Symantec NetBackup™ Vault™ Operator's Guide

UNIX, Windows, and Linux

Release 7.5

Symantec

Symantec NetBackup Vault Operator's Guide

Documentation version: 7.5

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

About NetBackup Vault

This chapter includes the following topics:

About storage administration and operation

This topic explains how to vault media as part of two major task areas: administration and operation. At some sites, different personnel do the different tasks; at other sites, the same personnel do all the tasks. Your site may assign the responsibilities differently than they are discussed in this guide.

The storage administration tasks are summarized in this topic. Operational procedures are performed in the **Vault Operator** menu interface.

See "Vault Operator Menu interface " on page 13.

About vaulting media

When you vault media, you send 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 datacenter 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.

About storage administration and operations tasks

Each storage administration task that is performed causes some storage operation to occur. For example an administrator can decide to run or monitor daily Vault sessions. An administrative task like this means you need to ensure that the Vault session completes and you then remove the off-site tapes from the robotic libraries.

The storage administration tasks include the following:

- Install and configure Vault.
- Run and monitor daily Vault sessions to ensure that they complete .
- Administer tape media to ensure sufficient media available for each day's duplicates.
- Resolve conflicts between printed reports and off-site vendor media status.
- Resolve issues about tapes improperly ejected.
- Manually recover media.

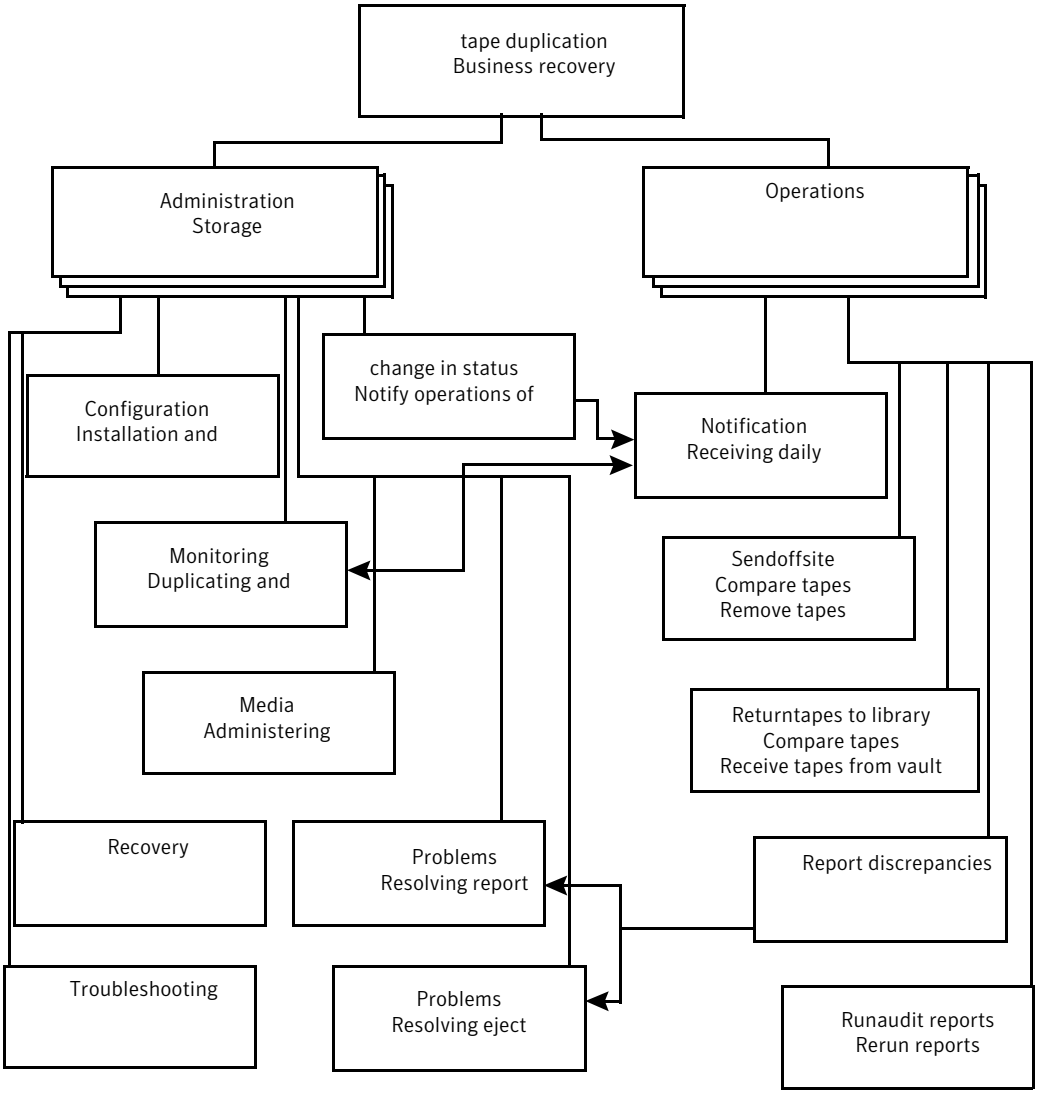
The storage operations tasks include the following:

- Receive daily notification of session completion.
- Remove off-site tapes from robotic libraries.
- Compare off-site tapes to be sent from library with report to send to off-site vendor.
- Send off-site tapes to off-site vendor.
- Receive returned tapes from off-site vendor.
- Compare returned tapes with report from off-site vendor.
- Insert returned tapes into robotic libraries.
- Report discrepancies between reports and tapes on-hand to storage administration.
- Re-run reports as needed.
- Periodically audit media on site.

About storage administration responsibilities

Figure 1-1 shows the various responsibilities that are involved when you vault media.

Figure 1-1 Summary of storage administration responsibilities



Storage administration involves the following tasks:

Install Vault	Storage administration installs Vault on a NetBackup master server. See the *NetBackup Vault Administrator's Guide*.
Configure Vault	Storage administration provides configuration information in profiles, that contain the rules Vault uses to select images to duplicate or eject from the robot. Storage administration accesses Vault through the NetBackup Administration Console or through the Vault Administration menu user interface (`vltadm`). See the *NetBackup Vault Administrator's Guide*.
Monitor 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 email notification is enabled in the profile, session information is sent to the appropriate personnel.
Administer media	Storage administration determines which volume pools and volume groups hold the media and must allocate sufficient media for vaulting needs. See the *NetBackup Vault Administrator's Guide*.
Notify 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 ever postponed, storage administration notifies operations of the job status.

Chapter 2

About NetBackup Vault operational procedures

This chapter includes the following topics:

Vault Operator Menu interface

Operational access to Vault is provided through the **Vault Operator Menu** interface. From the **Vault Operator Menu** interface, you can eject and inject tapes, and print reports for one or more Vault sessions. To be an authorized user of the interface, you must be able to run the `vltopmenu` command.

Figure 2-1 shows the main **Vault Operator Menu** screen.

