VERITAS™

VERITAS NetBackup™ Vault 5.1

Operator's Guide

for UNIX and Windows

N12351C

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2908
www.veritas.com

Third-Party Copyrights

Contents

Preface

NetBackup Vault simplifies the processes of image duplication, off-site storage, and off-site retrieval for both storage administrators and systems operators.

This *Operator's Guide* is intended for those who operate the robots and libraries and send and retrieve volumes to and from off site storage.

What Is In This Guide?

This guide is organized as follows:

- Chapter 1, "Introduction," explains the history and design of Vault.
- Chapter 2, "Operational Procedures," describes Vault tasks usually performed by the system operations staff.
- Chapter 3, "Vault Reports," describes the content of each report and how to generate the reports.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Technical Support Web Site

The VERITAS Support Web site allows you to:

- obtain updated information about NetBackup Vault, including system requirements, supported platforms, and supported peripherals
- contact the VERITAS Technical Support staff and post questions to them
- get the latest patches, upgrades, and utilities
- view the NetBackup Vault Frequently Asked Questions (FAQ) page
- search the knowledge base for answers to technical support questions

- receive automatic notice of product updates
- find out about NetBackup Vault training
- read current white papers related to NetBackup Vault

The address for the VERITAS Technical Support Web site follows:

- http://support.veritas.com

Subscribing to VERITAS Email Notification Service

Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

Go to http://support.veritas.com. Select a product and click "E-mail Notifications" on the right side of the page. Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.

Accessing VERITAS Telephone Support

Telephone support for NetBackup Vault is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

▼ To locate the telephone support directory on the VERITAS web site

1. Open http://support.veritas.com in your web browser.

2. Click the **Phone Support** icon. A page that contains VERITAS support numbers from around the world appears.

Accessing VERITAS E-mail Support

▼ To contact support using E-mail on the VERITAS web site

1. Open http://support.veritas.com in your web browser.

2. Click the **E-mail Support** icon. A brief electronic form will appear and prompt you to:
   - Select a language of your preference
   - Select a product and a platform
   - Associate your message to an existing technical support case
   - Provide additional contact and product information, and your message

3. Click **Send Message**.

Contacting VERITAS Licensing

For license information call 1-800-634-4747 option 3, fax 1-650-527-0952, or e-mail amercustomercare@veritas.com.

NetBackup Vault Documents

The companion document to this *NetBackup Vault Operator's Guide for Unix and Windows* is the *NetBackup Vault System Administrator's Guide for Unix and Windows*, which provides detailed instructions for system administrators on using NetBackup Vault.

The following documents provided related information:

- *VERITAS NetBackup Release Notes for UNIX and Windows*

  Provides important information about NetBackup on UNIX- and Windows-based servers, such as the platforms and operating systems that are supported and operating notes that may not be in the NetBackup manuals or the online help.

- *VERITAS NetBackup Installation Guide for UNIX*

  Explains how to install NetBackup software on UNIX-based platforms.

- *VERITAS NetBackup Installation Guide for Windows*

  Explains how to install NetBackup software on Windows-based platforms. Also explains how to install PC client software, which includes UNIX systems and Mac OS 10.

If you have a UNIX server, refer to these documents:

- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I*

  Explains how to configure and manage NetBackup on a UNIX server, including managing storage units, backup policies, catalogs and host properties.

- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II*

  Explains additional NetBackup features such as notify scripts, enhanced authorization and authentication, and role-based security. The guide also discusses using NetBackup with AFS, Intelligent Disaster Recovery (IDR), and the BE Tape Reader.

- *VERITAS NetBackup Media Manager System Administrator's Guide for UNIX*

  Explains how to configure and manage the storage devices and media on UNIX servers running NetBackup. Media Manager is part of NetBackup.

- *VERITAS NetBackup Troubleshooting Guide for UNIX and Windows*

  Provides troubleshooting information for UNIX- and Windows-based NetBackup, including Media Manager.

- *VERITAS NetBackup Commands for UNIX*

  Describes NetBackup and Media Manager commands and processes that can be run from a UNIX command line.

If you have a Windows server, refer to these documents:

- *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*

  Explains how to configure and manage NetBackup on a Windows server, including managing storage units, backup policies, catalogs and host properties.

- *VERITAS NetBackup System Administrator's Guide for Windows, Volume II*

  Explains additional NetBackup features such as notify scripts, enhanced authorization and authentication, and role-based security. The guide also discusses using NetBackup with AFS, Intelligent Disaster Recovery (IDR), and the BE Tape Reader.

- *VERITAS NetBackup Media Manager System Administrator's Guide for Windows*

  Explains how to configure and manage the storage devices and media on Windows servers running NetBackup. Media Manager is part of NetBackup.

- *VERITAS NetBackup Troubleshooting Guide for UNIX and Windows*

  Provides troubleshooting information for UNIX- and Windows-based NetBackup, including Media Manager.

- *VERITAS NetBackup Commands for Windows*

  Describes NetBackup commands and processes that can be executed from a Windows command prompt.

Glossary

If you encounter unfamiliar terminology, consult the NetBackup online glossary. The glossary contains terms and definitions for NetBackup and all additional NetBackup options and agents.

The NetBackup online glossary is included in the NetBackup help file.

