud.com`
22. In the **Identity domain** field, specify the identity domain. The identity domain is a construct for managing certain features of Oracle Cloud Infrastructure.
23. In the **Force** field, check the box to force association of the device with an existing container created by Oracle Secure Backup.
24. In the **Enable Checksum** field, select one of the following options:

    - **system default**

      Uses the setting specified by the **Enable cloud checksum** device policy to determine if a checksum must be computed for backup image instances. This is the default setting.
    - **yes**

      Computes a checksum for the all backup image instances that are written to this Cloud storage device. The checksum is stored as part of the backup metadata.
    - **no**

Does not compute or store a checksum for the backup image instances that are written to this Cloud storage device.

25. Click **OK** to create the cloud storage device.
26. After the cloud storage device is created, it should be pinged. To do so, select the device from the Configure: Devices page and click on **ping**.

Displaying the Defined Cloud Storage Devices

You must have the `query and display information about devices` right to display cloud storage devices.

To display the list of currently defined cloud storage devices using the Web tool:

1. On the Oracle Secure Backup Web tool Home page, click **Configure**.
2. In the Basic section, click **Devices**.
3. The Configure: Devices page is displayed. It lists all the currently-defined backup containers. The details displayed for each backup container are the type of device, status, and device name.

Editing Cloud Storage Device Properties

You can use the Web tool to edit properties of cloud storage devices. You must have the `manage devices` and `change device state` rights to edit properties.

Using the Web tool to edit cloud storage device properties

1. Perform the steps in "Displaying the Defined Cloud Storage Devices".

   The Configure: Devices page appears. The currently configured devices are listed on this page.
2. Select the cloud storage device whose properties need to be edited and click **Edit**.

   The Configure: Device > *cloud_storage_device_name* page is displayed.
3. Modify the required cloud storage device properties. Neither the container name nor the storage class can be modified.
4. Click **Save** to commit the changes.

Renaming Cloud Storage Devices

You must have the `manage devices` and `change device state` right to rename cloud storage devices.

Using the Web tool to rename a cloud storage device

1. Perform the steps in "Displaying the Defined Cloud Storage Devices".

   The Configure: Devices page appears. The currently configured devices, tape devices, and disk pools, are listed on this page.
2. Select the cloud storage device that you want to rename and click **Rename**.
3. In the **Rename *device_name* to** field, enter the new name of the cloud storage device.

Removing Cloud Storage Devices

You need the `manage devices` and `change device state` rights to remove cloud storage device.

Using the Web tool to remove a cloud storage device

1. Perform the steps in "Displaying the Defined Cloud Storage Devices".

   The Configure: Devices page appears. The currently configured devices, tape devices and disk pools, are listed on this page.

2. Select the cloud storage device to be removed and click **Remove**.

   A prompt is displayed asking if you want to delete all backup image instances for the device that is being removed.

3. To delete all backup image instances stored on the selected device, select **Yes**.

   To retain the backup image instances stored on the selected device, select **No**.

   A prompt is displayed asking if you want to force a delete of backup image instances even if they are unexpired.

4. Click **Yes** to force a delete of backup image instances on the selected device. Click **No** to retain all backup image instances.

5. On the Configure: Device Remove Summary page, a confirmation is displayed asking if you want to remove the device. Click **Yes**.

About Cloud Certificates

Oracle Secure Backup uses HTTPS/TLS to connect to Oracle Cloud Infrastructure object storage. To establish a secure connection, Oracle Secure Backup requires a certificate from the Object Storage region and validates it with its corresponding public trusted root certificate.

Every region has its own certificate, which belongs to the same certificate chain. Oracle Secure Backup stores the public trusted root certificate in a Cloud wallet and generally uses the same root certificate to validate the certificates from these regions. In certain situations, it may be required to add a new Cloud certificate to the Cloud wallet. For example, Oracle Cloud Infrastructure moves to a different certificate chain.

Oracle Secure Backup installation creates a Cloud wallet in Oracle Secure Backup home and populates the wallet with default certificates. A Cloud wallet can contain multiple certificates. Oracle Secure Backup does not add new certificates automatically to the Cloud wallet.

This section contains the following topics:

- Adding Certificates to the Cloud Wallet
- Manually Creating a Cloud Wallet

Adding Certificates to the Cloud Wallet

Add new certificates to the existing Cloud wallet, keeping the old certificates in the wallet intact.

Adding a new certificate to the wallet can resolve the `ORA-29024: Certificate validation failure` error.

> **Note:**
>
> Add the new certificate to the Cloud wallet on the Oracle Secure Backup administrative server and on all media servers in the domain. To use the Client Direct to Coud feature on a client host, you must update the Cloud wallet on that client.

To add a new certificate to the Cloud wallet:

1. Download a Cloud server Certification Authority (CA) certificate.
2. Import the certificate into the Cloud wallet.

Download a Cloud server CA certificate

Use the following steps to download the required certificate.

1. Determine the Oracle Cloud Infrastructure Object Storage's Region Identifier.
   a. Log on to the Oracle Cloud Infrastructure Console.
   b. Click the *Region Name* in the top control bar.
   c. Select **Manage Regions** from the drop-down menu.

      The Infrastructure page displays a list of regions and their Region Identifiers.
   d. Use the *region-identifier* for the region where the object storage bucket is located.
2. Open a web browser and go to the following URL.

   https://objectstorage.*region_identifier*.oraclecloud.com

   Replace the *region_identifier* with the Region Identifier from the previous step.

   > **Note:**
   >
   > In this example, the *region_identifier* is "us-phoenix-1".
   >
   > https://objectstorage.us-phoenix-1.oraclecloud.com

   Each browser, on each platform operating system, displays a slightly different message. The example below is from Firefox on a Windows 10 platform.

   ```
   code:        "NotFound"
   message:    "Not Found"
   ```

3. Click the security icon (padlock) located on the left side of the address bar. It opens a drop-down to display site information.
4. Click **Connection secure**. It opens a drop-down to display the connection security information for the site.
5. Click **More Information**.

   It opens the Certificate Property page, which contains three tabs - **General**, **Media**, and **Security**. The Certificate Property page displays the **Security** tab by default.
6. On the **Security** tab, click the **View Certificate** button. It opens a Certificate page with three certificate names on top.

7. Click the root certificate name to open the root certificate tab. It highlights the root certificate name.

> **Note:**
>
> In this example, the root certificate name is "DigiCert Global Root G2".

8. On the root certificate tab, scroll down to the **Download** link. Under **Miscellaneous**, it contains two links, "PEM (cert)" and "PEM (chain)".

   Click on the **PEM (cert)** link to download the certificate. In this example, the file name of the certificate is `objectstorage-us-phoenix-1-oraclecloud-com.pem`.

> **Note:**
>
> While downloading the certificate in Firefox, it populates the file name automatically and saves the certificate in `*.PEM` format. If you use Microsoft Edge, it prompts you to provide a file name for the certificate. In Microsoft Edge, export the certificate file as "Base-64 encoded X.509 (.CER)"

9. Follow the download wizard and save the **PEM (cert)** file on your host, for example, the `/tmp` location.

You can now import this downloaded certificate to the Cloud wallet.

Store this certificate file on the Oracle Secure Backup administrative server and on all media servers in the domain.

Import Certificate into the Cloud wallet

Add new certificates to the Cloud wallet in the Oracle Secure Backup Home.

To add a certificate to the cloud wallet:

1. Import the certificate into the Cloud wallet using the Oracle Secure Backup `obcm` tool.

```
#obcm wallet --cloudwallet --add /tmp/objectstorage-us-phoenix-1-
oraclecloud-com.pem
Trust point has been imported into wallet.
```

> **Note:**
>
> In this example, the certificate file name is "objectstorage-us-phoenix-1-oraclecloud-com.pem".

2. Verify that the Cloud wallet displays the newly added certificate.

```
# obcm display --cloudwallet -v
```

Example output:

The output displays the new trust points in the wallet with the CN of the downloaded certificate.

```
Trust point:
    DN: CN=DigiCert Global Root G2,OU=www.digicert.com,O=DigiCert Inc,C=US
    Issuer: CN=DigiCert Global Root G2,OU=www.digicert.com,O=DigiCert
Inc,C=US
    Type: NZDST_CLEAR_PTP
    Public key size: 2048
    Key usage: CA CERT SIGNING
    Serial number: 0x033AF1E6A711A9A0BB2864B11D09FAE5
    Version: NZTTVERSION_X509v3
    Signature algorithm: NZDCATSHA256RSA
    Valid from: 2013/08/01.12:00:00 (UTC)
    Valid to:   2038/01/15.12:00:00 (UTC)
```

> **Note:**
>
> Add the new certificate to the Cloud wallet on the Oracle Secure Backup administrative server and on all media servers in the domain.

Manually Creating a Cloud Wallet

Oracle Secure Backup installation creates a Cloud Wallet automatically in the Oracle Secure Backup Home.

However, you can manually create a new Cloud Wallet with the `obcm` utility. When you create a new Cloud Wallet manually, Oracle Secure Backup creates an empty wallet without any certificates.

> **WARNING:**
>
> Manually creating a new Cloud wallet deletes the old wallet and removes all the existing certificates stored in it. It is not recommended to create a Cloud wallet manually.

To manually create a Cloud wallet:

1. Run the `obcm` utility.

   ```
   # obcm wallet --create --cloudwallet
   Wallet has been created.
   ```

2. Display the newly created wallet.

   ```
   # obcm display -cloudwallet -v
   There are 0 certificate requests in the wallet
   There are 0 certificates in the wallet
   There are 0 trust points in the wallet
   ```

A new Cloud wallet contains no certificates or trust points.

> **Note:**
>
> Oracle Secure Backup requires a Cloud Wallet on the administrative server and on all media servers in the domain.

8

Performing Upgrade Installation of Oracle Secure Backup

You can upgrade Oracle Secure Backup on Linux or UNIX and on Windows platforms.

Topics

Preparing for Upgrade Installation

You can upgrade Oracle Secure Backup to a newer version on all hosts in your administrative domain.

In an upgrade installation, the Oracle Secure Backup catalogs (contained in the `admin` directory) are preserved, retaining configuration information and backup metadata for your administrative domain. This state information for your administrative domain, such as the backup catalog, host, user and device configuration information, and any scheduled backup jobs, is stored in the `admin` directory under the Oracle Secure Backup home on your administrative server.

> **Note:**
>
> Oracle recommends taking backups of the administrative server before performing an upgrade installation.

While performing an upgrade installation of Oracle Secure Backup, consider the following:

- Ensure that the platform supports the newer version of Oracle Secure Backup. If you try to upgrade Oracle Secure Backup on an unsupported platform, then it returns an error and exits the installation.

  > **See Also:**
  >
  > Supported Platforms and Tape Devices

- Before upgrading the administrative domain, shut down all drivers and background processes associated with Oracle Secure Backup on all hosts. Ensure that the media servers and the clients are out-of-service.
- Before upgrading the administrative server, verify that the backup domain is not performing any backup operations on any host.

- Upgrade the administrative server host first, and then the other hosts in the domain.
- The installer preserves the role of each host during the upgrade process.
- Retain the Oracle Secure Backup policy settings during the upgrade process.

Upgrading Oracle Secure Backup

You can upgrade Oracle Secure Backup 18.1.0.0, Oracle Secure Backup 18.1.0.1, or Oracle Secure Backup 18.1.0.2 to Oracle Secure Backup 19.1.

If you want to upgrade from an older version of Oracle Secure Backup, then you must first upgrade to Oracle Secure Backup 18.1.0.1 and then upgrade to Oracle Secure Backup 19.1.

> **Note:**
>
> You must upgrade all media servers to Oracle Secure Backup 19.1.

Access to any new commands and options introduced in Oracle Secure Backup 19.1 are not supported from earlier version clients. The new commands must be accessed from an Oracle Secure Backup 19.1 host or through the Oracle Secure Backup Web Tool. A database backup to a cloud storage device from an Oracle Secure Backup earlier than 18.1 is not supported.

The `obtool` utility is available for a client if the client version matches with that of the administrative server. For example, if the administrative server is upgraded to Oracle Secure Backup 19.1 and the clients have Oracle Secure Backup 18.1.0.2, then `obtool` is not available for those clients. For clients to use the `obtool` functionality and the new features, they must upgrade to the same version as the administrative server, that is, Oracle Secure Backup 19.1.

> **Note:**
>
> The clients can have earlier versions of Oracle Secure Backup if required in certain scenarios. For example, the operation system on client does not support the current version of Oracle Secure Backup.

Upgrading a client to the same Oracle Secure Backup version as on the administrative server ensures the highest level of interoperability.

> **See Also:**
>
> - About Oracle Secure Backup Client Backward Compatibility in the *Oracle Secure Backup Installation and Configuration Guide* for more information about Client Backward Compatibility
> - Upgrading Oracle Secure Backup in the *Oracle Secure Backup Installation and Configuration Guide* for more information about how to upgrade Oracle Secure Backup

Upgrade Installation on Linux or UNIX

You can upgrade your administrative server, media servers, and clients on a Linux or UNIX platform to a latest version of Oracle Secure Backup by running the setup utility.

Steps for Upgrade Installation on Linux or UNIX

1. Uninstall the existing Oracle Secure Backup from your system.

   While uninstalling the administrative server, ensure that you save the `admin` directory and remove the Oracle Secure Backup home directory.

   > **See Also:**
   >
   > Uninstalling Oracle Secure Backup

2. Run the Oracle Secure Backup installation script for the new version.

Upgrade Installation on Windows

You can upgrade your administrative server, media servers, and clients on a Windows platform to a latest version of Oracle Secure Backup by running the setup utility.

Steps for Upgrade Installation on Windows

1. Uninstall the existing Oracle Secure Backup and select the **Keep** option when prompted. This options saves the `admin` directory while removing the Oracle Secure Backup software.

