NetBackup Web UI Vault Administrator's Guide

UNIX, Windows, and Linux

Release 11.2.0.1

COHESITY

NetBackup Vault Administrator's Guide

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 About Vault 10

About Vault 10
About Vault and NetBackup functions 10
About accessing NetBackup Vault 11
About Vaulting original or duplicate images 11
About the Vault process 12
About choosing backup images 12
About backing up the NetBackup catalog 12
About ejecting media 13
About generating reports 13
About how Vault uses volume groups and pools 13
About NetBackup and Vault configuration 14
About Vault management procedures 14

Chapter 2 Installing Vault 16

About supported systems 16
About supported robots 16
About installing and configuring Vault on UNIX and Linux systems 17
Adding a valid license and configuring Vault for UNIX and Linux systems 17
About upgrading NetBackup Vault on UNIX and Linux systems 18
About installing and configuring Vault on Microsoft Windows systems 18
Adding a Vault license on a Windows system 18
About upgrading NetBackup Vault on a Windows system 19
Removing a Vault license 19

Chapter 3 Best Practices 20

About best practices 20
About vaulting paradigms 21
About preferred vaulting strategies 21
About Vault original backups 22

About how to ensure that data is vaulted 22
About overlapping the time window in the profile 22
About resolving multiple names for a single server 23
About specifying a robotic volume group when configuring a Vault 24
About not Vaulting more than necessary 24
About sending only the intended backups off-site 24
About avoiding vaulting partial images 24
About vaulting original backups in a 24x7 environment 26
About preparing for efficient recovery 26
About Vault NetBackup catalog requirements and guidelines 26
About naming conventions for volume pools and groups 27
About matching volume pools to data usage 27
About the primary copy 28
About suspending vaulted media 28
About revaulting unexpired media 29
About media ejection recommendations 29
About scratch volume pools 29
About organizing reports 30
About organizing reports by robot 30
About organizing reports by Vault 31
About organizing reports by profile 31
About the consequences of sharing an off-site volume group across multiple robots 31
About generating the lost media report regularly 31

Chapter 4 Configuring NetBackup Vault 33

About configuring NetBackup Vault 33
About off-site volume pools 33
Creating a volume pool 34
About creating catalog backup schedules for Vault 35
Creating a Vault catalog backup schedule in an existing policy 35
About setting primary server properties for Vault 35
Setting the maximum number of Vault jobs 36

Chapter 5 Configuring Vault 37

About configuring Vault 37
About Vault configuration 38
Configuration information about primary servers, media servers, and storage units 38
Robot information 39

About configuration methods 39
About configuring Vault Management Properties 40
General tab (Vault management settings) 40
Alternate Media Server Names tab (Vault Management Properties) 41
Reports tab (Vault Management Properties) 43
Configuring robots in Vault 44
Vault Robot dialog box options 45
About creating a vault 45
Creating a Vault 45
About configuring Vault dialog box attributes 46
Media access ports dialog box 49
About creating profiles 49
Profile dialog box 50
About the number of profiles required 50
Creating a profile 51
Configuring a profile 51
About configuring a profile using the Choose Backups tab 52
Choose Backups tab configuration options 52
Catalog backup tab (Profile dialog box) 55
Eject tab (Profile dialog box) 59
Reports tab (Profile dialog box) 65

Chapter 6 Vaulting and managing media 69

About Vault sessions 70
About scheduling a Vault session 70
About running a session manually 72
About running multiple sessions simultaneously 72
About previewing a Vault session 73
Stopping a Vault session 74
About resuming a Vault session 74
About monitoring a Vault session 74
About the list of images to be vaulted 75
About ejection exclusions 75
About Vault resiliency 75
About ejecting media 75
Previewing media to be ejected 76
Ejecting media by using NetBackup Web UI 77
Ejecting media by using the Vault operator menu 78
Ejecting media by using the vlteject command 79
Ejecting media by using a Vault policy 80
Consolidating ejects and reports 81