Figure 2-1 Example display of the Vault Operator Menu

```
                    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 shows the current profile, current session, and current report destinations. To select an option, type the number of the option and press **Enter**.

The `vltopmenu` command starts the **Vault Operator Menu**. The command is in the following directory:

- UNIX

  `/usr/openv/netbackup/bin`

- Windows

  `install_path``\NetBackup\bin`

The `vltopmenu` command writes messages about its operations to the log file for Vault commands:

- UNIX

  `/usr/openv/netbackup/logs/vault/log.`*`mmddyy`*

- Windows:

  `install_path``\NetBackup\logs\vault\`*`mmddyy`*`.log`

The following table describes the menu options:

p) Select Profile	Select a profile.
u) Profile Up	Select the previous profile.

d) Profile Down	Select the next profile.
s) Select Session	Select a specific session for the current profile.
i) Inject Media into Robot	Move media from the media access port (MAP) to the library slots.
e) Eject Media for This Session	Eject media from this session.
m) Modify Report Destinations	Change the following: ■ The print command ■ The email addresses to which Vault sends its reports ■ The directory to which Vault writes report files
r) Run Reports for This Session	Generate reports for the current session and distribute them as defined in the profile (print or distribute by email).
v) Run Individual Reports	Select individual reports to generate and distribute.
cr) Consolidate All Reports	Generate reports for any vault that does not have reports for a given session.
ce) Consolidate All Ejects	Eject media for any vault that has not ejected the media for a given session.
re) Consolidate All Reports and Ejects	Eject 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	Add volumes to containers, view or change a container's return date, or delete a container.
q) Quit	Quit the interface.

See "About Vault operational procedures" on page 15.

About Vault operational procedures

This topic explains the operational procedures in greater detail.

The following list summarizes the operational procedures that are described in the following topics:

- Process daily notifications of the completed Vault sessions.
  See "Processing Vault reports" on page 16.
- Remove the tapes from the library.
  See "About removing tapes from a library" on page 17.
- Compare the ejected tapes with the report.
  See "Vault report options" on page 17.

- Send tapes off-site.
  See "Sending reports and tapes to the off-site vendor" on page 19.
- Receive expired tapes from off-site vendor (daily or weekly).
- Compare the tapes that are received with the session status and notify storage administration of any discrepancies.
  See "Comparing received tapes to your reports" on page 19.
  See "About report discrepancies" on page 20.
- Rerun reports, if necessary.
  See "Rerunning reports" on page 20.
- Run the audit report and notify storage administration of any discrepancies.
  See "About running the audit report" on page 22.
- Manually eject tapes to resolve problems.
  See "About resending eject commands (manually eject tapes)" on page 22.

Processing Vault reports

Each time the vault process runs, it sends reports to various staff members to notify them that it ran. Storage operations should receive a copy of the daily Picking List for Robot report. This report notifies the operations staff that a job has completed and that tapes have been ejected from the library.

To process a Vault 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.
7. If you do not receive a report by the predetermined time, it may be difficult to process the tapes properly. For example, you may miss the time for off-site vendor delivery or pickup.

   If you have not received a report that you expected, contact storage administration to determine if there are any problems with the vault sessions. They can monitor the current jobs and interrupt them to allow the session to finish on time.

See "About Vault operational procedures" on page 15.

About removing tapes from a library

Libraries base decisions to eject media on their robotic capabilities. Robots that have media access ports (MAPs) place ejected media into one of their MAPs. 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 any robots that do not have MAPs, you must remove the media from the library slots in the robot.

You determine when media is ejected when you configure Vault for immediate or deferred ejection.

If you configure Vault for immediate ejection, the robot ejects the media into the MAP during the Vault session. The robot extends the MAP so that you can remove the media. Vault can select more media for ejection than the MAP can hold. If that is the case, Vault fills the MAP again and ejects more media. It continues until it ejects all the required media.

If you configure Vault for deferred ejection, you must eject the media and generate the reports manually. The vault process may include more media than can fit in the MAP. If this situation occurs, you must remove all ejected media before the robot can process the next set of media. You can use the Vault Operator Menu to eject media manually and generate reports.

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 Vault uses slot IDs to order the Picking List for Robot report. For this reason, the report matches the order of the tapes that are ejected. However, the order may not match if off-site slot IDs from the tapes that have returned from the vault have been reused.

Note: If media are not removed and a timeout condition occurs, the media are returned to (injected into) the library slots in the robot. If a timeout occurs, inventory the robot as described in the chapter about management of media in robots in the *NetBackup Administrator's Guide*. After the inventory completes, you can use the Vault Operator Menu to eject the media that was returned to the robot.

See "About Vault operational procedures" on page 15.

Vault report options

You can use several reports to process daily work. Symantec recommends that you send both printed copies and email copies of all reports to the staff members who are involved.

The following list describes the reports:

Picking List for Robot

The Picking List for Robot report lists the tapes you must remove from the robot. Note the following about the Picking List for Robot report:

- The tapes should be the same tapes that the robot has ejected.
- The media ID should match the tape label.
- The slot IDs should ascend in order.
- The slot IDs should not match any slot in use at the off-site vendor
- The slot IDs should not match any slot ID already in use 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 vary depending on the retention period of the backup policy.
- If the report does not list any media, Vault did not eject any media during the session.

Distribution List for Vault

Include this report with the media that is sent off-site. It contains the same information as the Picking List for Robot, but it is intended for distribution to the off-site vendor with the tape batch.

Picking List for Vault

The Picking List for Vault report shows the tapes that were 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 that they return the expired tapes. The report does 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 report contains information on the same tapes as the Picking List for Vault report. These tapes do not arrive on site for at least one day. Make sure that 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 still in the off-site vault. The tapes are those left after the off-site vendor receives the daily batch and removes the appropriate tapes. The tapes that are removed are those 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.

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

See "About Vault operational procedures" on page 15.

Sending reports and tapes to the off-site vendor

Symantec suggests the following procedure as a guideline only. Your site may have different procedures in place.

After you receive all reports and compare them to the tapes that are intended for off-site storage, prepare the tapes and reports for pickup.

To send reports and tapes to the off-site vendor

1. Use only the containers that storage operations or storage administration specify.
2. Include the following reports:
   - Vault Inventory
   - Distribution List for Vault
   - Picking List for Vault
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.
5. Sign off for completion.
6. Place a copy of the Distribution List for Robot report in an accessible location. This report is a reference for returning tapes.

See "About Vault operational procedures" on page 15.

Comparing received tapes to your reports

Symantec suggests the following procedure as a guideline only; your site may have different procedures in place. The off-site vendor returns tapes that were requested, usually the preceding day. Compare the tapes that you received from the off-site vendor to the reports that list the tapes you expect to receive. The comparison should ensure that you have received the full set of tapes.

To compare received tapes against your reports

1. Locate the Distribution List for Robot report. This report is normally the previous day's report.
2. Compare the tapes you received from the off-site vendor with the report. Notify storage administration if there are any discrepancies that 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 use NetBackup-controlled robots (such as TLD or TL8), run the inject process as storage administration specifies.

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

You must resolve all discrepancies in the report, whether they are from the tapes that have left or the tapes that have returned. Do not file a report until you have resolved all discrepancies.

See "About report discrepancies" on page 20.

See "About Vault operational procedures" on page 15.

About 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 any unassigned tapes that were left in the off-site vaulting location, and look for any expired media that was not 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. A tape should be picked up on the day when Vault generated the report that recalled it. If it is not picked up, that tape media ID does not appear on the following reports, and the piece of media may be forgotten. The Lost Media Report shows the media that was not picked from the vault as scheduled.

See "Comparing received tapes to your reports" on page 19.

Rerunning reports

You may choose to rerun 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 on to the NetBackup master server.

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