   > **See Also:**
   >
   > - Uninstalling Oracle Secure Backup on Windows

2. Run the Oracle Secure Backup setup utility for the new version.

For some hosts, such as media servers, the installer may prompt to restart the host.

Before starting a new installation, the setup utility checks for any existing Oracle Secure Backup on your system. If your system has Oracle Secure Backup installed, then the setup utility automatically runs an uninstaller program to remove the existing Oracle Secure Backup from your system.

The uninstaller displays the following prompt:

```
This system was configured as an Oracle Secure Backup Administrative Server.

Oracle Secure Backup creates files specific to this administrative
domain in the "admin" directory. Would you like to keep these files
in case you reinstall Oracle Secure Backup?

If you choose "Delete" all files related to Oracle Secure Backup
will be removed from this system. If you choose "Keep" the files
specific to this administrative domain will be retained.
```

- To perform an upgrade installation, you must select the **Keep** option to save the `admin` directory.
- If you select the **Delete** option, then the upgrade installation is not successful.

Removing the Administrative Directory

You have an option to remove the existing `admin` directory files as follows:

1. Exit the installation process, if it's running.
2. Uninstall the existing version of Oracle Secure Backup.
3. Select the **Delete** option when prompted to remove the `admin` directory.

After uninstalling the existing Oracle Secure Backup, you can reinstall a new version of Oracle Secure Backup by running the setup utility.

9

Managing Security for Backup Networks

This chapter describes how to make your backup network more secure. Oracle Secure Backup is automatically configured for network security in your administrative domain, but you can enhance that basic level of security in several ways. Secure communications among the nodes of your administrative domain concerns the encryption of network traffic among your hosts. Secure communications is distinct from Oracle Secure Backup user and roles security concerns and security addressed by the encryption of backups to tape.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information on users and roles management and backup encryption

This chapter contains these sections:

- Backup Network Security Overview
- Planning Security for an Administrative Domain
- Trusted Hosts
- Host Authentication and Communication
- Encryption of Data in Transit
- Default Security Configuration
- Configuring Security for the Administrative Domain
- Managing Certificates with obcm

Backup Network Security Overview

An Oracle Secure Backup administrative domain is a network of hosts. Any such network has a level of vulnerability to malicious attacks. The task of the security administrator is to learn the types of possible attacks and techniques to guard against them. Your backup network must meet the following requirements to be both useful and secure:

- Software components must not expose the hosts they run on to attack.

  For example, daemons should be prevented from listening on a well-known port and performing arbitrary privileged operations.
- Data managed by the backup software must not be viewable, erasable, or modifiable by unauthorized users.
- Backup software must permit authorized users to perform these tasks.

Oracle Secure Backup meets these requirements in its default configuration. By default, all hosts that run Oracle Secure Backup must have their identity verified before they can join the administrative domain. A host within the domain uses an X.509 certificate for host authentication. After a Secure Sockets Layer (SSL) connection is established between hosts,

control and data messages are encrypted when transmitted over the network. SSL protects the administrative domain from eavesdropping, message tampering or forgery, and replay attacks.

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

Planning Security for an Administrative Domain

If security is of primary concern in your environment, then you might find it helpful to plan for network security in the following stages:

- Identifying Assets and Principals
- Identifying Your Backup Environment Type
- Choosing Secure Hosts for the Administrative and Media Servers
- Determining the Distribution Method of Host Identity Certificates

After completing these stages, you can proceed to the implementation phase as described in "Configuring Security for the Administrative Domain".

Identifying Assets and Principals

The first step in planning security for an administrative domain is determining the assets and principals associated with the domain. The assets of the domain include:

- Database and file-system data requiring backup
- Metadata about the database and file-system data
- Passwords
- Identities
- Hosts and storage devices

Principals are users who either have access to the assets associated with the administrative domain or to a larger network that contains the domain. Principals include the following users:

- Backup administrators

  These Oracle Secure Backup users have administrative rights in the domain, access to the tapes containing backup data, and the rights required to perform backup and restore operations.

- Database administrators

  Each database administrator has complete access to his or her own database.

- Host owners

  Each host owner has complete access to its file system.

- System administrators

  These users might have access to the corporate network and to the hosts in the administrative domain (although not necessarily root access).

- Onlookers

  These users do not fall into any of the preceding categories of principals, but can access a larger network that contains the Oracle Secure Backup domain. Onlookers might own a host outside the domain.

The relationships between assets and principals partially determine the level of security in the Oracle Secure Backup administrative domain:

- In the highest level of security, the only principal with access to an asset is the owner. For example, only the owner of a client host can read or modify data from this host.
- In a medium level of security, the asset owner and the administrator of the domain both have access to the asset.
- In the lowest level of security, any principal can access any asset in the domain.

Identifying Your Backup Environment Type

After you have identified the assets and principals involved in your administrative domain, you can characterize the type of environment in which you are deploying the domain. The type of environment partially determines which security model to use.

The following criteria partially distinguish types of network environments:

- Scale

  The number of assets and principals associated with a domain plays an important role in domain security. A network that includes 1000 hosts and 2000 users has more points of entry for an attacker than a network of 5 hosts and 2 users.

- Sensitivity of data

  The sensitivity of data is measured by how dangerous it would be for the data to be accessed by a malicious user. For example, the home directory on a rank-and-file corporate employee's host is presumably less sensitive than a credit card company's subscriber data.

- Isolation of communication medium

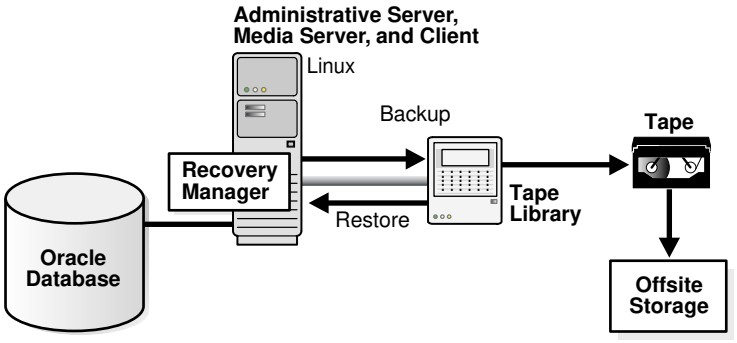
  The security of a network is contingent on the accessibility of network communications among hosts and devices in the domain. A private, corporate data center is more isolated in this sense than an entire corporate network.

The following sections describe types of network environments in which Oracle Secure Backup administrative domains are typically deployed. The sections also describe the security model typical for each environment.

Single System

The most basic administrative domain is illustrated in Figure 9-1. It consists of an administrative server, media server, and client on a single host.

Figure 9-1 Administrative Domain with One Host



This type of environment is small and isolated from the wider network. The data in this network type is probably on the low end of the sensitivity range. For example, the domain might consist of a server used to host personal Web sites within a corporate network.

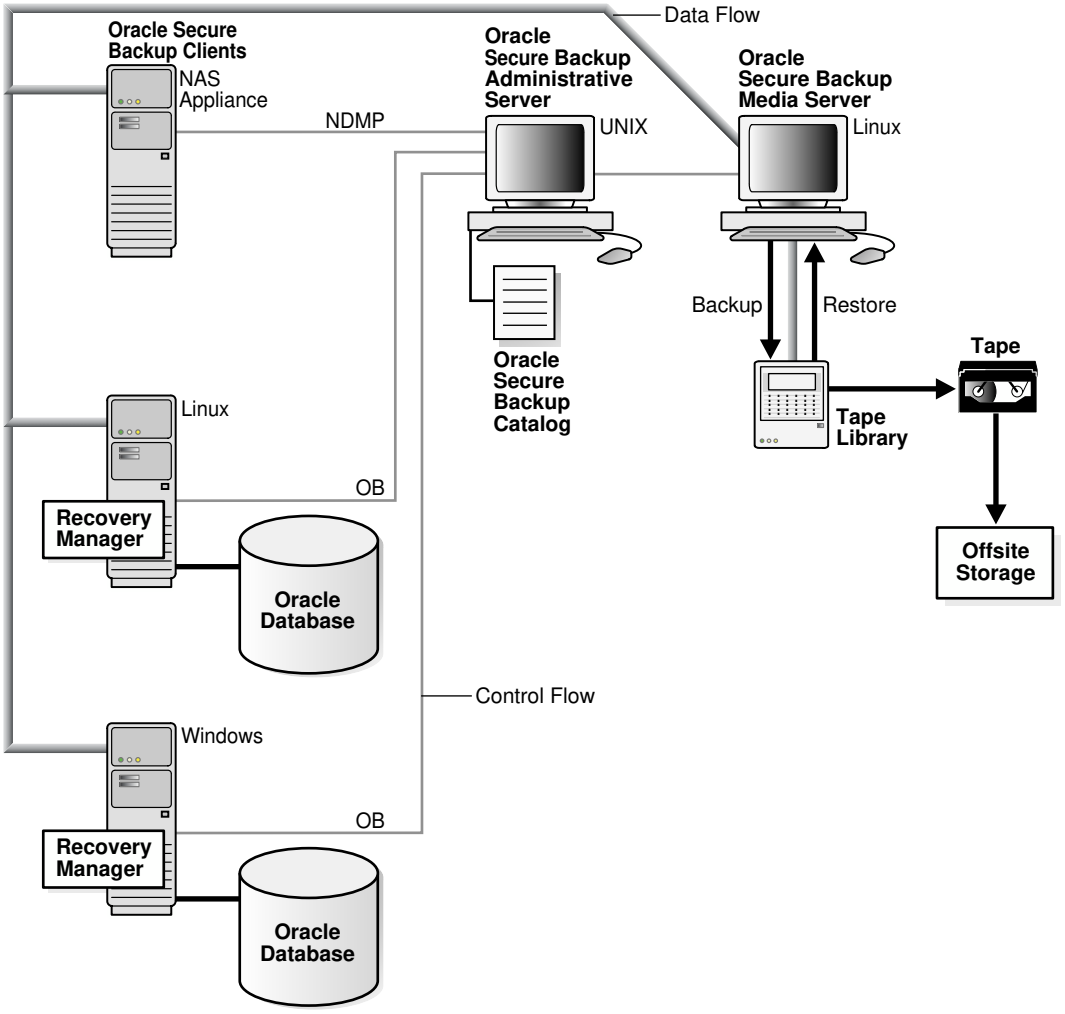
The assets include only a host and a tape device. The users probably include only the backup administrator and system administrator, who might be the same person. The backup administrator is the administrative user of the Oracle Secure Backup domain and is in charge of backups on the domain. The system administrator manages the hosts, tape devices, and networks used by the domain.

In this network type, the domain is fairly secure because it has one isolated host accessed by only a few trusted users. The administrator of the domain would probably not make security administration a primary concern, and the backup administrator could reasonably expect almost no overhead for maintaining and administering security in the Oracle Secure Backup domain.

Data Center

The administrative domain illustrated in Figure 9-2 is of medium size and is deployed in a secure environment such as a data center.

Figure 9-2 Administrative Domain with Multiple Hosts



The number of hosts, devices, and users in the administrative domain is much larger than in the single system network type, but it is still a small subset of the network at large. The data in this network type is probably on the high end of the sensitivity range. An example could be a network of hosts used to store confidential employee data. Network backups are conducted on a separate, secure, dedicated network.

The assets are physically secure computers in a dedicated network. The administrative domain could potentially include a dozen media server hosts that service the backups of a few hundred databases and file systems.

Principals include the following users:

- The backup administrator accesses the domain as an Oracle Secure Backup administrative user.
- The system administrator administers the computers, devices, and network.
- Database administrators can access their own databases and possibly have physical access to their database computers.
- Host administrators can access their file systems and possibly have physical access to their computers.

As with the single system network type, the administrative domain exists in a network environment that is secure. Administrators secure each host, tape device, and tapes by external means. Active attacks by a hacker are not likely. Administrators assume that security maintenance and administration for the domain requires almost no overhead. Backup and system administrators are primarily concerned with whether Oracle Secure Backup moves data between hosts efficiently.

Corporate Network

In this environment, multiple administrative domains, multiple media server hosts, and numerous client hosts exist in a corporate network.

The number of hosts, devices, and users in the administrative domains is extremely large. Data backed up includes both highly sensitive data such as human resources information and less sensitive data such as the home directories of low-level employees. Backups probably occur on the same corporate network used for e-mail, and Internet access. The corporate network is protected by a firewall from the broader Internet.

The assets include basically every piece of data and every computer in the corporation. Each administrative domain can have multiple users. Some host owners can have their own Oracle Secure Backup account to initiate a restore of their file systems or databases.

The security requirements for this backup environment are different from the single system and data center examples. Given the scope and distribution of the network, compromised client hosts are highly likely. For example, someone could steal a laptop used on a business trip. Malicious employees could illicitly log in to computers or run tcpdump or similar utilities to listen to network traffic.

The compromise of a client host must not compromise an entire administrative domain. A malicious user on a compromised computer must not be able to access data that was backed up by other users on other hosts. This user must also not be able to affect normal operation of the other hosts in the administrative domain.

Security administration and performance overhead is expected. Owners of sensitive assets must encrypt their backups, so physical access to backup media does not reveal the backup contents. The encryption and decryption must be performed on the client host itself, so sensitive data never leaves the host in unencrypted form.

> **Note:**
>
> Oracle Secure Backup offers an optional and highly configurable backup encryption mechanism that ensures that data stored on tape is safe from prying eyes. Backup encryption is fully integrated with Oracle Secure Backup and is ready to use as soon as Oracle Secure Backup is installed. Backup encryption applies to both file-system data and Recovery Manager (RMAN) generated backups.

Choosing Secure Hosts for the Administrative and Media Servers

Your primary task when configuring security for your domain is providing physical and network security for your hosts and determining which hosts should perform the administrative server and media server roles.

When choosing administrative and media servers, remember that a host should only be an administrative or media server if it is protected by both physical and network security. For example, a host in a data center could be a candidate for an administrative server because it presumably belongs to a private, secured network accessible to a few trusted administrators.