▼ To access the NetBackup online glossary

1. In the NetBackup Administration Console, click **Help** > **Help Topics**.

2. Click the **Contents** tab.

3. Click **Glossary of NetBackup Terms**.

Use the scroll function to navigate through the glossary.

Accessibility Features

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX, Volume I*.

Conventions

The following conventions apply throughout the documentation set.

Product-Specific Conventions

The following term is used in the NetBackup Vault 5.1 documentation to increase readability while maintaining technical accuracy.

- Microsoft Windows, Windows

  Terms used to describe a specific product or operating system developed by Microsoft, Inc. Some examples you may encounter in NetBackup documentation are, Windows servers, Windows 2000, Windows Server 2003, Windows clients, Windows platforms, or Windows GUI.

When Windows or Windows servers is used in the documentation, it refers to all of the currently supported Windows operating systems. When a specific Windows product is identified in the documentation, only that particular product is valid in that instance.

For a complete list of Windows operating systems and platforms that NetBackup supports, refer to the *NetBackup Release Notes for UNIX and Windows* or go to the VERITAS support web site at `http://www.support.veritas.com`.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: *This step is only applicable for NetBackup Enterprise Server.*
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

```
command arg1|arg2
```

In this example, the user can use either the *arg1* or *arg2* variable.

Navigating Multiple Menu Levels

When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action.

The following example shows how the > is used to condense a series of menu selections into one step:

❖ Select **Start** > **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**.

The corresponding actions could be described in more steps as follows:

1. Click **Start** in the task bar.

2. Move your cursor to **Programs**.

3. Move your cursor to the right and highlight **VERITAS NetBackup**.

4. Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.

Introduction 1

This guide explains vaulting procedures as part of two major task areas: administrative and operational. At some sites, different personnel do the different tasks; at other sites, the same personnel do all the tasks. Your site may assign the responsibilites differently than they are discussed in this guide.

The storage administration tasks are summarized in this chapter; operational tasks are documented in “Operational Procedures” on page 5.

Background

At a high level, vaulting is the process of sending backup images off site to a protected storage location. NetBackup Vault simplifies the processes of image duplication, off-site storage, and off-site retrieval for both storage administrators and systems operators. Its purpose is to assist in disaster recovery by creating duplicate copies of backup tapes and of the NetBackup catalog.

If backup tapes are destroyed at a primary data center location, Vault ensures that copies of selected backups are available at an off-site location. Vault keeps track of the copies and requests these tapes to be returned from the off-site location after a specified period of time.

Administration and Operations Tasks

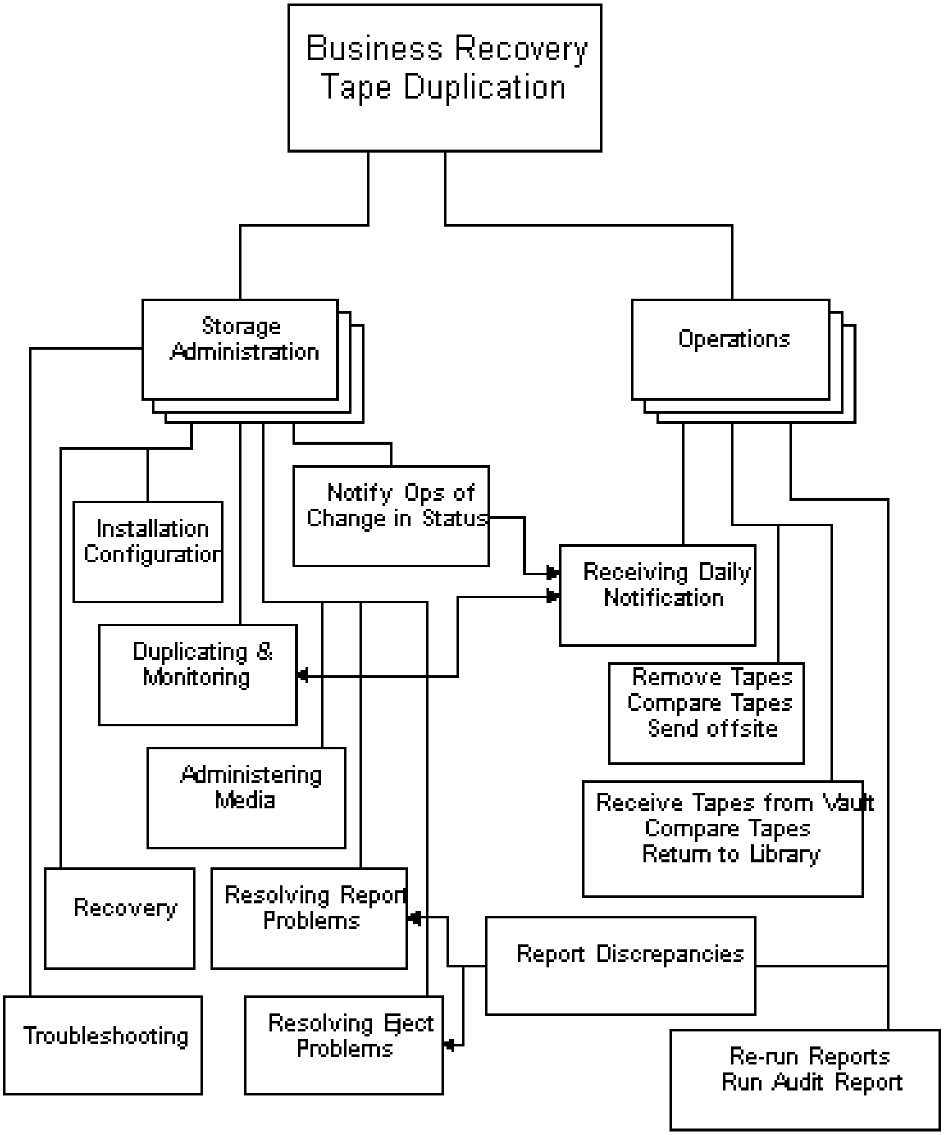
The following table summarizes the responsibilities for both storage administration and storage operations in the table below to help system operations staff understand how to gain necessary support. Detailed operations instructions are provided in the next chapter.:

Vault Tasks

Storage Administration	Storage Operations
Installation and configuration of Vault.	Receiving daily notification of session completion.
Running and monitoring daily Vault sessions to ensure they complete.	Removing off-site tapes from robotic libraries.
Administering tape media to ensure sufficient media available for each day's duplicates.	Comparing off-site tapes to be sent from library with report to send to off-site vendor.
Resolving conflicts between printed reports and off-site vendor media status.	Sending off-site tapes to off-site vendor.
Resolving issues about tapes improperly ejected.	Receiving returned tapes from off-site vendor.
Manually recovering media.	Comparing returned tapes with report from off-site vendor.
	Inserting returned tapes into robotic libraries.
	Reporting discrepancies between reports and the tapes on-hand to storage administration.
	Re-running reports as needed.
	Periodic auditing of media on site.

Operational Design

The following diagram shows the various responsibilites associated with vaulting media. This guide documents the procedures associated with the operations part of the process.


Business Recovery Tape Duplication
Storage Administration
Operations
Notify Ops of Change in Status
Installation Configuration
Receiving Daily Notification
Duplicating & Monitoring
Remove Tapes Compare Tapes Send offsite
Administering Media
Receive Tapes from Vault Compare Tapes Return to Library
Recovery
Resolving Report Problems
Report Discrepancies
Troubleshooting
Resolving Eject Problems
Re-run Reports Run Audit Report

Summary of Storage Administration Responsibilities

Briefly, storage administration does the following:

- Installs Vault. Storage administration installs Vault on a NetBackup master server. For more information on how to install Vault, please refer to the *NetBackup Vault System Administrator's Guide*.
- Configures Vault. Storage administration provides configuration information in profiles, which contain the rules Vault uses to select images to duplicate and/or eject from the robot.

  Storage Administration accesses Vault through the NetBackup Administration Console or through the Vault Administration menu user interface (`vltadm`).
- Monitors Vault. Storage administration monitors Vault activity by using the NetBackup Administration Console and by reading the session log files for information about vault sessions. If e-mail notification is enabled in the profile, session information is sent to the appropriate personnel..
- Administers Media. Storage administration determines which volume pools and volume groups will hold the media and must allocate sufficient media for vaulting needs.
- Notifies Operations of Change in Status. Storage administration must report any change in daily run status to operations. In most situations, Vault jobs are scheduled to run each day. If duplications are postponed for some reason, storage administration should notify operations of job status.

Operational Procedures 2

This chapter provides instructions for each of the Vault operational procedures. The operational procedures in this guide document how to remove tapes from the robotic libraries, run Vault reports, compare the tapes and the reports, and send the tapes to an off-site vendor.

The primary tool used by the Vault operator is the Vault Operator Menu user interface.

Using the Vault Operator Menu Interface

Operational access to Vault is provided through the Vault Operator Menu user interface. The Vault Operator Menu interface lets an authorized user eject and inject tapes and print reports for one or more Vault sessions (an authorized user is one who can invoke the `vltopmenu` command).

The following is the main Vault Operator Menu screen:

```
                       NetBackup Vault Operator Menu

Current Profile: None
Current Session: 0
Current Report Destinations - Print command: /usr/ucb/lpr
                              Email:
                              Directory:

 p) Select Profile                  m) Modify the Report Destinations...
 u) Profile Up                      r) Run Reports for This Session
 d) Profile Down                    v) Run Individual Reports...
 s) Select Session
                                   cr) Consolidate All Reports
 i) Inject Media into Robot        ce) Consolidate All Ejects
 e) Eject Media for This Session   re) Consolidate All Reports and Ejects

                                    c) Container Management...


 q) Quit
Selection-->
```

The Vault Operator Menu screen displays the current profile, current session, and current report destinations. To select an option, type the number of the option, then press Enter.

The results of each operation are written in a log file. The name and location of the log file is located at the end of the output for each command. For example, if you choose **Eject Media for This Session** on a UNIX system, the output is similar to the following:

```
vlteject Started
vlteject Completed
The results of this operation have been logged in the following
file:
/usr/openv/netbackup/vault/sessions/vlteject_status/details.log.ti
mestamp
```

Note Do not run another session for this vault while using this menu.