About injecting media 82
Injecting media for libraries with and without barcode readers 83
Injecting media by using the Vault Operator Menu 84
Injecting media by using the vltinject command 84
About using containers 85
About vaulting media in containers 87
About managing containers and media 89
Generating a Container Inventory Report 91
Revaulting unexpired media 92
About tracking volumes not ejected by Vault 94
About notifying a tape operator when an eject begins 95
About using notify scripts 96
About notify script for a specific robot 97
About notify script for a specific Vault 98
About notify script for a specific profile 98
Notify script order of execution 98
About clearing the media description field 99
Restoring data from vaulted media 99

Chapter 7 Creating originals or copies concurrently 100

About concurrent copies 100
About the continue or fail for concurrent copies 101
About continue copies 101
About fail all copies 102
Creating multiple original images concurrently 102

Chapter 8 Reporting 104

About reports 104
About generating reports 104
Generating reports by using the Vault operator menu 105
Generating reports by using the `vlteject` command 106
Creating a Vault policy to generate reports 106
About consolidating reports 108
About consolidated reports in previous Vault releases 109
Viewing Vault reports 109
Vault report types 110
Reports for media going off site 110
Reports for media coming on-site 115
Inventory reports 117
Lost Media report 122
Non-vaulted Images Exception report 123

About the Iron Mountain FTP file 124

Chapter 9 Administering Vault 125

About setting up email 125
About administering access to Vault 126
Copying a profile 126
About moving a vault to a different robot 127
About changing volume pools and groups 127
About NetBackup Vault session files 128
About setting up Vault session log files 130
Setting the duration of Vault session files 130

Chapter 10 Using the menu user interface 131

About using the menu interfaces 131
About the Vault administration interface 131
Vault operator menu interface 132
Vault fields in bpdbjobs output 134

Chapter 11 Troubleshooting 135

About troubleshooting Vault 135
About printing problems 135
About errors returned by the Vault session 136
About media that are not ejected 136
About media that is missing in robot 137
About the tape drive or robot offline 137
About stopping bpvault 137
About ejecting tapes that are in use 138
About tapes not removed from the MAP 138
Revaulting unexpired tapes 138
Debug logs 139
Setting the duration and level for log files 140
Logs to accompany problem reports 140

Appendix A Recovering from disasters 142

About disaster recovery 142
About what defines a disaster 143
About the disaster recovery process 144
About disaster recovery plans 144
About recovery priorities 144
About developing disaster recovery plans 145
About testing disaster recovery plans 146

About disaster recovery in the NetBackup Vault context 146
About preparing for recovery 147
About recovering NetBackup 149
Recovering data and restoring backup images 149
Archiving and recovering from a specific point in time 152

Appendix B Vault file and directory structure 154

UNIX files and directories 154
Windows files and directories 158

Index 163

Chapter 1

About Vault

This chapter includes the following topics:

- About Vault
- About Vault and NetBackup functions
- About accessing NetBackup Vault
- About Vaulting original or duplicate images
- About the Vault process
- About how Vault uses volume groups and pools
- About NetBackup and Vault configuration
- About Vault management procedures

About Vault

Vault is an extension to NetBackup that automates selection of backup images. It also automates ejection of media for transfer to and from a separate, off-site storage facility. NetBackup Vault also generates reports to track the location and content of the media. Vault functionality does not have to be used only for disaster recovery. You can use Vault to manage the data and the media that you store off-site for regulatory archival purposes.

About Vault and NetBackup functions

NetBackup Vault uses existing NetBackup functions for all operations, such as media control, reporting, and ejecting and injecting of tapes. Information from Vault is integrated with other NetBackup components and appears in the NetBackup Activity Monitor.

NetBackup Vault interacts with the following NetBackup services and catalogs:

- Media Manager, which manages robots and media
- The NetBackup catalog and the Media Manager database record of the images that have been vaulted
- The Media Manager database information which determines when expired media can be returned to the robot for reuse
- The Activity Monitor which displays the status of the Vault job

About accessing NetBackup Vault

NetBackup Vault is installed on a NetBackup primary server. The **Vault management** node is available if you add the appropriate license. You can add licenses during the installation from **Settings > License management**. You can use the NetBackup web UI to configure and manage Vault.

Alternatively, you can manage Vault by using the following methods:

- Menu-based user interfaces
- Command line utilities

About Vaulting original or duplicate images

One of your most important choices is whether to send original or duplicate images off site. If you send original images off site, you do not have to duplicate images and therefore do not have to configure duplication.