Oracle Secure Backup cannot itself provide physical or network security for any host nor verify whether such security exists. For example, Oracle Secure Backup cannot stop malicious users from performing the following illicit activities:

- Physically compromising a host

  An attacker who gains physical access to a host can steal or destroy the primary or secondary storage. For example, a thief could break into an office and steal servers and tapes. Encryption can reduce some threats to data, but not all. An attacker who gains physical access to the administrative server compromises the entire administrative domain.

- Accessing the operating system of a host

  Suppose an onlooker steals a password by observing the owner of a client host entering his or her password. This malicious user could telnet to this host and delete, replace, or copy the data from primary storage. The most secure backup system in the world cannot protect data from attackers if they can access the data in its original location.

- Infiltrating or eavesdropping on the network

  Although backup software can in some instances communicate securely over insecure networks, it cannot always do so. Network security is an important part of a backup system, especially for communications based on Network Data Management Protocol (NDMP).

- Deliberately misusing an Oracle Secure Backup identity

  If a person with Oracle Secure Backup administrator rights turns malicious, then he or she can wreak havoc on the administrative domain. For example, he or she could overwrite the file system on every host in the domain. No backup software can force a person always to behave in the best interests of your organization.

Determining the Distribution Method of Host Identity Certificates

After you have analyzed your backup environment and considered how to secure it, you can decide how each host in the domain obtains its identity certificate. Oracle Secure Backup uses Secure Sockets Layer (SSL) to establish a secure and trusted communication channel between domain hosts. Each host has an identity certificate signed by the Certification

Authority (CA) that uniquely identifies this host within the domain. The identity certificate is required for authenticated SSL connections.

> **See Also:**
>
> - "Host Authentication and Communication"
> - "Certification Authority"

The administrative server of the administrative domain is the CA for the domain. After you configure the administrative server, you can create each media server and client in the domain in either of the following modes:

- automated certificate provisioning mode

  In this case, no manual administration is required. When you configure the hosts, the CA issues identity certificates to the hosts over the network.

- manual certificate provisioning mode

  In this case, you must manually import the identity certificate for each host into its wallet.

Automated mode is easier to use but is vulnerable to unlikely man-in-the-middle attacks in which an attacker steals the name of a host just before you invite it to join the domain. This attacker could use the stolen host identity to join the domain illicitly. Manual mode is more difficult to use than automated mode, but is not vulnerable to the same kinds of attacks.

In manual mode, the administrative server does not transmit identity certificate responses to the host. Instead, you must carry a copy of the signed identity certificate on physical media to the host and then use the obcm utility to import the certificate into the wallet of the host. The obcm utility verifies that the certificate request in the wallet matches the signed identity certificate. A verification failure indicates that a rogue host likely attempted to masquerade as the host. You can reissue the `mkhost` command after the rogue host has been eliminated from the network.

> **See Also:**
>
> - "Managing Certificates with obcm"
> - *Oracle Secure Backup Reference* for more information on the obcm utility

If you are considering manual certificate provisioning modes, then you must decide if the extra protection provided is worth the administrative overhead. Automated mode is safe in the single system and data center environments, because network communications are usually isolated.

Automated mode is also safe in the vast majority of corporate network cases. The corporate network is vulnerable to man-in-the-middle attacks only if attackers can insert themselves into the network between the administrative server and the host being added. This is the only place they can intercept network traffic and act as the man in the middle. This is difficult without the assistance of a rogue employee.

Manual certificate provisioning mode is recommended if the host being added is outside the corporate network, because communications with off-site hosts offer more interception and diversion opportunities.

Trusted Hosts

Starting with Oracle Secure Backup release 10.3 certain hosts in the administrative domain are assumed to have a higher level of security, and are treated as having an implicit level of trust. These hosts are the administrative server and each media server. These hosts are classified by Oracle Secure Backup as *trusted hosts*. Hosts configured with only the client role are classified as *non-trusted hosts*.

> **See Also:**
>
> "Choosing Secure Hosts for the Administrative and Media Servers"

Many Oracle Secure Backup operations are reserved for use by trusted hosts, and fail if performed by a non-trusted host. These operations include:

- Use of obtar commands
- Direct access to physical devices and libraries
- Access to encryption keys

This policy provides an extra level of security against attacks that might originate from a compromised client system. For example, consider an Oracle Secure Backup administrative domain with host `admin` as the administrative server, host `media` as the media server, and host `client` as the client. An Oracle Secure Backup user belonging to a class that has the `manage devices` class right attempts to run `lsvol -L` *`library_name`* in obtool. If the attempt is made on client, then it fails with an `illegal request from non-trusted host` error. The same command succeeds when attempted on `admin` or `media`.

You can turn off these trust checks by setting the Oracle Secure Backup security policy `trustedhosts` to `off`. This disables the constraints placed on non-trusted hosts.

> **Note:**
>
> Commands that originate from the Oracle Secure Backup Web tool are always routed to the administrative server for processing, and are not affected by the `trustedhosts` policy.

Host Authentication and Communication

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

> **Note:**
>
> Currently, the Network Data Management Protocol (NDMP) does not support an SSL connection to a filer.

You can validate the authenticity of your domain by using the `obtool -authenticate` command. This command invokes obtool and requests for the domain credentials, before executing a command.

This section contains these topics:

- Identity Certificates and Public Key Cryptography
- Authenticated SSL Connections
- Certification Authority
- Oracle Wallet
- Web Server Authentication
- Revoking a Host Identity Certificate

Identity Certificates and Public Key Cryptography

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

- A public key
- The identity of the host
- What the host is authorized to do

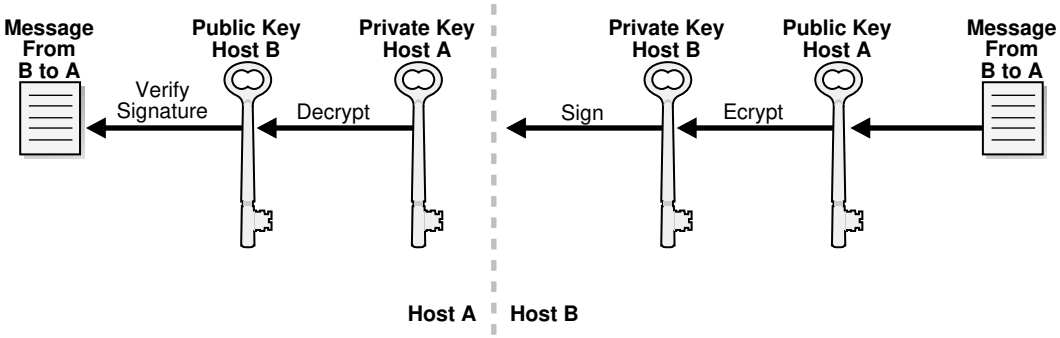
Every host in the domain, including the administrative server, has a private key known only to that host that is stored with the host's identity certificate. This private key corresponds to a public key that is made available to other hosts in the administrative domain.

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

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

Figure 9-3 illustrates how host B can encrypt and sign a message to host A, which can in turn decrypt the message and verify the signature.

Figure 9-3 Using Public and Private Keys to Encrypt and Sign Messages



Authenticated SSL Connections

For hosts to securely exchange control messages and backup data within the domain, they must first authenticate themselves to one another. Host connections are always two-way authenticated except for the initial host invitation to join a domain and communication with Network Data Management Protocol (NDMP) servers.

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

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

Certification Authority

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

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

For more information on managing CA, see Managing Certificates with obcm.

Automated and Manual Certificate Provisioning Mode

Oracle Secure Backup provides automated and manual modes for initializing the security credentials for a client host that wants to join the domain. The automated mode is easy to use, but it has potential security vulnerabilities. The manual mode is harder to use, but it is less vulnerable to tampering.

In automated certificate provisioning mode, which is the default, adding a host to the domain is transparent. The host generates a public key/private key pair and then sends a certificate

request, which includes the public key, to the Certification Authority (CA). The CA issues the host an identity certificate, which it sends to the host along with any certificates required to establish a chain of trust to the CA.

The communication between the two hosts is over a secure but non-authenticated Secure Sockets Layer (SSL) connection. It is conceivable that a rogue host could insert itself into the network between the CA and the host, thereby masquerading as the legitimate host and illegally entering the domain.

In manual certificate provisioning mode, the CA does not automatically transmit certificate responses to the host.

To transfer the certificate:

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

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

Oracle Wallet

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

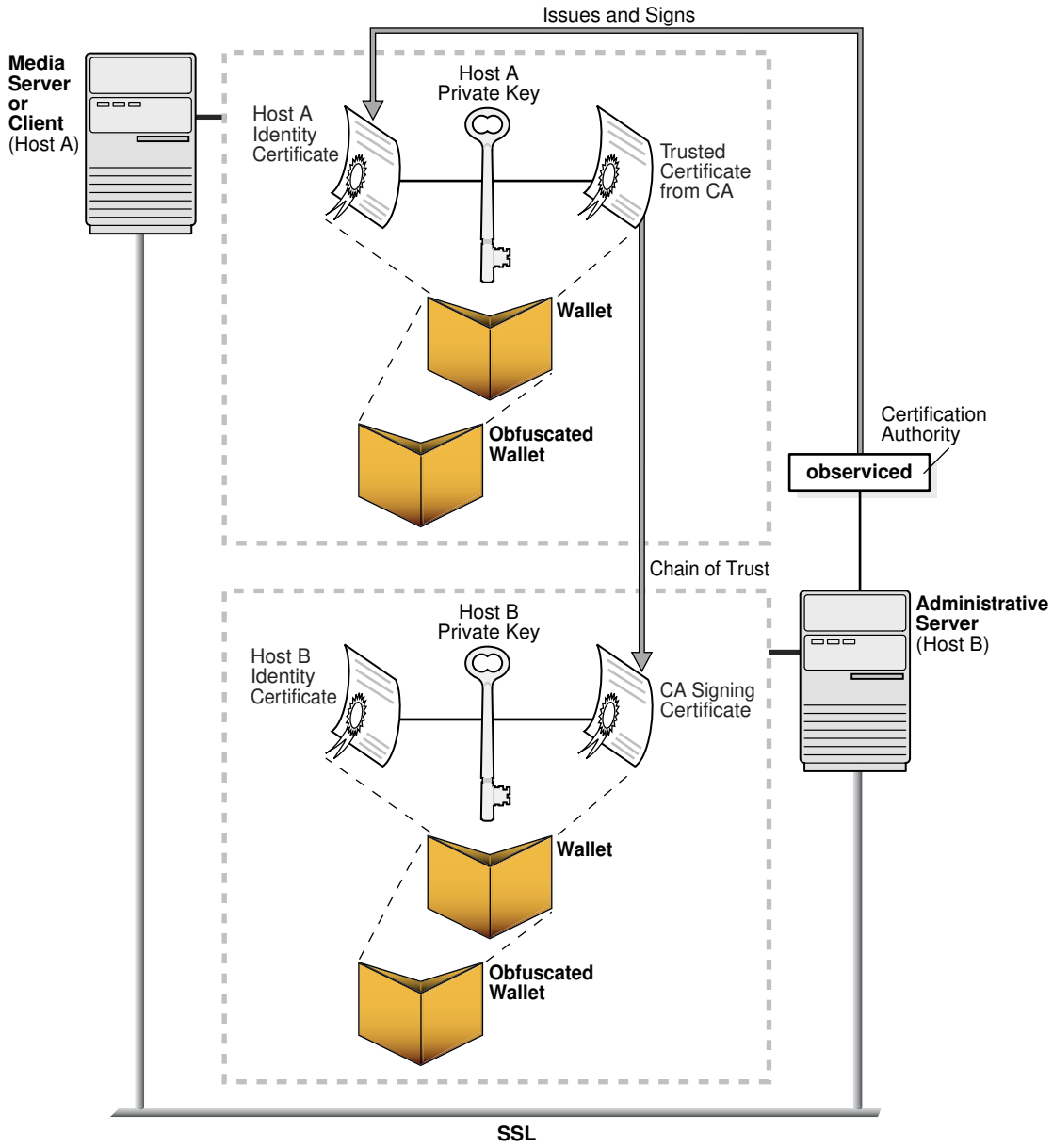
Besides maintaining its password-protected wallet, each host in the domain maintains an obfuscated wallet. This version of the wallet does not require a password. The obfuscated wallet, which is scrambled but not encrypted, enables the Oracle Secure Backup software to run without requiring a password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

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

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

Figure 9-4 illustrates the relationship between the certificate authority and other hosts in the domain.

Figure 9-4 Oracle Wallets



Oracle Secure Backup Encryption Wallet

The administrative server has a second wallet that is used to store the master keys that encrypt secure data, such as the passwords for Network Data Management Protocol (NDMP) servers and the backup encryption key store. This wallet is separate from the wallet used for a host identity certificate. The key wallet is named `ewallet.p12` and is located in *`OSB_HOME`*`/admin/encryption/wallet`.

It is a best practice to use Oracle Secure Backup catalog recovery to back up the wallet.

If you do not use Oracle Secure Backup catalog recovery to back up the wallet, then Oracle recommends that the ewallet.p12 encryption wallet not be backed up on the same media as encrypted data. Encryption wallets are not excluded from backup operations automatically. You must use the `exclude` dataset statement to specify what files to skip during a backup:

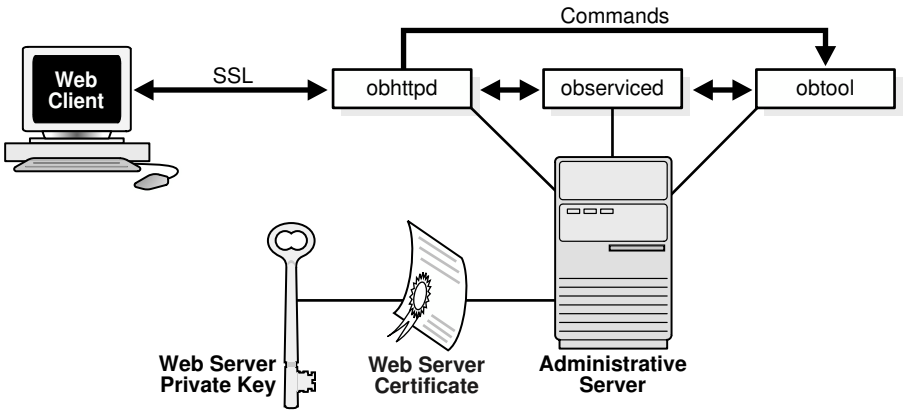
```
exclude name *.p12
```

Web Server Authentication

The Apache Web server for the administrative domain runs on the administrative server as the obhttpd daemon. When you issue commands through the Oracle Secure Backup Web tool, obhttpd repackages them as obtool commands and passes them to an instance of `obtool` running on the administrative server.