The Vault Operator Menu is started by the `vltopmenu` command, which is located in the following directory:

UNIX: `/usr/openv/netbackup/bin`

Windows: `*install_path*\NetBackup\bin`

The following describe the menu options:

p) Select Profile Use this option to select a profile.

u) Profile Up Use this option to select the previous profile.

d) Profile Down Use this option to select the next profile.

s) Select Session You this option to select a specific session for the current profile.

i) Inject Media into Robot Use this option to moves media from the media access port (MAP) to the library slots.

e) Eject Media for This Session Use this option to eject media from this session.

m) Modify Report Destinations Use this option to change the print command, the e-mail addresses to which the reports are sent, and the directory to which report files are written.

r) Run Reports for This Session Use this option to generate reports for the current session and distribute them as defined in the profile (print and/or distribute by e-mail).

v) Run Individual Reports Use this option to select individual reports to generate and distribute.

cr) Consolidate All Reports Use this option to generate reports for any vault that has not had reports generated for a given session.

ce) Consolidate All Ejects Use this option to eject media for any vault that has not had media ejected for a given session.

re) Consolidate All Reports and Ejects Use this option to ejects media from all vault sessions and run the reports as configured in the profiles. You can eject media and run reports for a single vault or for all vaults.

c) Container Management Use this option to add volumes to containers, view or change a container's return date, or delete a container.

q) Quit Use this option to quit the interface.

Summary of Operational Procedures

- Receive daily notification of completed Vault sessions.
- Remove tapes from library.
- Compare ejected tapes with report.
- Send tapes off-site.
- Receive expired tapes from off-site vendor (daily or weekly).
- Compare tapes received with session status, and notify storage administration of any discrepancies.
- Re-run reports, if necessary.
- Run the audit report, and notify storage administration of any discrepancies.
- Resolve eject problems by manually ejecting tapes.

Receiving Vault Reports

Each time the vaulting process is run, reports are sent to various staff members to notify them that vaulting is finished. Operations should receive a copy of the daily Picking List for Robot report. This report is meant to notify operations that a job has completed and that tapes are being ejected from the library.

▼ Follow these steps when you receive the report

1. Determine who is responsible for processing the ejected tapes.

2. Retrieve printed reports from the assigned printer, if applicable.

3. Retrieve ejected tapes from the library doors.

4. Prepare tapes for off-site storage.

5. Compare ejected tapes with the Picking List for Robot.

6. Work with Storage Administration to resolve any discrepancies.

If you do not receive the reports by a predetermined time it may be difficult to process the tapes in time for off-site vendor delivery and pickup. Contact storage administration to determine if there are any problems with a given vault session. They can monitor the current jobs and interrupt them to allow the session to finish on time.

Removing Tapes from a Library

How libraries process media ejections depends on their robotic capabilities. Robots that have media access ports (MAPs) place ejected media into one of their MAPs, and you must remove the media from the slots in the MAP. For ACS robots that have multiple MAPs, media are placed in the MAP nearest the media volume (depending on configuration of the vault). For robots that do not have MAPs, you must remove the media from the library slots in the robot.

When ejection occurs depends on whether the vault is configured for immediate or deferred ejection.

If Vault is configured for immediate ejection, the robot ejects the media into the MAP during the vault session and extends the MAP so you can remove the media. If more media are selected for ejection than the capacity of the MAP, Vault fills the MAP again and ejects the media, continuing the process until all media are ejected.

If vault is configured for deferred ejection, you must eject the media and generate the reports manually. If the vault includes more media than will fit in the MAP, you must remove all ejected media before the robot will process the next set of media. To eject media manually and generate reports, you can use the Vault Operator Menu.

The robot should eject the tapes in order of Media ID and Slot ID. Vault assigns a new Slot ID on a session-by-session basis, in Media ID order. The order of ejected tapes should match the order that tapes are listed on the Picking List for Robot report because it is organized by Slot ID. Exception: If off-site slot IDs from tapes that have returned from the vault are reused, the order may not match.

Caution If media are not removed and a timeout condition occurs, the media are returned to (injected into) the library slots in the robot. If this occurs, you should inventory the robot (see the Managing Media in Robots chapter of the *Media Manager System Administrator's Guide*) and then eject the media that was returned to the robot (use `vltopmenu` to eject the media).

Comparing Tapes with Reports to Send to the Off-site Vault

There are several reports you will refer to in processing daily work. We recommend that you send both printed and e-mail copies of all reports to staff members involved.

- **Picking List for Robot**. The Picking List for Robot report lists the tapes you must remove from the robot. It lists the media ID, slot ID, expiration date of the volume, the number of images on the volume, and the size of the images on the volume. This report should list the same tapes that the robot has ejected. The media ID should match the tape label. Slot ID should be in ascending order and should not match any slot in use at the off-site vendor or any slot used by a tape in transit to or from the off-site vendor. The Date Assigned should be the same date as the report. Expiration dates will vary depending on the retention period of the backup policy. If the report does not list any media, then Vault did not eject any media during this session.
- **Distribution List for Vault**. Include this report with the media that is going off-site. It contains the information as the Picking List for Robot, but is intended for distribution to the off-site vendor with the tape batch.
- **Picking List for Vault**. The Picking List for Vault report shows tapes requested for return from the off-site vendor. Provide the off-site vendor with a copy of this report with each batch of media that goes off-site so they will return the expired tapes. The report will not list any tapes if no tapes have expired on the reporting day. Give a copy to the off-site vendor whether or not it lists any tapes.
- **Distribution List for Robot**. The Distribution List for Robot contains information on the same tapes as the Picking List for Vault report. These tapes will not arrive on site for at least one day. Make sure the report is available when the tapes arrive the following day. Do not file the report until the tapes are checked in.
- **Vault Inventory**. The Vault Inventory report shows all the tapes that will be in the off-site vault after the off-site vendor receives the daily batch and they have removed all the tapes shown in the Distribution List for Vault report. Provide one copy of this report to the vendor with each batch. Place another copy in an easily accessible location.