Note: NetBackup do not support image duplication in this release.

Vault distinguishes between original images and duplicate images as follows:

- NetBackup creates original images during a backup job, including all of the copies that are created concurrently by a backup policy. NetBackup can create up to four copies of an image concurrently during the backup process; all are considered originals.

  If you create multiple original backups in a NetBackup policy, assign the primary copy to the volume pool for the media that remains on site. And send a copy off site.
- Duplicate images are the copies that Vault creates. A Vault job reads the primary backup image and writes one or more duplicate images concurrently. The Vault job is separate from the NetBackup policy job.

About the Vault process

Vaulting is the process of sending backup images off site to a protected storage location.

For more information about the specific steps in a Vault process, see the following:

- See "About choosing backup images" on page 12.
- See "About backing up the NetBackup catalog" on page 12.
- See "About ejecting media" on page 13.
- See "About generating reports" on page 13.

A Vault job must select images (Choose Backups). The other steps are optional. You can separate the Vault tasks into separate jobs if desired that use different jobs to accomplish different tasks. For example, you can use one job to another job to eject media and generate reports weekly.

Note: Injecting returned media back into the robot is a manual operation. The Vault reports include the media that should be recalled from the off-site location and injected into the robot.

The term *vault* refers to a logical entity that is associated with a particular robot. It also refers to the off-site storage location of a set of tapes.

About choosing backup images

If you create multiple original images concurrently during a backup job, Vault can send original images off site (depending on the profile rules).

Note: Vault does not select the SLP-managed images that are not lifecycle complete.

About backing up the NetBackup catalog

The NetBackup catalog is backed up in the third step of the Vault process. The NetBackup catalog consists of databases of information about the NetBackup configuration and any backups that have been performed. The information about backups includes records of the files and the media on which the files are stored, including information about media sent off-site. The catalogs also have information about the media and the storage devices that are under the control of Media Manager.

Backing up the catalog is optional. However, vaulting a catalog backup with your data can help you recover from a disaster more efficiently. Vault creates its own catalog backup with up-to-date information.

Note: Vault does not duplicate the NetBackup catalog.

About ejecting media

The media that you then transfer to secure storage is ejected, often at a separate facility, in the fourth step of the Vault process. The Vault reporting facilities track the media that are ejected and are recalled from off-site storage for reuse after the images expire. The media can be ejected automatically by a scheduled Vault job or manually after the job has completed. The media can be ejected for each job individually or can be consolidated into a single eject operation for multiple Vault jobs.

About generating reports

Vault reports are generated in the fourth step of the Vault process. The reports track the media that Vault manages. You and your off-site storage vendor can use the reports to determine which media should be moved between your site and the off-site storage location. You can also determine when the moves should occur.

Reports can be generated as part of the Vault job or manually after the job is finished. Reports can be generated for each job individually or consolidated with a consolidated eject operation. Generating reports is optional.

About how Vault uses volume groups and pools

The volume groups identify where volumes reside. They are used as a tracking mechanism by Vault to determine where a volume is located. Volumes in a robotic volume group reside in a robot. During a Vault job, Vault searches the robotic volume group for the media that matches a profile's criteria. If media is found, Vault ejects that media and then moves it logically to an off-site volume group. A logical move means to change the volume attributes to show the new location. When a volume in off-site storage expires and is injected back into the robot, Vault moves it back into the robotic volume group.

Volume pools identify logical sets of volumes by usage. Vault uses them to determine if a volume should be ejected. Volume pools for images to be transferred off site are known as off-site volume pools. When you create the images that you want to send off site, write them to media in an off-site volume pool. During a Vault job,

Vault searches a robot for the images that match the selection criteria. If the media the images reside on are in an off-site volume pool, Vault ejects that media.

About NetBackup and Vault configuration

Before you begin to use Vault, you must set up and configure NetBackup so that volume pools and policies are available to support Vault operations.

See "About configuring NetBackup Vault" on page 33.

After configuring NetBackup for use with Vault, you must configure Vault robots and profiles.

See "About configuring Vault" on page 37.

Read the best practices information to help determine how to set up and configure Vault most effectively for your environment.