The Web server requires a signed X.509 certificate and associated public key/private key pair to establish an Secure Sockets Layer (SSL) connection with a client Web browser. The X.509 certificate for the Web server is self-signed when you install Oracle Secure Backup on the administrative server. Figure 9-5 shows the interaction between Web server and client.

Figure 9-5 Web Server Authentication



The X.509 certificate and keys for the Web server are stored separately from the Oracle Secure Backup authentication keys. When the Web server starts, it obtains the password by using a mechanism specified in the Web server configuration file. This password is never transmitted over the network. When you access the Oracle Secure Backup Web tool, if the browser does not display a warning that the certificate is not trusted, or if the browser reports unable to connect or can't find the page, the web certificates may have expired. To renew the web certificates, open a command prompt and run `obwebcert upgrade`, then follow the instructions on your command prompt.

Revoking a Host Identity Certificate

Revoking a host identity certificate is an extreme measure that would only be performed if the backup administrator determined that the security of a computer in the Oracle Secure Backup administrative domain had been breached in some way.

You can revoke a host identity certificate with the `revhost` command in obtool.

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

If you revoke a host identity certificate, then none of the Oracle Secure Backup service daemons accept connections from that host. Revocation is not reversible. If you revoke a host identity certificate and then change your mind, then you must reinstall the Oracle Secure Backup software on the affected host.

Encryption of Data in Transit

Figure 1-2 illustrates the control flow and data flow within an administrative domain. Control messages exchanged by hosts in the administrative domain are encrypted by Secure Sockets Layer (SSL).

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

File-system backups and unencrypted RMAN backups on tape (data at rest) can be encrypted by Oracle Secure Backup. RMAN-encrypted backups made through the Oracle Secure Backup SBT interface are supported, but the encryption is provided by RMAN before the backup is provided to the SBT interface. The Oracle Secure Backup SBT interface is the only supported interface for making encrypted RMAN backups directly to tape.

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* for more information on Oracle Secure Backup encryption

If you have selected RMAN or Oracle Secure Backup encryption, then Oracle Secure Backup does not apply additional encryption to data in transit within an administrative domain. If you have not selected either RMAN encryption or Oracle Secure Backup encryption, then backup data in transit, both file-system and database data, is not encrypted through SSL by default. To improve security, you can enable encryption for data in transit within the administrative domain with the `encryptdataintransit` security policy.

To enable backup encryption in the `encryptdataintransmit` security policy:

1. Log in to obtool as a user with the `modify administrative domain's configuration` right.
2. Use the `setp` command to switch the `encryptdataintransit` policy to `no`, as shown in the following example:

```
ob> cdp security
ob> setp encryptdataintransit yes
```

> **See Also:**
>
> *Oracle Secure Backup Reference* for more information on the `encryptdataintransit` security policy

Suppose you want to back up data on client host client_host to a tape drive attached to media server media_server. Data encryption depends on what encryption options you choose and on what you are backing up, as shown in the following examples:

- Encrypted RMAN backup of a database on client_host.

  RMAN encrypts the backup before it is provided to the SBT interface on client_host. Oracle Secure Backup transfers the RMAN-encrypted data over the network to media_server. Oracle Secure Backup does not apply additional encryption to the data as it passes over the network. After Oracle Secure Backup writes the data to tape, the data resides on tape in encrypted form.
- Unencrypted RMAN backup of a database on client_host.

  Oracle Secure Backup does not encrypt the data before transferring it over the network to media_server. After Oracle Secure Backup writes the data to tape, the data resides on tape in unencrypted form.
- Unencrypted RMAN backup of a database on client_host with `encryptdataintransit` set to `yes`.

  Oracle Secure Backup encrypts the data before transferring it over the network to media_server. The encrypted data is decrypted at media_server. After Oracle Secure Backup writes the data to tape, the data resides on tape in unencrypted form.
- Encrypted Oracle Secure Backup backup of the file system on client_host.

  Oracle Secure Backup transfers the encrypted backup data over the network to media_server. Oracle Secure Backup does not apply additional encryption to the data as it passes over the network. After Oracle Secure Backup writes the data to tape, the file-system data resides on tape in encrypted form.
- Unencrypted Oracle Secure Backup of the file system on client_host.

  Oracle Secure Backup does not encrypt the data before transferring it over the network to media_server. After Oracle Secure Backup writes the data to tape, the data resides on tape in unencrypted form.
- Unencrypted Oracle Secure Backup of the file system on client_host with `encryptdataintransit` set to `yes`.

  Oracle Secure Backup encrypts the data before transferring it over the network to media_server. The encrypted data is decrypted at media_server. After Oracle Secure Backup writes the data to tape, the data resides on tape in unencrypted form.

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

Default Security Configuration

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

- Secure Sockets Layer (SSL) is used for host authentication and message integrity.
- The CA signs and issues the identity certificate for each domain host in automated certificate provisioning mode.
- The size of the public key and private key for every host in the domain is 3072 bits.
- Host communications within the domain are encrypted by SSL.

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

You can also change the default configuration in any of the following ways:

- Disable SSL for inter-host authentication and communication by setting the `securecomms` security policy
- Transmit identity certificates in manual certificate provisioning mode
- Set the key size for a host to a value greater or less than the default of 3072 bits
- Enable encryption for backup data in transit by setting the `encryptdataintransit` security policy

Configuring Security for the Administrative Domain

This section describes how to configure security for the administrative domain.

This section contains these topics:

- Providing Certificates for Hosts in the Administrative Domain
- Setting the Size for Public and Private Keys
- Enabling and Disabling SSL for Host Authentication and Communication

Providing Certificates for Hosts in the Administrative Domain

Providing a certificate for each host in the Oracle Secure Backup administrative domain requires that you first configure the administrative server and then configure each media server and client.

Configuring the Administrative Server

If you install Oracle Secure Backup on a host and specify this host as the administrative server, then this server is the Certification Authority (CA) for the Oracle Secure Backup administrative domain. Oracle Secure Backup configures the host as the CA automatically as part of the standard installation. You are not required to take additional steps to provide a signing certificate for this server.

Oracle Secure Backup automatically creates the following items:

- A host object corresponding to the administrative server in the object repository on the administrative server.
- A wallet to contain the administrative server's certificates. The wallet resides in the directory tree of the Oracle Secure Backup home. Oracle Secure Backup uses the host ID as the wallet password.
- A request for a signing certificate in the wallet.
- A signed certificate in response to the request and stores the certificate in the wallet.
- A request for an identity certificate in the wallet.
- A signed certificate in response to the request and stores it in the wallet.
- An obfuscated wallet in the local wallet directory.

The administrative server now has the signing certificate, which it must have to sign the identity certificates for other hosts, and its identity certificate, which it must have to establish authenticated Secure Sockets Layer (SSL) connections with other hosts in the domain.

Configuring Media Servers and Clients

Oracle Secure Backup creates security credentials for a host when you use the Oracle Secure Backup Web tool or run the `mkhost` command in obtool to configure the host. The procedure differs depending on whether you add hosts in automated or manual certificate provisioning mode.

> **See Also:**
>
> "Determining the Distribution Method of Host Identity Certificates"

Automated Certificate Provisioning Mode

If you create the hosts in automated certificate provisioning mode, then you are not required to perform additional steps. Oracle Secure Backup creates the wallet, keys, and certificates for the host automatically as part of the normal host configuration.

Manual Certificate Provisioning Mode

You must use the `obcm` utility when you add hosts in the domain in manual rather than automated certificate provisioning mode. In this case, the certificate authority does not issue a signed certificate to a host over the network, so you must export the signed certificate from the administrative server, manually transfer the certificate to the newly configured host, and then import the certificate into the host's wallet.

Both an identity certificate and a wallet exist as files on the operating system. The operating system user running obcm must have write permissions in the wallet directory. By default, the wallet used by Oracle Secure Backup is located in the following locations:

- `/usr/etc/ob/wallet` (UNIX and Linux)
- `C:\Program Files\Oracle\Backup\db\wallet` (Windows)

The `obcm` utility always accesses the wallet in the preceding locations. You cannot override the default location.

If you choose to add hosts in manual certificate provisioning mode, then you must perform the following steps for each host:

1. Enter the following command to set the security policy `autocertissue` to No:

   ```
   obtool setp security/autocertissue --no
   ```

2. Log on to the administrative server.
3. Assuming that your PATH variable is set correctly, enter `obcm` at the operating system command line to start the obcm utility. The operating system user running obcm must have write permissions in the wallet directory.
4. Enter the following command, where *`hostname`* is the name of the host requesting the certificate and *`certificate_file`* is the filename of the exported request:

   ```
   export --certificate --file certificate_file --host hostname
   ```

For example, the following command exports the signed certificate for host `brhost2` to file `/tmp/brhost2_cert.f`:

```
export --certificate --file /tmp/brhost2_cert.f --host brhost2
```

5. Copy the signed identity certificate to some type of physical media and physically transfer the media to the host.
6. Log on to the host whose wallet contains the certificate.
7. Assuming that your PATH variable is set correctly, enter `obcm` at the operating system command line to start the obcm utility. The operating system user running obcm must have write permissions in the wallet directory.
8. Copy the signed identity certificate to a temporary location on the file system.
9. Enter the following command at the obcm prompt, where *`signed_certificate_file`* is the filename of the certificate:

   ```
   import --file signed_certificate_file
   ```

   Because only one Oracle Secure Backup wallet exists on the host, you are not required to specify the `--host` option. For example, the following example imports the certificate from `/tmp/brhost2_cert.f`:

   ```
   import --file /tmp/brhost2_cert.f
   ```

   The obcm utility issues an error message if the certificate being imported does not correspond to the certificate request in the wallet.
10. Remove the certificate file from its temporary location on the operating system. For example:

    ```
    rm /tmp/brhost2_cert.f
    ```
11. Enter the following command to reset the security policy:

    ```
    obtool resetp security/autocertissue
    ```

The obcm utility checks that the public key associated with the certificate for the host corresponds to the private key stored in the wallet with the certificate request. If the keys match, then the host is a member of the domain. If the keys do not match, then an attacker probably attempted to pass off their own host as the host during processing of the `mkhost` command. You can run the `mkhost` command again after the rogue host has been eliminated from the network.

Setting the Size for Public and Private Keys

As a general rule, the larger the sizes of the public key and the private key, the more secure they are. On the other hand, the smaller the key, the better the performance. The default key size for all hosts in the domain is 3072 bits. If you accept this default, then you are not required to perform any additional configuration.

Oracle Secure Backup enables you to set the key to any of the following bit values, which are listed in descending order of security:

- 4096
- 3072
- 2048
- 1024

- 768
- 512

This section contains these topics:

- Setting the Key Size During Installation
- Setting the Key Size in the certkeysize Security Policy
- Setting the Key Size in mkhost

Setting the Key Size During Installation

The key size in the security policy can be set when you install Oracle Secure Backup on the administrative server. Oracle Secure Backup uses the key size specified at installation time to set the initial value for the `certkeysize` security policy. This security policy specifies the default security key size for hosts in the domain. You can change or override this default when configuring an individual host.

The Oracle Secure Backup installer uses a default value for the key size. To modify this default value, you must configure advanced installation settings during installation.

> **See Also:**
>
> - "Identity Key Certificate Length"
> - "Specifying Advanced Settings for Linux/UNIX"
> - "Configuring Advanced Settings for Windows"

Setting the Key Size in the certkeysize Security Policy

You can change the default certificate key size security policy at any time. This change will not affect existing hosts. It will only affect new hosts added to the domain.

You can set the key size in the `certkeysize` security policy through obtool or the Oracle Secure Backup Web tool. Oracle Secure Backup uses the modified key size the next time you configure a host. You can change the `certkeysize` value at any time, but the change only applies to the next `mkhost` command.

To set the `certkeysize` security policy:

1. Log in to `obtool` as a user with the `modify administrative domain's configuration` right.
2. Set the `certkeysize` policy to the desired default value. The following example shows how to use `obtool` to set the key size to 3072 bits:

```
ob> cdp security
ob> setp certkeysize 3072
```

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* to learn how to set a policy

Setting the Key Size in mkhost

You can override the default key size for any individual host. Different hosts in the domain can have different key sizes.

You can set the key size when you use the `mkhost` command or Oracle Secure Backup Web tool to configure a host. If you specify the `--certkeysize` option on the `mkhost` command, then the specified value overrides the default certificate key size set in the security policy. The key size applies only to the newly configured host and does not affect the key size of any other current or future hosts.

Because larger key sizes require more computation time to generate the key pair than smaller key sizes, the key size setting can affect the processing time of the `mkhost` command. While the `mkhost` command is running, obtool might display a status message every 5 seconds. `obtool` displays a command prompt when the process has completed.

To set the key size in the `mkhost` command:

1. Log in to `obtool` as a user with the `modify administrative domain's configuration` right.
2. Issue the `mkhost` command to set the key size for a host. The following example sets the key size to 4096 bits when configuring client stadf56. This setting applies only to host stadf56.

```
ob> mkhost --inservice --role client --certkeysize 4096 stadf56
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
Info: waiting for host to update certification status...
ob> lshost stadf56
stadf56          client                           (via OB)    in service
```

> **See Also:**
>
> *Oracle Secure Backup Reference* to learn how to use the `mkhost` command

Enabling and Disabling SSL for Host Authentication and Communication

By default Oracle Secure Backup uses authenticated and encrypted Secure Sockets Layer (SSL) connections for all control message traffic among hosts.