Other reports may be printed after a vault session. The storage administration team should notify operations of all reports that will be printed and which reports need to be sent off site. For example, the administration team may print detailed distribution lists that show the actual data stored on each tape.

Sending Reports and Tapes to the Off-site Vendor

We suggest the following steps as a guideline only; your site may have different procedures in place. After you have received all reports and compared the tapes intended for off-site storage to the reports, you must prepare the tapes and appropriate reports for pickup by the off-site vendor.

▼ To prepare tapes for pickup

1. Use only containers specified by Operations or Storage Administration.

2. Include the Vault Inventory, Distribution List for Vault, and Picking List for Vault reports.

3. Complete the off-site vendor pickup form. Note container numbers, vault number, and date of shipment.

4. File a copy of the Picking List for Robot report in an accessible location. Sign off for completion.

5. Place a copy of the Distribution List for Robot report in an accessible location. This report is a reference for returning tapes.

Receiving Tapes from the Off-site Vendor Vault

We suggest the following steps as a guideline only; your site may have different procedures in place. The off-site vendor will return tapes that have been requested, usually the preceding day. You need to compare the tapes received from the off-site vendor to the reports listing the tapes you expect to receive to ensure that you have received the full set of tapes.

▼ To compare tapes received to report

1. Find the Distribution List for Robot report. This is normally the previous day's report.

2. Compare the tapes you have received from the off-site vendor with the report. Notify storage administration if there are any discrepancies which you cannot resolve with the off-site vendor.

3. Remove the tapes from the containers and enter them into the robot according to your normal operating procedures. Be sure not to skip any slots because the robot may not reload the tapes properly. If you are using Media Manager controlled robots (such as TLD or TL8), run the inject process as specified by storage administration.

4. Sign off the report and file in the proper location.

5. You must resolve all discrepancies (outgoing or returning). Do not file a report until you have resolved all discrepancies.

Report Discrepancies

If you find report discrepancies, we suggest you run one or more reports to audit the location of your media. One option is to run the Off-site Inventory report. Look for unassigned tapes that have been left in the off-site vaulting location, and look for expired media that has not been recalled. The All Media Inventory report also may be useful; it shows media on site, media in transit, and media off site.

Expired media may not be recalled in the following circumstances: A tape is only called back once. If a tape is not picked up (for example, if the report is not run, or if it is a holiday) on the day the report recalling it is generated, that tape media ID does not appear on the following reports, and the piece of media may be forgotten. The Lost Media Report will show media that was not picked from the vault as scheduled.

Rerunning Reports

You may choose to re-run a report because you lost the original copy, or because you want updated information. Use the Vault Operator Menu to rerun reports.

▼ **To rerun a report**

1. Log into the machine on which the NetBackup master server is installed.

2. Run `vltopmenu` as follows, using the name of the profile for which you want to run reports:

```
vltopmenu profile
```

The Vault Operator Menu will regenerate the reports for the most recent session. Select the report or reports you wish to rerun.

Printing Reports from a Previous Day

Change the session number to run a report from a previous day. Choose **Select Session**, and enter the number of the session for which you would like to re-run reports.

Sending Reports through E-mail

You may change the report destination to allow the report to be sent through e-mail. First select **Modify the Report Destinations**, then select **Modify E-mail address(es)**, and finally enter the e-mail address(es) to which the reports should be e-mailed.

Windows: configure the `nbmail.cmd` script in the \bin directory.

Saving a Report to a File

You can save the reports to a file. First select **Modify the Report Destinations**, then select **Modify Directory Destination**, and finally enter the pathname of a directory in which you want the report files stored.

Running the Audit Report

You can use the All Media Inventory report as an audit report. It prints out a full inventory of all media used for duplication of backups. First, it prints out all the media in the robot that is used for duplicates, and then all the media that is in the off-site vault. This information is printed in order by media ID.

Resending Eject Commands (Manually Ejecting Tapes)

Select **Eject Media for This Session** allows you to resend the eject commands from a particular session.

Normally, this option is only used if the eject process was interrupted and some media were not ejected from the library. This option would also be used if the number of tapes you needed to eject exceeded the size of the MAP. If there are still discrepancies between ejected media and the Vault reports after using this command, contact storage administration.

Injecting Tapes into Robot

Choosing **Inject Media into Robot** moves tapes from the media access port (MAP) to the library slots and updates the volume database.

If any problems occur during this process, contact storage administration.

Vault Reports 3

This chapter discusses the reports available in Vault.

Vault Report Types

The following reports and types of reports are available in Vault:

- Reports for Media Going Off-Site
- Reports for Media Coming On-Site
- Inventory Reports
- Container Inventory Report
- Recovery Report for Vault
- Lost Media Report
- Non-vaulted Images Exception Report
- Iron Mountain FTP File

Reports for Media Going Off-Site

The reports for media going off-site show the volumes that have been ejected from the robot and will be transported off-site. They vary in the amount of detail included in each report.

Picking List for Robot

The Picking List for Robot report shows the volumes ejected from the robot that should be transported off-site. This report is sorted by media ID and should be used by the operations staff as a checklist for media that has been ejected from the robots. You can save the report for tracking purposes, or you can reprint it as long as the session directory still exists.