```
vltopmenu profile
```

The **Vault Operator Menu** regenerates the reports for the most recent session. Select the report or reports you want to rerun.

See "Printing reports from a previous day" on page 21.

See "Sending reports through email" on page 21.

See "Saving a report to a file" on page 21.

See "About running the audit report" on page 22.

See "About resending eject commands (manually eject tapes)" on page 22.

See "About Vault operational procedures" on page 15.

Printing reports from a previous day

To print reports from a previous day, change the session number.

To print reports from a previous day

- Choose **Select Session** and enter the number of the session for which you printed reports.

See "Rerunning reports" on page 20.

Sending reports through email

To allow the report to be sent through email, change the report destination to include one or more email addresses.

Choose **Modify the Report Destinations > Modify Email address(es)**. Enter the email addresses to which the reports should be emailed.

On Windows systems, configure the `nbmail.cmd` script in the `\bin` directory.

To send reports through email

1. Choose **Modify the Report Destinations > Modify Email address(es)**.
2. Enter the email addresses to which the reports should be emailed.
3. (On Windows systems only) Configure the `nbmail.cmd` script in the `\bin` directory.

See "Rerunning reports" on page 20.

Saving a report to a file

To save the reports to a file, change the report destination to include a path name.

Choose **Modify the Report Destinations > Modify Directory Destination**. Enter the path name of a directory in which you want the report files stored.

To save a report to a file

1. Choose **Modify the Report Destinations > Modify Directory Destination**.
2. Enter the path name of a directory in which you want the report files stored.

See "Rerunning reports" on page 20.

About running the audit report

To create an audit report, use the All Media Inventory report. This report prints an inventory of all media that is used for duplication of backups. First, it prints all the media in the robot that is used for duplicates. Next, it prints all the media that is in the off-site vault. This information is printed in order by media ID.

See "Rerunning reports" on page 20.

About resending eject commands (manually eject tapes)

Select **Eject Media for This Session** 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 is also used if the number of tapes you need 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.

See "Rerunning reports" on page 20.

About injecting tapes into a robot

When you choose **Inject Media into Robot**, Vault 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.

See "About Vault operational procedures" on page 15.

Index