You can disable SSL encryption by setting the `securecomms` security policy to `off`. Disabling SSL might improve performance, but be aware of the inherent security risks in this action.

> **See Also:**
>
> "Host Authentication and Communication"

To set the `securecomms` security policy:

1. Log in to obtool as a user with the `modify administrative domain's configuration` right.

2. Use the `setp` command to switch the `securecomms` policy to `off`, as shown in the following example:

```
ob> cdp security
ob> setp securecomms off
```

> **See Also:**
>
> *Oracle Secure Backup Administrator's Guide* to learn how to set a policy

Managing Certificates with obcm

This section explains how to use the obcm utility. You can use this utility to renew certificates in either certification mode, import certificate chains, export certificate chains, and export certificate requests.

You must use obcm when you add hosts to the domain in manual rather than automated certificate provisioning mode. In this case, the Certification Authority (CA) does not issue a signed certificate chain to a host over the network, so you must export the signed certificate chain from the administrative server, manually transfer the certificate chain to the newly configured host, and then import the certificate chain into the host's wallet.

Both an identity certificate and a wallet exist as files on the operating system. The operating system user running obcm must have write permissions in the wallet directory. By default, the wallet used by Oracle Secure Backup is located in the following locations:

- `/usr/etc/ob/wallet` (UNIX and Linux)
- `C:\Program Files\Oracle\Backup\db\wallet` (Windows)

The obcm utility always accesses the wallet in the preceding locations. You cannot override the default location.

In case of any errors, use the `obcm verifycomm` command to diagnose any connection issues in your domain and ensure that you describe the location of the obcm log file.

This section contains the following topics:

Renewing Certificates in Automated Certificate Provisioning Mode

This section lists the steps to renew the certification authority on your domain, in automated certificate provisioning mode.

From Oracle Secure Backup 12.1.0.2 and later, you can use `obcm` to renew certificates on your domain in automated certificate provisioning mode.
For more information on how to renew certificates in automated certificate provisioning mode, on Oracle Secure Backup 12.1.0.1 and 10.4 versions, see Renewing Certificates in Automated Certificate Provisioning Mode on Earlier Versions of Oracle Secure Backup

On the administrative host, complete the following steps to renew certification authority in automated certificate provisioning mode for your domain.

1. Enter the following command to temporarily disable your backup domain:

   ```
   obtool ctldameon --command suspend
   ```

2. Enter the following command to list all active jobs in your domain:

   ```
   obtool lsjobs --active
   ```

3. Once all active jobs have completed, enter the following command to regenerate the signing certificates:

   ```
   obcm recertifydomain
   ```

4. Use the following command to identify existing unauthenticated hosts:

   ```
   obtool lshost --unauthenticated
   ```

5. Complete the steps listed in Manually Authenticating Hosts to manually update unauthenticated hosts.
6. Verify that all hosts in your domain have been authenticated by repeating step 4.
7. Enter the following command to verify that you can successfully reach all hosts in your domain:

   ```
   obtool --pinghost all
   ```

8. Resume all backup operations.

   ```
   obtool ctldaemon --command resume
   ```

Renewing Certificates in Manual Certificate Provisioning Mode

This section lists the steps to renew certificates in manual certificate provisioning mode on OSB 12.1.0.2 and later.

Oracle Secure Backup 12.1.0.2 and later allow you to use `obcm` to renew certificates on your domain in manual certificate provisioning mode
For more information on renewing certification authority in manual certificate provisioning mode on Oracle Secure Backup 12.1.0.1 and 10.4 versions, see Renewing Certificates in Manual Certificate Provisioning Mode on Earlier Oracle Secure Backup Versions

On the administrative host, complete the following steps to renew certification authority in manual certificate provisioning mode for your domain.

1. Enter the following command to set the security policy to no:

   ```
   obtool setp security/autocertissue --no
   ```

2. Enter the following command to temporarily disable your domain:

```
obtool ctldaemon --command suspend
```

3. Enter the following command to list all active jobs in your domain:

   ```
   obtool lsjobs --active
   ```

4. Once all active jobs have completed, enter the following command to regenerate the signing certificate:

   ```
   obcm recertifydomain
   ```

5. Enter the following command to export signed certificates for each non-administrative host:

   ```
   obcm export --certificate --file non-admistrative hostname.cert --host non-administrative hostname
   ```

6. Make the `non-administrative host.cert` file accessible to the non-administrative host. Then, import the signed certificates on each unauthenticated host by using the following command:

   ```
   obtool import --file non-administrative host.cert
   ```

7. Restart the non-administrative host so that it picks the renewed certificates.
8. Run the following command to verify that all hosts in the domain have been authenticated:

   ```
   obtool lshost --unauthenticated
   ```

9. Verify that you can reach all hosts in your domain:

   ```
   obtool pinghost --all
   ```

10. Enter the following command to resume all backup operations:

    ```
    obtool ctldaemon --command resume
    ```

11. Enter the following command to reset the security policy:

    ```
    obtool resetp security/autocertissue
    ```

Renewing Certificates in Automated Certificate Provisioning Mode on Earlier Versions of Oracle Secure Backup

This section lists the steps for certificate renewal in automated certificate provisioning mode for OSB 10.4.x and 12.1.0.1.

This section lists the steps to renew certification authority in automated certificate provisioning mode on Oracle Secure Backup 12.1.0.1 and 10.4 versions.

To regenerate signing certificates in automated certificate provisioning mode for your domain, complete the following steps:

1. Download the latest version of `obcm`.
   For more information on `obcm`, see the *Oracle Secure Backup Reference*
2. Run the following command to temporarily disable the domain:

   ```
   obtool ctldaemon --command suspend
   ```

3. Run the following command to list all active jobs in your domain:

   ```
   obtool lsjobs --active
   ```

4. Once all active jobs have completed, remove expired signed certificates on each non-administrative host:

   ```
   obcm decertify
   ```

5. On the administrative host, log in as the `root` user.
6. Enter the following command to regenerate the signing certificate:

   ```
   obcm recertifydomain --nocomm --expire months
   ```

7. Stop and restart the `observiced` daemon.

> **See Also:**
>
> *Oracle Secure Backup Reference* for more information on `observiced` scripts

8. Run the following command to regenerate the signed certificates for each non-administrative host:

   ```
   obtool updatehost --recertify non-administrative hostname
   ```

9. Repeat step 7 on each non-administrative host.
10. Resume all host operations:

    ```
    obtool ctldaemon --command resume
    ```

11. Verify that all hosts can be reached:

    ```
    obtool pinghost --all
    ```

Renewing Certificates in Manual Provisioning Mode on Earlier Versions of Oracle Secure Backup

This section lists the steps to renew certification authority in manual provisioning mode on Oracle Secure Backup 12.1.0.1 and 10.4 versions.

This section lists the steps to renew certification authority in manual certificate provisioning mode on Oracle Secure Backup 12.1.0.1 and 10.4 versions.

To regenerate signing certificates in manualcertificate provisioning mode for your domain, complete the following steps:

1. Download the latest version of `obcm`.
   For more information on `obcm`, see the *Oracle Secure Backup Reference*
2. Run the following command to temporarily disable the domain:

   ```
   obtool ctldaemon --command suspend
   ```

3. Run the following command to list all active jobs in your domain:

   ```
   obtool lsjobs --active
   ```

4. Once all active jobs have completed, remove expired signed certificates on each non-administrative host:

   ```
   obcm recertify
   ```

5. On each non-administrative host, run the following scripts to stop and start the `observiced` daemon:

   ```
   /etc/init.d/obcerviced stop
   /etc/init.d/observiced start
   ```

6. On the administrative host, log in as the `root` user.

7. Enter the following command to regenerate the signing certificate:

   ```
   obcm recertifydomain --nocomm --expire months
   ```

8. Stop and restart the `observiced` daemon.

> **See Also:**
>
> *Oracle Secure Backup Reference* for more information on `observiced` scripts

9. Run the following command to regenerate the signed certificates for each non-administrative host:

   ```
   obtool updatehost --recertify non-administrative hostname
   ```

10. Assign the certificates using the `obcm export` and `obcm import` commands.

    For more information on exporting and importing certificates, see Exporting Signed Certificates and Importing Signed Certificates, respectively.

11. Resume all host operations:

    ```
    obtool ctldaemon --command resume
    ```

12. Verify that all hosts can be reached:

    ```
    obtool pinghost --all
    ```

Manually Authenticating Hosts After Certificate Renewal

This section describes how to authenticate unauthenticated, non-administrative hosts.

Ensure that you run the `obcm recertifydomain` command to renew certificates for your host.

To manually authenticate an unauthenticated, non-administrative hosts, complete the following steps:

1. On the unauthenticated host, remove all expired signed certificates by using the following command:

   ```
   obcm decertify
   ```

2. On the administrative host, regenerate the signed certificates by using the following command:

   ```
   obtool updatehost --recertify uncertified hostname
   ```

3. Assign the certificates by using the `obcm export` and `obcm import` commands.

   For more information on exporting and importing certificates using `obcm`, see Exporting Signed Certificates and Importing Signed Certificates, respectively.

Exporting Signed Certificates

You can use `obcm` on the administrative server to export a signed certificate chain for a newly configured host.

To export a signed certificate chain:

1. Log on to the administrative server.

2. Enter the following command, where *hostname* is the name of the host requesting the certificate and *certificate_file* is the filename of the exported request:

   ```
   obcm export --certificate --file certificate_file --host hostname
   ```

   For example, the following command exports the signed certificate chain for host brhost2 to file /tmp/brhost2_cert.f:

   ```
   obcm export --certificate --file /tmp/brhost2_cert.f --host brhost2
   ```

Importing Signed Certificate Chains

You can use obcm on the host to import a signed certificate chain into the host's wallet.

To import a signed certificate chain into the wallet of a host:

1. Log in to the host whose wallet contains the certificate.
2. Copy the signed certificate chain to a temporary location on the file system.
3. Enter the following command, where *signed_certificate_file* is the filename of the certificate:

   ```
   obcm import --file signed_certificate_file
   ```

   Because only one Oracle Secure Backup wallet exists on the host, you are not required to specify the --host option. For example, the following example imports the certificate from /tmp/brhost2_cert.f:

   ```
   obcm import --file /tmp/brhost2_cert.f
   ```

   The obcm utility issues an error message if the certificate chain being imported does not correspond to the certificate request in the wallet.
4. Remove the certificate file from its temporary location on the operating system. For example:

   ```
   rm /tmp/brhost2_cert.f
   ```

A

Oracle Secure Backup Directories and Files

This appendix explains the structure and contents of the Oracle Secure Backup directories.

This appendix contains these sections:

- Oracle Secure Backup Home Directory
- Administrative Server Files and Directories
- Media Server Files and Directories
- Client Host Files and Directories

> **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. Oracle recommends the following locations for the Oracle Secure Backup home:

- `C:\Program Files\Oracle\Backup` on Windows.
- `/usr/local/oracle/backup` on Linux and UNIX. Create this directory before you begin the Oracle Secure Backup installation.

On Windows, 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.

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 Files and Directories

An administrative server contains a set of executable and data files for each installed operating system.

This section describes the executable and data files of an administrative server.

- Table A-1
- Table A-2
- Table A-3

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/apache	Apache data
admin/config/apache/conf	Apache configuration data
admin/config/apache/logs	Apache log data
admin/config/class/	User class data
admin/config/dataset/	Datasets
admin/config/default/	Defaults and policies data
admin/config/device/	Device data
admin/config/duplication/	Duplication data
admin/config/family/	Media family data
admin/config/host/	Host data
admin/config/location/	Vaulting location data
admin/config/rotation/	Volume rotation data
admin/config/schedule/	Backup schedules
admin/config/summary/	Summary data
admin/config/user/	User data
admin/encryption/	Encryption data
admin/encryption/keys/	Keys used in encryption
admin/encryption/wallet/	Wallet used in encryption
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/*host_name*/	Backup catalog for *host_name*
admin/log/	Generated log files
admin/log/device/	Log files for devices
admin/log/device/*device_name*/	Log files for *device_name*
admin/log/index/	Backup catalog manager logs
admin/log/scheduler/	Scheduler-generated logs
admin/log/scheduler/summary/	Log files for email summary reports
admin/security/ctrl	Certificate Revocation List data file
admin/state/	Dynamic state data
admin/state/device/	Device state
admin/state/device/ *device_name*/	State for *device_name*
admin/state/family/	Media family state
admin/state/family/ *media_family_name*	State for *media_family_name*

Table A-1 (Cont.) Architecture-Independent Directories and Files for an Administrative Server

Directory or File	Description
admin/state/general/	Miscellaneous state
admin/state/host/	Host state
admin/state/host/*host_name*/	State for *host_name*
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
bin/	Executable or links to executable: • In an installation on a Windows operating system, this directory contains the executable for the Windows operating system. • In an installation on a Linux or UNIX operating system, this directory contains links to the executable for the operating system.
device/	Device tables
help/	Oracle Secure Backup help files
samples/	Sample tools for scripting with Oracle Secure Backup
install/	Installation data and scripts
install/common	Installation common scripts
install/configuration	Installation configuration scripts
install/data	Installation data files
install/main	Installation main scripts

Table A-2 Directories of Administrative Server on Windows

Directory	Description
db\xcr\	Transcripts for jobs that ran on this host
db\.hostid	Identifying information for this host

Table A-2 (Cont.) Directories of Administrative Server on Windows

Directory	Description
db\wallet	Security credentials for this host
temp\	Log file for observiced and temporary files

Table A-3 Files and Directories of Administrative Server on Linux and UNIX

Directory or File	Description
.bin.*executable*/	Executable for *operating_system*, where *operating_system* is a derivative of the operating system name. For example, the directory for Sun Solaris is .bin.solaris.
.drv.*device_drivers*/	Device drivers for *operating_system*
etc/	Architecture-independent executable for daemons and maintenance tools
install/	Installation programs
lib/	Architecture-independent shared library for the system backup to tape (SBT) interface
/usr/etc/ob/.hostid	Identifying information for this host
/usr/etc/ob/wallet	Security credentials for this host
/usr/etc/ob/xcr/	Transcripts for jobs that ran on this host
/usr/tmp/	Log files for installation, uninstallation, observiced files, obndmpd files, and temporary files

Media Server Files and Directories

Every media server contains a subset of the files and directories of an administrative server. It contains files that are pertinent to the computer architecture of the server and its function as a media server and client.