The information in the report depends on whether the vault uses containers or slots.

Picking List for Robot Report Headings

Column	Description
#IMAGES	The number of images on the volume. For Vault catalog backup volumes, displays zero.
CONTAINER ID	The ID of the container in which the volume will reside in the vault.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup volumes, displays the date calculated as a return date during the volume assignment.
KBYTES	The size in kilobytes of images on the volume. For Vault catalog backup volumes, displays the notation NB Catalog.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
SLOT ID	The ID of the slot in which the volume will reside at the off-site vault.

Distribution List for Vault

The Distribution List for Vault report shows the volumes that have been ejected from the robot and will be transported off-site. This report is sorted by off-site slot number and should accompany the media that is destined for the off-site vault. The vault vendor should use this report to verify that all the volumes listed were actually received.

The information in the report depends on whether the vault uses containers or slots.

Distribution List for Vault Report Headings

Column	Description
#IMAGES	The number of images on the volume. For Vault catalog backup volumes, displays zero.
CONTAINER ID	The ID of the container in which the volume resides in the vault.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup volumes, displays the date calculated as a return date during the volume assignment.

Distribution List for Vault Report Headings (continued)

Column	Description
KBYTES	The size in kilobytes of images on the volume. For Vault catalog backup volumes, displays the notation NB Catalog.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
RETURN DATE	The date the container should be returned from the off-site vault.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Detailed Distribution List for Vault

This report is similar to the Picking List for Robot and Distribution List for Vault reports except that detailed information is listed for each media. Because backup jobs can span volumes, it is possible that detailed listings of a backup job appear on more than one volume. This report is useful at a disaster recovery site. VERITAS recommends that you send this report off-site.

The information in the report depends on whether the vault uses containers or slots.

Detailed Distribution List for Vault Report Headings

Column	Description
#IMAGES	The number of images on the volume. For Vault catalog backup volumes, displays zero.
BACKUP ID	Identifier that NetBackup assigns when it performs the backup.
BACKUP TIME	When the backup occured.
CLIENT	Name of the client that was backed up.
CONTAINER ID	The ID of the container in which the volume resides in the vault.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup volumes, displays the date calculated as a return date during the volume assignment.
KBYTES	The size in kilobytes of images on the volume or the size in kilobytes of the image fragements on the volume. TIR indicates a true image restore image. For Vault catalog backup volumes, displays the notation NB Catalog.

Detailed Distribution List for Vault Report Headings (continued)

Column	Description
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
PARTIAL?	Partial images on the volume. The field displays: ◆ Complete if the image is not partial (that is, does not span volumes). ◆ PARTIAL(*x*) if it is a partial images (*x* is the fragment number). ◆ EXTRA if the images does not belong to the session.
POLICY	Name of the policy that was used to back up the client.
SCHEDULE	Name of the schedule that was used to back up the client.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Summary Distribution List for Vault

This report is similar to the Detailed Distribution List for Vault report, except that the entry for each piece of media will list only a unique client, policy, schedule and date. That is, if multiple backup jobs for a given client, policy and schedule (usually seen with RDBMS backups or SAP backups) are written to the same volume on the same date, only one line of information will be printed out on this report. The Detailed Distribution List would show each of these backup jobs as a separate entry, which may generate a very long report. The Summary Distribution List for Vault report summarizes the information and presents it in a more compact form. This report is also very useful for disaster recovery situations; we recommend that you send this report off-site.

The information in the report depends on whether the vault uses containers or slots.

Summary Distribution List for Vault Report Headings

Column	Description
#IMAGES	The number of images on the volume. For Vault catalog backup volumes, displays zero.
BACKUP TIME	When the backup occured.
CLIENT	Name of the client that was backed up.
CONTAINER ID	The ID of the container in which the volume resides in the vault.

Summary Distribution List for Vault Report Headings (continued)

Column	Description
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup volumes, displays the date calculated as a return date during the volume assignment.
KBYTES	The size in kilobytes of images on the volume. For Vault catalog backup volumes, displays the notation NB Catalog.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
POLICY	Name of the policy that was used to back up the client.
SCHEDULE	Name of the schedule that was used to back up the client.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Reports for Media Coming On-Site

The reports for media coming on-site show the volumes that are being requested back from the off-site vault. Vault will not generate these reports until the media have been ejected for the current Vault session.

Picking List for Vault

The Picking List for Vault report shows the volumes that are being requested back from the off-site vault. This report should be sent off-site to the vault vendor. Volumes are listed on this report because Vault determined that they are in an off-site volume group and that all images have expired. When Vault identifies these volumes, it changes the Date Requested field within the Media Manager description field for the media. It then prints out the media ID on this report along with the date requested.

Expired media only appear on the report generated on the date the media expire or the next time the report is generated. If for some reason expired media does not appear on the Picking List for Vault, they will be listed on the Lost Media report.

A slot at the off-site vault from which an expired volume is recalled will be available for use one day after the volume has been physically returned to the robot.

If you use a scratch pool, this report may include volumes from other profiles or vaults that have expired and moved back into the scratch pool even if the report is for a specific Vault profile or session.

The information in the report depends on whether the vault uses containers or slots.