This section describes the files and directories of a media server.

- Table A-4
- Table A-5
- Table A-6

Table A-4 Architecture-Independent Directories for a Media Server

Directory	Description
bin/	Executable or links to executable: • In an installation on a Windows operating system, this directory contains the executable for the Windows operating system. • In an installation on a Linux or UNIX operating system, this directory contains links to the executable for the operating system.
device/	Device tables
install/	Installation data and scripts

Table A-5 Directories of Media Server on Windows

Directory	Description
drv\	Device driver
help\	Oracle Secure Backup help files
temp\	Log file for observiced and temporary files
db\.hostid	Identifying information for this host
db\wallet	Security credentials for this host

Table A-6 Files and Directories of Media Server on Linux and UNIX

Directory or File	Description
.bin.*executable*/	Executable for *operating_system*, where *operating_system* is a derivative of the operating system name. For example, the directory for Sun Solaris is .bin.solaris.
.drv.*device_drivers*/	Device drivers for *operating_system*
etc/	Architecture-independent executable for daemons and maintenance tools
/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 installation, uninstallation, observiced files, obndmpd files, and temporary files

Client Host Files and Directories

Every host system that is designated as a client contains files and directories required for Oracle Secure Backup operations.

This section describes the files and directories of a client host.

- Table A-7
- Table A-8
- Table A-9

Table A-7 Architecture-Independent Directory for a Client Host

Directory	Description
bin/	Executable or links to executable • In an installation on a Windows operating system, this directory contains the executable for the Windows operating system. • In an installation on a Linux or UNIX operating system, this directory contains links to the executable for the operating system.
install/	Installation data and scripts

Table A-8 Files and Directories on a Windows Client

Directory	Description
db\.hostid	Identifying information for this host
db\wallet	Security credentials for this host.
temp\	Log file for observiced and temporary files
help\	Oracle Secure Backup help files

Table A-9 Files and Directories on a Linux or UNIX Client

Directory or File	Description
.bin.*executable*/	Executable for *operating_system*, where *operating_system* is a derivative of the operating system name. For example, the directory for Sun Solaris is .bin.solaris.
etc/	Architecture-independent executable for daemons and maintenance tools
/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 installation, uninstallation, observiced files, obndmpd files, and temporary files

B

Determining Linux SCSI Parameters

For the Linux and UNIX platforms, if you do not know the SCSI parameters of a tape device, then you must determine them before you begin installation. This appendix describes procedures for determining SCSI device parameters on Linux and UNIX.

Determining SCSI Device Parameters on Linux

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

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

> **See Also:**
>
> "Configuring Devices on Linux Media Servers" for information about configuring attach points for Linux

Example B-1 shows sample output for a host called `storabck05` with two attached tape devices.

A device of type `Sequential-Access`, such as the first tape device in the list, is a tape drive. A device of type `Medium Changer`, such as the second tape device, is a tape library.

For each tape 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 `scsi`*`n`*. For example, for both tape 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 tape 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 B-1, Table B-1 summarizes the tape device information for `storabck05`.

Table B-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

Example B-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
```

C

Oracle Secure Backup and ACSLS

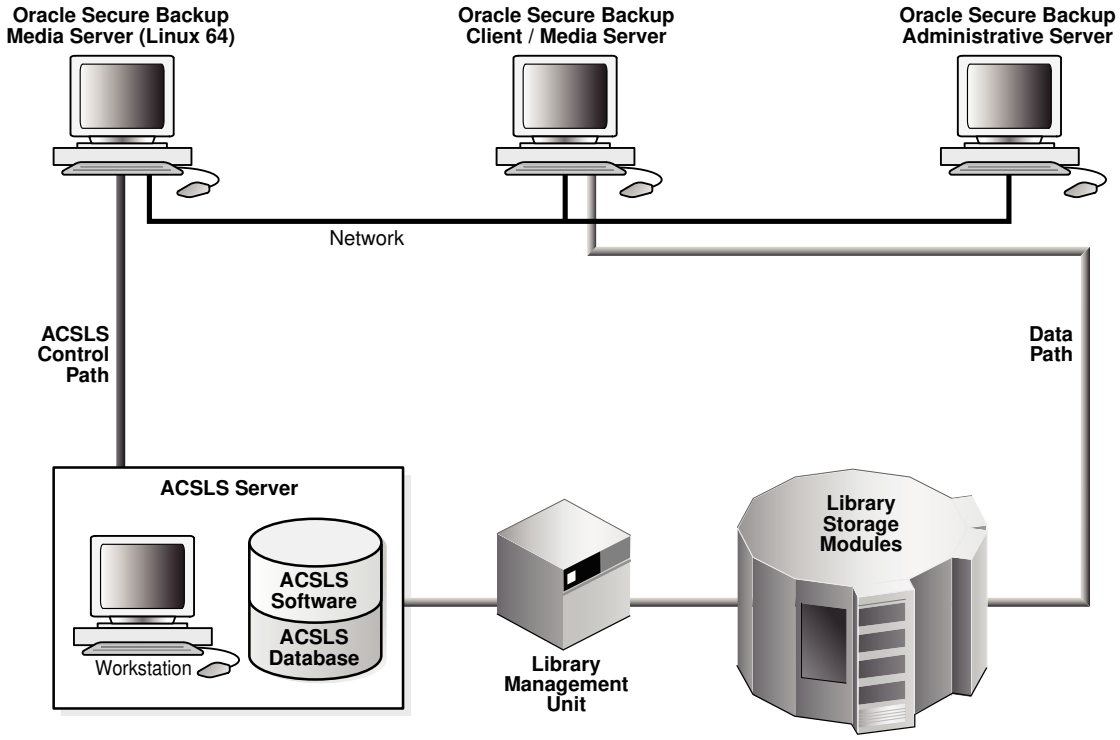
This appendix describes Oracle Secure Backup support for StorageTek Automated Cartridge System Library Software (ACSLS). ACSLS is a package of server software that controls one or more Automated Cartridge Systems tape library.

This appendix contains these sections:

About ACSLS

Figure C-1 shows how ACSLS fits into a configuration of client systems, Library Storage Modules (LSMs), and a single Library Management Unit (LMU). The LSM is hardware that has cartridge slots, a robotic arm, pass through ports, cartridge access ports, and the tape drive. The LMU is the hardware interface between the ACSLS and the LSM.

Figure C-1 Library with ACSLS Server



ACSLS offers the following advantages:

- Handles multiple libraries and multiple clients
- Manages tape drive loading and unloading
- Manages tape volume importing and exporting
- Handles mixed media types
- Optionally imposes access controls based on user ID, command, and volume ID
- Supports multiple pools of scratch tapes
- Generates inventory and configuration reports
- Manages cleaning cartridges and cleaning operations

ACSLS and Oracle Secure Backup

An ACSLS volume is called a cartridge. Cartridges are loaded and unloaded through cartridge access points. Oracle Secure Backup obtool device commands `mkdev`, `chdev`, `lsdev`, and `rmdev` have been modified to manage these cartridge access points.

> **See Also:**
>
> - "Modified Oracle Secure Backup Commands"
> - *Oracle Secure Backup Reference* for more information on `obtool` device commands

ACSLS references all of its volumes by their external barcode labels, which are required for all ACS volumes. Oracle Secure Backup continues to allow the operator to access these ACS volumes by storage element, volume label, and barcode label.

> **Note:**
>
> ACSLS supports *virtual tapes* that do not have a physical barcode attached to them. Oracle Secure Backup does not support virtual tapes within an ACS system. Oracle Secure Backup requires that all cartridges within an ACS system have properly affixed and readable barcodes.

The concept of a scratch pool in ACSLS is simply a blank tape. Once a tape has been mounted in a tape drive, its scratch pool identity is removed, and it acquires a permanent media family, identical in functionality to the pre-labeling volumes. Oracle Secure Backup supports scratch pools through an extension to the media family and retains this concept through the existing media family functionality. In addition, when a volume is force unlabeled it is moved back into the scratch pool that is assigned to the media family.

ACSLS has optional access control mechanisms on commands and volumes. This optional access control user ID can be defined as part of the `mkdev` or `chdev` commands.

Because an ACSLS system is meant to be shared by multiple clients, tape drive cleaning is managed and maintained by ACSLS.

Communicating with ACSLS

Oracle Secure Backup uses the obrobotd daemon when talking to a non-ACSLS tape library. When talking with an ACSLS tape library, Oracle Secure Backup uses two daemons named obacslibd and obacsssid. The obacslibd daemon spawns obacsssid, which is responsible for communications with the ACSLS server.

Drive Association

When you install a tape drive other than an ACS tape drive, Oracle Secure Backup requires that you attach the tape drive to a media server, install an appropriate operating system driver for the tape drive, create a device within Oracle Secure Backup, and map the operating system device to the Oracle Secure Backup device. The same steps are required for ACSLS. But you must also further define the ACSLS mapping of the tape drive through the `mkdev` or `chdev` command. The additional information required is the `acs`, `lsm`, `panel`, and `drive`.

Volume Loading and Unloading

Drive identification for mounts and dismounts is by tape drive name.

ACSLS always identifies a volume by its barcode. Because Oracle Secure Backup associates this barcode with a volume ID, you can supply either one. If a mapping is not possible, then the request is rejected with appropriate logging.

Imports and Exports

The `exportvol` command has been modified to conform to ACSLS usage. Individual ACS cartridge access port (CAP) slots are not addressable, although an entire CAP can be selected based on CAP name.

Once the request is made to eject the tape, the request does not return until the CAP has been opened, the cartridge loader emptied, and the cartridge loader reinserted in that emptied state. Because there is only one obacslibd daemon controlling each ACS tape library, no other tape library operations are permitted until the CAP is cleared. You can control how long an outstanding request waits for the CAP to be cleared with the `maxacsejectwaittime` policy.

Oracle Secure Backup does not support the `importvol` command for ACSLS tape libraries. You can use the ACSLS cmd_proc utility to enter a volume into the tape library.

Access Controls

ACSLS optionally allows fine-grained access control over the commands that a user can issue and the volumes that can be accessed. Setting up the ACSLS access controls is done at the ACSLS console. Oracle Secure Backup does not support setting, modifying, or displaying the ACSLS access controls.

If ACSLS access control is enabled, then a user must have the correct `acsls_access_id` to access the ACS device. Oracle Secure Backup maps this `acsls_access_id`, which is defined on the obtool `mkdev` or `chdev` commands, to the Oracle Secure Backup device object.

Scratch Pool Management

ACSLS enables you to define one or more scratch pools to which a blank or recycled volume can be assigned. Subsequent scratch mount requests are then restricted to volumes in the pool or pools specified with the request. Oracle Secure Backup offers equivalent functionality with an optional scratch pool ID for media family objects.

When a volume is pulled from the scratch pool, Oracle Secure Backup automatically labels the volume with a permanent media family when its volume header is written. You are not required to label volumes with the `labelvol` command beforehand. This ensure that separation of tapes within the tape libraries is persistent.

When an `unlabelvol` operation is performed, the tape is put back into the scratch pool that is defined within the current definition of the media family.

Oracle Secure Backup does not support creating scratch pools, entering cartridges into a scratch pool, or removing cartridges from a scratch pool. These operations must be performed at the ACSLS console.

Modified Oracle Secure Backup Commands

The following Oracle Secure Backup commands are modified for ACSLS tape libraries:

- mkdev
- chdev
- lsdev
- exportvol
- mkmf
- chmf

> **See Also:**
>
> *Oracle Secure Backup Reference* for syntax and semantics for device, library, and media family commands

Unsupported Oracle Secure Backup Commands

The following Oracle Secure Backup commands are not supported for ACSLS tape libraries:

- `importvol`
- `extractvol`
- `insertvol`
- `clean`
- `opendoor`
- `closedoor`

Installation and Configuration

The Oracle Secure Backup media server attached to the ACSLS server must either be a Linux x86-64 bit media server.

Oracle Secure Backup installation assumes that the ACSLS hardware and software has been correctly installed and configured. Oracle Secure Backup installation procedures do not attempt to create or modify any ACSLS configuration files.

Oracle Secure Backup handles ACS tape devices no differently from other devices. The Oracle Secure Backup device driver (if any) is installed, and special device files are created. The data path is controlled solely by Oracle Secure Backup. ACSLS is not involved.

creating Oracle Secure Backup objects for ACSLS devices is performed with the `mkdev` command in obtool with the following modifications:

- For ACSLS tape libraries, the usual host:devname attach point is replaced with information identifying the `acs` of the tape library and the host name and port where the associated ACS software is listening. A barcode reader is assumed, and barcodes are required.

- For each tape drive contained within an ACSLS tape library, you must specify `acs`, `lsm`, `panel`, and `drive`. The `acs` is obtained from the tape library in which the tape drive is contained.

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

D

Oracle Secure Backup and Reliable Datagram Socket (RDS)

This appendix discusses Oracle Secure Backup support for Reliable Datagram Socket (RDS). It also describes how to use RDS for communication between a client and media server.

Overview of Reliable Datagram Socket (RDS)

Reliable Datagram Socket (RDS) is an open source protocol that is used for communication over Infiniband. RDS provides a high-performance and low latency connectionless protocol for communication. It minimizes CPU utilization and is therefore preferred for communication over Infiniband.

Remote Direct Access Memory (RDMA) is a zero-copy extension of RDS. When an application performs an RDMA read or write, the application data is delivered directly to the network, thus reducing latency & enabling fast transfer. Therefore, RDMA provides high throughput. RDMA, when available, can be used with RDS for communication over Infiniband.

Using Reliable Datagram Socket (RDS) Protocol over Infiniband for Data Transfer in Oracle Secure Backup

Starting with Oracle Secure Backup 10.4, you can use the Reliable Datagram Socket (RDS) protocol over Infiniband to transfer data between a client and media server. You can also use Remote Direct Memory Access (RDMA) with RDS, thus maximizing the benefits of using RDS over Infiniband. Wherever it is possible, Oracle Secure Backup uses RDS with RDMA. When you set up an Infiniband network between a client and media server, Oracle Secure Backup automatically uses RDS to transfer data between them. If RDS is not enabled, then Oracle Secure Backup uses TCP/IP for interhost communication.

> **Note:**
>
> Oracle Secure Backup supports RDS over Infiniband for the Linux and Solaris x86 platforms. Starting with Oracle Secure Backup 10.4.0.2, RDS over Infiniband is also supported for SPARC 11.

To transfer data using RDS, both the client and media server must use Infiniband. Additionally, RDS support must be available for the operating system used by the client and media server. If the operating system does not support RDS, Oracle Secure Backup reverts to TCP/IP over Infiniband for the data transfer.

You can also set up a Preferred Network Interface (PNI) on the media server that points to the Infiniband connection.

> **See Also:**
>
> "Configuring Preferred Network Interfaces (PNI)" for information about PNI

Enabling RDS for Interhost Communication

When an Infiniband connection is set up between a client and a media server, Oracle Secure Backup automatically uses RDS to transfer data between the client and media server. However, you can control the usage of RDS either at the administrative domain level or at the host level. The setting made at the host level takes precedence over the setting made at the administrative-level domain level.

Enabling RDS for the Administrative Domain

You can specify if RDS must be used for data communication between a client and media server by using one of the following interfaces:

- `obtool`

  To specify that RDS must be used for data communication, ensure that the Operations policy `disablerds` is set to `no`. This setting is applicable to the entire administrative domain. The default setting for the `disablerds` policy is `no`.

  > **See Also:**
  >
  > *Oracle Secure Backup Reference* for information about the `disablerds` operations policy

- Oracle Secure Backup Web tool

  In the Configure: Defaults and Policies page, select **operations** under the Policy column. On the Configure: Defaults and Policies > Operations page, ensure that the value in the Disable RDS field is set to **no** for RDS to be used.

Enabling RDS at the Host Level

For a particular host, you can specify the use of RDS by using one of the following interfaces:

- `obtool`

  To modify an existing host and enable the use of RDS for data transfer, set the `disablerds` option of the `chhost` command to `no`. During the initial configuration of a host, you can specify that RDS must be used for data transfer by setting the `disablerds` option of the `mkhost` command to `no`.

  The values you can set for the `disablerds` option are `yes`, `no`, or `systemdefault`. The default value is `systemdefault`.

  > **See Also:**
  >
  > *Oracle Secure Backup Reference* for information about the `disablerds` option

- Oracle Secure Backup Web tool

  Use the Disable RDS field in the Configure: Defaults and Policies > Operations page to specify the use of RDS for a particular host. To use RDS for data transfer, ensure that the Disable RDS field is set to **no**.

  The values you can select for the Disable RDS field are yes, no, or systemdefault and the default value in this field is systemdefault.

> **See Also:**
>
> "Adding a Host to the Administrative Domain" for information about disabling the use of RDS for a particular host

Glossary

active location

A location in a tape library or tape drive.

administrative domain

A group of computers on your network that you manage as a common unit to perform backup and restore operations. An administrative domain must include one and only one administrative server. It can include the following:

- One or more clients
- One or more media servers

An administrative domain can consist of a single host that assumes the roles of administrative server, media server, and client.

administrative server

The host that stores configuration information and catalog files for hosts in the administrative domain. There must be one and only one administrative server for each administrative domain. One administrative server can service all clients on your network. The administrative server runs the scheduler, which starts and monitors backups within the administrative domain.

Apache Web server

A public-domain Web server used by the Oracle Secure Backup Web tool.

attachment

The physical or logical connection (the path in which data travels) of a tape device to a host in the administrative domain.

automated certificate provisioning mode

A mode of certificate management in which the Certification Authority (CA) signs and then transfers identity certificates to hosts over the network. This mode of issuing certificates is vulnerable to a possible, although extremely unlikely, man-in-the-middle attack. Automated mode contrasts with manual certificate provisioning mode.

backup container

The physical storage media on which a backup is stored. Backup containers can be tape devices or disk pools.

backup encryption

The process of obscuring backup data so that it is unusable unless decrypted. Data can be encrypted at rest, in transit, or both.

backup ID

An integer that uniquely identifies a backup section.

backup image

The product of a backup operation. It stores metadata about the backup. This includes information that is independent of the storage medium on which the backup is created such as the backup time, host name, backup level, and type of backup.

backup image instance

A backup image instance consists of the actual data that is backed up. A single backup image instance can span multiple volumes in a volume set. The part of a backup image that fits on a single volume is called a backup section.

backup image file

The logical container of a backup image. A backup image consists of one file. One backup image consists of one or more backup sections.

backup job

A backup that is eligible for execution by the Oracle Secure Backup scheduler. A backup job contrasts with a backup request, which is an on-demand backup that has not yet been forwarded to the scheduler with the `backup --go` command.

backup level

The level of an incremental backup of file-system data. Oracle Secure Backup supports 9 different incremental backup levels for file-system backup.

backup piece

A backup file generated by Recovery Manager (RMAN). A backup piece is stored in a logical container called a backup set.

backup request

An on-demand backup that is held locally in obtool until you run the `backup` command with the `--go` option. At this point Oracle Secure Backup forwards the requests to the scheduler, at which time each backup request becomes a backup job and is eligible to run.

backup schedule

A description of when and how often Oracle Secure Backup should back up the files specified by a dataset. The backup schedule contains the names of each dataset file and the name of the media family to use. The part of the schedule called the trigger defines the days and times when the backups should occur. In obtool, you create a backup schedule with the `mksched` command.

backup section

A portion of an backup image file that exists on a single tape. One backup image can contain one or more backup sections. Each backup section is uniquely identified by a backup ID.

backup transcript

A file that contains the standard output from a particular backup dispatched by the Oracle Secure Backup scheduler.

backup window

A time frame in which a backup operation can be run.

barcode

A symbol code, also called a tag, that is physically applied to a volume for identification purposes. Oracle Secure Backup supports the use of tape libraries that have an automated means to read barcodes.

blocking factor

The number of 512-byte blocks to include in each block of data written to each tape drive. By default, Oracle Secure Backup writes 64K blocks to tape, which is a blocking factor of 128. Because higher blocking factors usually result in better performance, you can try a blocking factor larger than the obtar default. If you pick a value larger than is supported by the operating system of the server, then Oracle Secure Backup fails with an error.

CA

See Certification Authority (CA)

catalog

A repository that records backups in an Oracle Secure Backup administrative domain. You can use the Oracle Secure Backup Web tool or obtool to browse the catalog and determine what files you have backed up. The catalog is stored on the administrative server.

certificate

A digitally signed statement from a Certification Authority (CA) stating that the public key (and possibly other information) of another entity has a value. The X.509 standard specifies the format of a certificate and the type of information contained in it: certificate version, serial number, algorithm ID, issuer, validity, subject, subject public key information, and extensions such as key usage (signing, encrypting, and so on). A variety of methods are used to encode, identify, and store the certificate.

Certification Authority (CA)

An authority in a network that performs the function of binding a public key pair to an identity. The CA certifies the binding by digitally signing a certificate that contains a representation of the identity and a corresponding public key. The administrative server is the CA for an Oracle Secure Backup administrative domain.

Certificate Revocation List (CRL)

A list used in a public key infrastructure that enumerates the revoked certificates maintained by the Certification Authority (CA).

class

A named set of rights for Oracle Secure Backup users. A class can have multiple users, but each user can belong to one and only one class.

client

Any computer or server whose files Oracle Secure Backup backs up or restores.

content-managed expiration policy

A volume with this type of expiration policy expires when every backup piece on the volume is marked as deleted. You can make Recovery Manager (RMAN) backups, but not file-system backups, to content-managed volumes. You can use RMAN to delete a backup piece.

cryptographic hash function

A one-way function that accepts a message as input and produces an encrypted string called a "hash" or "message digest" as output. Given the hash, it is computationally infeasible to retrieve the input. MD5 and SHA-1 are commonly used cryptographic hash functions.

cumulative incremental backup

A type of incremental backup in which Oracle Secure Backup copies only data that has changed at a lower backup level. For example, a level 3 incremental backup copies only that data that has changed since the most recent backup that is level 2 or lower.

daemons

Background processes that are assigned a task by Oracle Secure Backup during the execution of backup and restore operations. Some daemons run continually and others are started and stopped as required.

data management application (DMA)

An application that controls a backup or restore operation over the Network Data Management Protocol (NDMP) through connections to a data service and tape service. The DMA is the session master, whereas the NDMP services are the slaves. In an Oracle Secure Backup administrative domain, obtar is an example of a DMA.

data service

An application that runs on a client and provides Network Data Management Protocol (NDMP) access to database and file-system data on the primary storage system.

data transfer element (DTE)

A secondary storage device within a tape library. In tape libraries that contain multiple tape drives, data transfer elements are sequentially numbered starting with 1.

database backup storage selector

An Oracle Secure Backup configuration object that specifies characteristics of Recovery Manager (RMAN) SBT backups. The storage selector act as a layer between RMAN, which accesses the database, and the Oracle Secure Backup software, which manages the backup media.

dataset

The contents of a file-system backup. A dataset file describes a dataset. For example, you could create the dataset file my_data.ds to describe a dataset that includes the `/home` directory on host `brhost2`.

dataset directory

A directory that contains at least one dataset file. The directory groups dataset files as a set for common reference.

dataset file

A text file that describes a dataset. The Oracle Secure Backup dataset language provides a text-based means to define file-system data to back up.

defaults and policies

A set of configuration data that specifies how Oracle Secure Backup runs in an administrative domain.

device discovery

The process by which Oracle Secure Backup automatically detects devices accessed through Network Data Management Protocol (NDMP) and configuration changes for such devices.

attach point