Picking List for Vault Report Headings

Column	Description
CONTAINER ID	The ID of the container in which the volume resides in the vault.
DENSITY	Density of the volume.
LAST MOUNT	The date the volume was last mounted. For Vault catalog backup volumes, displays the notation NB Catalog.
LAST SID	The last session ID of the profile that accessed this volume.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
REQUESTED	Date when the volume is requested back from the off-site vault.
RETURN DATE	The date the container should be returned from the off-site vault.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Distribution List for Robot

The Distribution List for Robot report shows the volumes that are being requested back from the off-site vault. This report is identical to the Picking List for Vault, except that it has a different report title. Retain this report on-site to use as a checklist for the media returned from the off-site vault.

If you use a scratch pool, this report may include volumes from other profiles or vaults that have expired and moved back into the scratch pool even if the report is for a specific Vault profile or session.

The information in the report depends on whether the vault uses containers or slots.

Distribution List for Robot Report Headings

Column	Description
CONTAINER ID	The ID of the container in which the volume resides in the vault.
DENSITY	Density of the volume.

Distribution List for Robot Report Headings (continued)

Column	Description
LAST MOUNT	The date the volume was last mounted. For Vault catalog backup volumes, displays the notation NB Catalog.
LAST SID	The last session ID of the profile that accessed this volume.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
REQUESTED	Date when the volume is requested back from the off-site vault.
RETURN DATE	The date the container should be returned from the off-site vault.
ROBOT	The robot from which the volumes were ejected.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Inventory Reports

The inventory reports show the location of the media. These reports are not generated until the media have been ejected.

If you use the NetBackup Administration Console to display an inventory report, you must select a profile that ejects media. Also, select the most recent session for that profile so the most recent data is reported.

Vault Inventory

The Vault Inventory (or Inventory List for Vault) report shows all media that are off-site at the vault vendor and media being sent off-site. This list is generated by checking the description field for the media, the volume pool, and the off-site volume group. VERITAS recommends that you send this report to your vault vendor so they can verify that they have the volumes that Vault indicates are at the vault vendor.

The information in the report depends on whether the vault uses containers or slots.

Vault Inventory Report Headings

Column	Description
ASSIGNED	The date when the volume was assigned by NetBackup Media Manager. For Vault catalog backup volumes, displays the notation NB Catalog.

Vault Inventory Report Headings (continued)

Column	Description
CONTAINER ID	The ID of the container in which the volume resides in the vault.
EXPIRATION	Date when the images on the volume expire.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Off-site Inventory

The Off-site Inventory (or Full Inventory List for Vault) report includes the information in the Vault Inventory report and also includes any volumes that have been requested back from the off-site vault vendor (that is, volumes in transit). Usually, this report is not generated on a daily basis. Rather, the Inventory List for Vault report is sent to the vault vendor to perform verification.

If you use a scratch pool, this report may include volumes from other profiles or vaults that have expired and moved back into the scratch pool even if the report is for a specific Vault profile or session.

The information in the report depends on whether the vault uses containers or slots.

Off-site Inventory Report Headings

Column	Description
ASSIGNED	The date when the volume was assigned by NetBackup Media Manager. For Vault catalog backup volumes, displays the notation NB Catalog.
CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
EXPIRATION	Date when the images on the volume expire.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
REQUESTED	The date the volume was requested to be returned from the off-site vault.
SLOT ID	The ID of the slot in which the volume resides in the vault. (Slot vaulting only.)

All Media Inventory

The All Media Inventory (or Complete Inventory List for Vault) report shows all volumes in the off-site volume pool.

If you use a scratch pool, this report may include volumes from other profiles or vaults that have expired and moved back into the scratch pool even if the report is for a specific Vault profile or session.

Note Volumes within the off-site volume pool must belong to either the off-site volume group or the robotic volume group or they will not appear on this report.

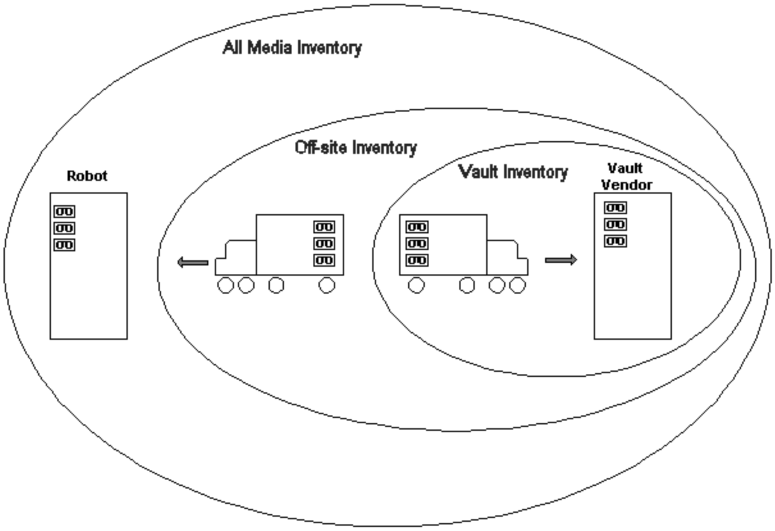
The information in the report depends on whether the vault uses containers or slots.

All Media Inventory Report Headings

Column	Description
CONTAINER ID	The ID of the container in which the volume resides in the vault.
EXPIRATION	Date when the images on the volume expire.
LOCATION	Where the volume resides, the robot (R) or vault (V).
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
REQUESTED	The date the volume was requested to be returned from the off-site vault.
SID	The ID of the session that duplicated and/or ejected this volume.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.