A filename in the `/dev` file system on UNIX or Linux that represents a hardware tape device. A attach point does not specify data on disk, but identifies a hardware unit and the device driver that handles it. The inode of the file contains the device number, permissions, and ownership data. An attachment consists of a host name and the attach point name by which that device is accessed by Oracle Secure Backup.

differential incremental backup

A type of incremental backup in which Oracle Secure Backup copies only data that has changed at the same or lower backup level. This backup is also called a level 10 backup. Oracle Secure Backup does not support the level 10 backup on some platforms, including Network Attached Storage (NAS) devices such as a Network Appliance filer.

digital signature

A set of bits computed by an Certification Authority (CA) to signify the validity of specified data. The algorithm for computing the signature makes it difficult to alter the data without invalidating the signature.

disk pool

A file-system directory that stores backups. Disk pools can be accessed concurrently by multiple backup or restore jobs.

DMA

See data management application (DMA)

domain

A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

error rate

The number of recovered write errors divided by the total blocks written, multiplied by 100.

expiration policy

The means by which Oracle Secure Backup determines how a volume in a media family expires, that is, when they are eligible to be overwritten. A media family can either have a content-managed expiration policy or time-managed expiration policy.

Fiber Distributed Data Interface (FDDI)

A set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps. FDDI networks are typically used as backbones for wide-area networks.

Fibre Channel

A protocol used primarily among devices in a Storage Area Network (SAN).

file-system backup

A backup of files on the file system initiated by Oracle Secure Backup. A file-system backup is distinct from a Recovery Manager (RMAN) backup made through the Oracle Secure Backup SBT interface.

filer

A network-attached appliance that is used for data storage.

firewall

A system designed to prevent unauthorized access to or from a private network.

full backup

An operation that backs up all of the files selected on a client. Unlike in an incremental backup, files are backed up whether they have changed since the last backup or not.

heterogeneous network

A network made up of a multitude of computers, operating systems, and applications of different types from different vendors.

host authentication

The initialization phase of a connection between two hosts in the administrative domain. After the hosts authenticate themselves to each other with identity certificates, communications between the hosts are encrypted by Secure Sockets Layer (SSL). Almost all connections are two-way authenticated; exceptions include initial host invitation to join a domain and interaction with hosts that use NDMP access mode.

identity certificate

An X.509 certificate signed by the Certification Authority (CA) that uniquely identifies a host in an Oracle Secure Backup administrative domain.

incremental backup

An operation that backs up only the files on a client that changed after a previous backup. Oracle Secure Backup supports 9 different incremental backup levels for file-system backups. A cumulative incremental backup copies only data that changed since the most recent backup at a lower level. A differential incremental backup, which is equivalent to a level 10 backup, copies data that changed since an incremental backup at the same or lower level.

An incremental backup contrasts with a full backup, which always backs up all files regardless of when they last changed. A full backup is equivalent to an incremental backup at level 0.

job list

A catalog created and maintained by Oracle Secure Backup that describes past, current, and pending backup jobs.

job summary

A text file report produced by Oracle Secure Backup that describes the status of selected backup and restore jobs. Oracle Secure Backup generates the report according to a user-specified job summary schedule.

job summary schedule

A user-defined schedule for generating job summaries. You create job summary schedules with the `mksum` command in obtool.

location

A location is a place where a volume physically resides; it might be the name of a tape library, a data center, or an off-site storage facility.

logical unit number

Part of the unique identifier of a tape device. See Oracle Secure Backup logical unit number and SCSI LUN.

manual certificate provisioning mode

A mode of certificate management in which you must manually export the signed identity certificate for a host from the administrative server, transfer it to the host, and manually import the certificate into the wallet of the host. Unlike automated certificate provisioning mode, this mode is not vulnerable to a possible (if extremely unlikely) man-in-the-middle attack.

media family

A named classification of backup volumes that share the same volume sequence file, expiration policy, and write window.

media server

A computer or server that has at least one tape device connected to it. A media server is responsible for transferring data to or from the devices that are attached to it.

NAS

See Network Attached Storage (NAS)

native access mode

A synonym for primary access mode.

NDMP

See Network Data Management Protocol (NDMP)

NDMP access mode

The mode of access for a filer or other host that uses Network Data Management Protocol (NDMP) for communications within the administrative domain. NDMP access mode contrasts with primary access mode, which uses the Oracle Secure Backup network protocol. Note that Oracle Secure Backup uses NDMP for data transfer among hosts regardless of whether a host is accessed through the primary or NDMP access modes.

Network Attached Storage (NAS)

A NAS server is a computer on a network that hosts file systems. The server exposes the file systems to its clients through one or more standard protocols, most commonly Network File System (NFS) and CIFS.

Network Data Management Protocol (NDMP)

An open standard protocol that defines a common architecture for backups of heterogeneous file servers on a network. This protocol allows the creation of a common agent used by the central backup application, called a data management application (DMA), to back up servers running different operating systems. With NDMP, network congestion is minimized because the data path and control path are separated. Backup can occur locally—from a file server direct to a tape drive—while management can occur centrally.

network description file

A text file that lists the hosts in your network on which Oracle Secure Backup should be installed. For each host, you can identify the Oracle Secure Backup installation type, the host name, and each tape drive attached. The install subdirectory in the Oracle Secure Backup home includes a sample network description file named obndf.

Network File System (NFS)

A client/server application that gives all network users access to shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP. Users can manipulate shared files as if they were stored on local disk. With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

OB access mode

A synonym for primary access mode.

obfuscated wallet

A wallet whose data is scrambled into a form that is extremely difficult to read if the scrambling algorithm is unknown. The wallet is read-only and is not protected by a password. An obfuscated wallet supports single sign-on (SSO).

obtar

The underlying engine of Oracle Secure Backup that moves data to and from tape. obtar is a descendent of the original Berkeley UNIX tar(2) command.Although obtar is typically not accessed directly, you can use it to back up and restore files or directories specified on the command line. obtar enables the use of features not exposed through obtool or the Web tool.

obtool

The principal command-line interface to Oracle Secure Backup. You can use this tool to perform all Oracle Secure Backup configuration, backup and restore, maintenance, and monitoring operations. The obtool utility is an alternative to the Oracle Secure Backup Web tool.

offsite backup

A backup that is equivalent to a full backup except that it does not affect the full or incremental backup schedule. An offsite backup is useful when you want to create an backup image for offsite storage without disturbing your incremental backup schedule.

on-demand backup

A file-system backup initiated through the `backup` command in obtool or the Oracle Secure Backup Web tool. The backup is one-time-only and either runs immediately or at a specified time in the future. An on-demand backup contrasts with a scheduled backup, which is initiated by the Oracle Secure Backup scheduler.

operator

A person whose duties include backup operations, backup schedule management, tape swaps, and error checking.

Oracle Secure Backup home

The directory in which the Oracle Secure Backup software is installed. The Oracle Secure Backup home is typically `/usr/local/oracle/backup` on UNIX/Linux and `C:\Program Files\Oracle\Backup` on Windows. This directory contains binaries and configuration files. The contents of the directory differ depending on which role is assigned to the host within the administrative domain.

Oracle Secure Backup logical unit number

A number between 0 and 31 used to generate unique attach point names during device configuration (for example, `/dev/obt0`, `/dev/obt1`, and so on). Although it is not a requirement, unit numbers typically start at 0 and increment for each additional device of a given type, whether tape library or tape drive.

The Oracle Secure Backup logical unit number is part of the name of the attach point. Do not confuse it with SCSI LUN, which is part of the hardware address of the device.

Oracle Secure Backup user

An account defined within an Oracle Secure Backup administrative domain. Oracle Secure Backup users exist in a separate namespace from operating system users.

overwrite

The process of replacing a file on your system by restoring a file that has the same file name.

originating location

A location where a volume was first written.

Preferred Network Interface (PNI)

The preferred network interface for transmitting data to be backed up or restored. A network can have multiple physical connections between a client and the server performing a backup or restore on behalf of that client. For example, a network can have both Ethernet and Fiber Distributed Data Interface (FDDI) connections between a pair of hosts. PNI enables you to specify, on a client-by-client basis, which of the server's network interfaces is preferred.

preauthorization

An optional attribute of an Oracle Secure Backup user. A preauthorization gives an operating system user access to specified Oracle Secure Backup resources.

primary access mode

The mode of access for a host that uses the Oracle Secure Backup network protocol for communications within the administrative domain. Oracle Secure Backup must be installed on hosts that use primary access mode. In contrast, hosts that use NDMP access mode do not require Oracle Secure Backup to be installed. Note that Oracle Secure Backup uses Network Data Management Protocol (NDMP) for data transfer among hosts regardless of whether a host is accessed through the primary or NDMP access modes.

private key

A number that corresponds to a specific public key and is known only to the owner. Private and public keys exist in pairs in all public key cryptography systems. In a typical public key cryptosystem, such as RSA, a private key corresponds to exactly one public key. You can use private keys to compute signatures and decrypt data.

privileged backup

A file-system backup operation initiated with the `--privileged` option of the `backup` command. On UNIX and Linux systems, a privileged backup runs under the `root` user identity. On Windows systems, the backup runs under the same account (usually `Local System`) as the Oracle Secure Backup service on the Windows client.

public key

A number associated with a particular entity intended to be known by everyone who must have trusted interactions with this entity. A public key, which is used with a corresponding private key, can encrypt communication and verify signatures.

Recovery Manager (RMAN)

A utility supplied with Oracle Database used for database backup, restore, and recovery. RMAN is a separate application from Oracle Secure Backup. Unlike RMAN, you can use Oracle Secure Backup to back up any file on the file system—not just database files. Oracle Secure Backup includes an SBT interface that RMAN can use to back up database files directly to tape.

retention period

The length of time that data in a volume set is not eligible to be overwritten. The retention period is an attribute of a time-managed media family. The retention period begins at the write window close time. For example, if the write window for a media family is 7 days, then a retention period of 14 days indicates that the data is eligible to be overwritten 21 days from the first write to the first volume in the volume set.

rights

Privileges within the administrative domain that are assigned to a class. For example, the `perform backup as self` right is assigned to the `operator` class by default. Every Oracle Secure Backup user that belongs to a class is granted the rights associated with this class.

roles

The functions that hosts in your network can have during backup and restore operations. There are three roles in Oracle Secure Backup: administrative server, media server, and client. A host in your network can serve in any of these roles or any combination of them. For example, the administrative server can also be a client and media server.

SAN

See Storage Area Network (SAN)

SBT interface

A media management software library that Recovery Manager (RMAN) can use to back up to tertiary storage. An SBT interface conforms to a published API and is supplied by a media management vendor. Oracle Secure Backup includes an SBT interface for use with RMAN.

scheduled backup

A file-system backup that is scheduled through the `mksched` command in obtool or the Oracle Secure Backup Web tool (or is modified by the `runjob` command). A backup schedule

describes which files should be backed up. A trigger defined in the schedule specifies when the backup job should run.

scheduler

A daemon (obscheduled) that runs on an administrative server and is responsible for managing all backup scheduling activities. The scheduler maintains a job list of backup job operations scheduled for execution.

service daemon

A daemon (observiced) that runs on each host in the administrative domain that communicates through primary access mode. The service daemon provides a wide variety of services, including certificate operations.

SCSI

See Small Computer System Interface (SCSI)

SCSI LUN

SCSI logical unit number. A 3-bit identifier used on a SCSI bus to distinguish between up to eight devices (logical units) with the same SCSI ID. Do not confuse with Oracle Secure Backup logical unit number

Secure Sockets Layer (SSL)

A cryptographic protocol that provides secure network communication. SSL provides endpoint authentication through a certificate. Data transmitted over SSL is protected from eavesdropping, tampering or message forgery, and replay attacks.

Small Computer System Interface (SCSI)

A parallel I/O bus and protocol that permits the connection of a variety of peripherals to host computers. Connection to the SCSI bus is achieved through a host adapter and a peripheral controller.

SSL

See Secure Sockets Layer (SSL)

Storage Area Network (SAN)

A high-speed subnetwork of shared storage devices. A SAN is designed to assign data backup and restore functions to a secondary network so that they do not interfere with the functions and capabilities of the server.

storage device

A computer that contains disks for storing data.

storage element

A physical location within a tape library where a volume can be stored and retrieved by a tape library's robotic arm.

storage location

A location outside of a tape library or tape drive where a volume can be stored.

tape device

A tape drive or tape library identified by a user-defined device name.

tape drive

A tape device that reads and writes data stored on a tape. Tape drives are sequential-access, which means that they must read all preceding data to read any particular piece of data. The tape drives are accessible through various protocols, including Small Computer System Interface (SCSI) and Fibre Channel. A tape drive can exist standalone or in a tape library.

tape library

A medium changer that accepts Small Computer System Interface (SCSI) commands to move a volume from a storage element to a tape drive and back again.

tape service

A Network Data Management Protocol (NDMP) service that transfers data to and from secondary storage and allows the data management application (DMA) to manipulate and access secondary storage.

TCP/IP

Transmission Control Protocol/Internet Protocol. The suite of protocols used to connect hosts for transmitting data over networks.

three-way backup

The process of backing up an NDMP server that supports NDMP but does not have a locally attached backup device to another NDMP server that has an attached backup device. The backup is performed by sending the data through a TCP/IP connection to the NDMP server with the attached backup device. In this configuration, the NDMP data service exists on the NDMP server that contains the data to be backed up and the NDMP tape service exists on the NDMP server with the attached tape device.

time-managed expiration policy

A media family expiration policy in which every volume in a volume set can be overwritten when it reaches its volume expiration time. Oracle Secure Backup computes the volume expiration time by adding the volume creation time for the first volume in the set, the write window time, and the retention period.

For example, you set the write window for a media family to 7 days and the retention period to 14 days. Assume that Oracle Secure Backup first wrote to the first volume in the set on January 1 at noon and subsequently wrote data on 20 more volumes in the set. In this scenario, all 21 volumes in the set expire on January 22 at noon.

You can make a Recovery Manager (RMAN) backup or a file-system backup to a volume that use a time-managed expiration policy.

trigger

The part of a backup schedule that specifies the days and times at which the backups should occur.

trusted certificate

A certificate that is considered valid without validation testing. Trusted certificates build the foundation of the system of trust. Typically, they are certificates from a trusted Certification Authority (CA).

unprivileged backup

File-system backups created with the `--unprivileged` option of the `backup` command. When you create or modify an Oracle Secure Backup user, you associate operating system accounts with this user. Unprivileged backups of a host run under the operating system account associate with Oracle Secure Backup user who initiates the backup.

volume

A volume is a unit of media, such as an 8mm tape. A volume can contain multiple backup image instances.

volume creation time

The time at which Oracle Secure Backup wrote backup image file number 1 to a volume.

volume expiration time

The date and time on which a volume in a volume set expires. Oracle Secure Backup computes this time by adding the write window duration, if any, to the volume creation time for the first volume in the set, then adding the volume retention period.

For example, assume that a volume set belongs to a media family with a retention period of 14 days and a write window of 7 days. Assume that the volume creation time for the first volume in the set was January 1 at noon and that Oracle Secure Backup subsequently wrote data on

20 more volumes in the set. In this scenario, the volume expiration time for all 21 volumes in the set is January 22 at noon.

volume ID

A unique alphanumeric identifier assigned by Oracle Secure Backup to a volume when it was labeled. The volume ID usually includes the media family name of the volume, a dash, and a unique volume sequence number. For example, a volume ID in the RMAN-DEFAULT media family could be RMAN-DEFAULT-000002.

volume label

The first block of the first backup image on a volume. It contains the volume ID, the owner's name, the volume creation time, and other information.

volume sequence file

A file that contains a unique volume ID to assign when labeling a volume.

volume sequence number

A number recorded in the volume label that indicates the order of volumes in a volume set. The first volume in a set has sequence number 1. The volume ID for a volume usually includes the media family name of the volume, a dash, and a unique volume sequence number. For example, a volume ID for a volume in the RMAN-DEFAULT media family could be RMAN-DEFAULT-000002.

volume set

A group of volumes spanned by a backup image. The part of the backup image instance that fits on a single volume is a backup section.

volume tag

A field that is commonly used to hold the barcode identifier, also called a volume tag, for the volume. The volume tag is found in the volume label.

wallet

A password-protected encrypted file. An Oracle wallet is primarily designed to store X.509 certificates and their associated public key/private key pair. The contents of the wallet are only available after the wallet password has been supplied, although with an obfuscated wallet no password is required.

Web tool

The browser-based GUI that enables you to configure an administrative domain, manage backup and restore operations, and browse the backup catalog.

write window

The period for which a volume set remains open for updates, usually by appending an additional backup image. The write window opens at the volume creation time for the first volume in the set and closes after the write window period has elapsed. After the write window close time, Oracle Secure Backup does not allow further updates to the volume set until it expires (as determined by its expiration policy), or until it is relabeled, reused, unlabeled, or forcibly overwritten.

A write window is associated with a media family. All volume sets that are members of the media family remain open for updates for the same time period.

write window close time

The date and time that a volume set closes for updates. Oracle Secure Backup computes this time when it writes backup image file number 1 to the first volume in the set. If a volume set has a write window close time, then this information is located in the volume section of the volume label.

write window time

The length of time during which writing to a volume set is permitted.

Index

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X