Graphical Representation of Inventory Reports Scope

The following illustration shows the different scopes of the reports:



Container Inventory Report

The Container Inventory Report shows all the containers configured in your vaulting environment, the return date of each container, and the media that are in each container. Alternatively, you can specify a container ID to generate a report of the media in a specific container.

Generate this report only if you vault your media in containers. Reports will not show container information until after you add container and media IDs in Vault. Media are removed logically from a container when they are injected back into the robot.

Container Inventory Report Headings

Column	Description
CONTAINER ID	The ID of the container in which the volume resides in the vault.
LAST SID	The last session ID of the profile that accessed this volume.
MEDIA ID	ID of the media ID that are in the container.

Container Inventory Report Headings (continued)

Column	Description
REQUESTED	Date when the container is requested back from the off-site vault.
RETURN DATE	The date the container should be returned from the off-site vault.
ROBOT	The robot from which the volumes were ejected.

Recovery Report for Vault

The Recovery Report for Vault shows all policies defined on a NetBackup master server and all media that is required for restores between a given set of dates. The report displays the date range to which the images on the media apply.

This report includes the three most recent NetBackup catalog volumes that are currently off-site. For the NetBackup catalog media to be listed in this section, their volume group must match the volume group specified in the off-site volume group. Only NetBackup catalog media that are assigned will appear on this report.

Sending the Recovery Report to the vault vendor on a regular basis will help with disaster recovery efforts. If the master server is destroyed by a disaster, you will not be able to generate a Recovery Report to determine which volumes to request from the vault vendor. Therefore, it is very important that the vault vendor have a copy of the Recovery Report.

The information in the report depends on whether the vault uses containers or slots.

Recovery Report for Vault Fields

Field	Description
BACKUP POLICY	Name of the policy that was used to back up the client.
CLIENT	Name of the client that was backed up.
DATE	Date when the original backup occurred.
EXPIRATION	Date when the catalog backup expire.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
SCHEDULE	Name of the schedule that was used to back up the client.
WRITTEN	The date and time the catalog backup was written to this volume.

Lost Media Report

The Lost Media report lists expired media that has not been returned from the off-site vault vendor. Media can get stranded at the off-site vault for various reasons, as follows:

- Frozen backup media never expires. Media that does not expire will not appear on the Picking List for Vault and will not be recalled from the vault.
- A volume appears on the Picking List for Vault only once. If a volume from that report is missed and is not returned to the robot, it will never again be listed for recall.

You must generate the Lost Media Report; it is not generated when you eject media. You do not have to configure your profiles for the Lost Media Report. Usually, media included in the Lost Media Report should be returned from off-site and injected back into the appropriate vault in the robot.

A good practice is to run the Lost Media Report periodically, such as weekly or monthly (depending on your operations). The Lost Media Report will list media that expired and should have been returned on-site and injected back into a robot for reuse.

Lost Media Report Headings

Column	Description
DENSITY	Density of the volume.
LAST MOUNT	The date the volume was last mounted.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
REQUESTED	Date when the volume is requested back from the off-site vault.
VAULT	The vault to which the volume belongs.
VOLUME GROUP	The volume group to which the volume is assigned.

Non-vaulted Images Exception Report

The Non-vaulted Images report lists images that are not in an off-site volume pool (that is, images that were not duplicated) and media that were not ejected and therefore were not transferred to the off-site vault vendor. When generated as part of a scheduled Vault job, the Non-vaulted Images report uses the same time window as the Vault session and includes information for that specific profile; if generated manually, you can specify a date range by one of the following methods:

- Specifying a calendar date
- Specifying a range of days beginning *x* days ago
- Specifying a session date range beginning with the start time of the session and using the profile's time window

Non-vaulted Images Report Headings

Column	Description
ASSIGNED	The date when the volume was assigned by NetBackup Media Manager.
BACKUP ID	Identifier that NetBackup assigns when it performs the backup.
CLIENT	Name of the client that was backed up.
CREATED	The date the volume was created (original backup or duplicated).
EXPIRATION	Date when the images on the volume expire.
MEDIA ID	Media ID that is assigned when the volume is added to Media Manager.
POLICY	Name of the policy that was used to back up the client.
SCHEDULE	Name of the schedule that was used to back up the client.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault.
VOLUME GROUP	The volume group to which the volume is assigned.
VOLUME POOL	The volume pool to which the volume is assigned.

Iron Mountain FTP File

If Iron Mountain is your vault vendor, you can configure Vault to produce an Iron Mountain Electronic Format report, which is a file that can include the following reports:

- Picking List for Vault
- Distribution List for Vault
- Off-site Inventory Report (if you are vaulting in slots)
- Container Inventory Report (if you are vaulting containers)
- Recovery Report

The reports included in the file depend on your selections on the **Reports** tab of the profile dialog; you must select a report so that it will appear in the Iron Mountain report file.

The report will be in a format that Iron Mountain's automated vaulting mechanism can read and contain the information they require. You can use the file transfer protocol (FTP) to send the report file to Iron Mountain electronically, and they use it to update their vaulting mechanism automatically.

Before you send the report to Iron Mountain, you should verify that the volumes ejected match the Distribution List for Vault. You should contact Iron Mountain to determine where and when to send the report.

Index