See "About best practices" on page 20.

About Vault management procedures

Table 1-1 summarizes the operational procedures for Vault. The *NetBackup Vault Operator's Guide* provides detailed information on day-to-day procedures.

Table 1-1 Vault management procedures

Operational procedure	Staff responsibilities
Choosing Backups: Vault incorporates the new criteria when choosing a backup for vaulting.	
Monitoring: use the NetBackup Activity Monitor to determine progress. Set up links between log files and the email monitoring system and the paging notification.	Ensure that duplication jobs complete successfully. Ensure that errors are reported to appropriate personnel.
Compare report output with ejected and returned media.	Review production duplication cycle for thoroughness. Ensure which media goes to off-site and returning on-site matches reports.
Use Media Manager to expire or freeze tapes manually when needed for retrieval from the vault.	Recall the media that was not recalled during normal Vault operations.
Back up the catalog: Set up a schedule for Vault backup of image catalog. Ensure media available to store catalog.	Ensure that Vault catalog backup occurs.

Table 1-1 Vault management procedures *(continued)*

Operational procedure	Staff responsibilities
Recovery review: test recovery procedures regularly to ensure recovery of essential data from off-site storage.	Know procedures for restoring duplicated images. Know how to restore database catalog, backup software, and so on in case of disaster on NetBackup server(s).

Chapter 2

Installing Vault

This chapter includes the following topics:

- About supported systems
- About supported robots
- About installing and configuring Vault on UNIX and Linux systems
- About installing and configuring Vault on Microsoft Windows systems
- Removing a Vault license

About supported systems

Vault runs on the same operating systems and versions and in the same clustering environments as NetBackup except as noted in the *NetBackup Release Notes*. The NetBackup restrictions and the limitations that relate to systems, clusters, and peripherals also apply to Vault. One exception is that Vault does not support standalone drives.

For information about supported systems and supported upgrade paths, see the *NetBackup Release Notes*.

About supported robots

Vault supports all Media Manager-supported robot types.

Vault also supports the robots that do not have media access ports and barcode readers. For best performance, and to avoid errors when you enter media IDs, Cohesity recommends that you use robots that have media access ports and barcode readers.

You can use Vault with the robots that do not have media access ports.

See "About media ejection" on page 60.

About installing and configuring Vault on UNIX and Linux systems

NetBackup Vault installs on a UNIX and Linux system when the NetBackup primary server is installed or upgraded. No separate installation or upgrade procedure is required. However, you must enter a valid license to use Vault and configure Vault.

See *NetBackup Installation Guide for UNIX and Linux*.

Adding a valid license and configuring Vault for UNIX and Linux systems

To license NetBackup Vault on a UNIX or Linux system, the NetBackup primary server must be installed and running on the UNIX or Linux computer. In addition, you must have a valid NetBackup Vault license.

To add a valid license and configure Vault for UNIX and Linux systems

1. To make sure a valid license for NetBackup Vault is registered on the primary server, enter the following command to list and add licenses:

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

   In a cluster environment, license NetBackup Vault on all nodes in the NetBackup cluster.

2. If you add the NetBackup Vault license after the NetBackup primary server installation is complete, you must start the NetBackup Vault daemon. Perform the following command:

   ```
   /usr/openv/netbackup/bin/nbvault
   ```

3. Sign into the web UI.

   To complete the Vault configuration, you must configure the appropriate NetBackup attributes that Vault uses and identify which NetBackup policies you want to use with Vault (or create new attributes to use with Vault). Please read the following chapters to develop an understanding of how Vault works and how best to configure Vault for your operations. You should configure the email address for notification of session status and enter alternate media server names, if appropriate.

   See "About configuring Vault Management Properties" on page 40.

About upgrading NetBackup Vault on UNIX and Linux systems

On UNIX and Linux systems, NetBackup Vault is upgraded at the same time NetBackup is upgraded. To upgrade NetBackup Vault, follow the upgrade installation procedures for NetBackup.

See the *NetBackup Installation Guide*.

About installing and configuring Vault on Microsoft Windows systems

NetBackup Vault is installed on a Windows system when NetBackup is installed; no separate installation procedure is required.

To use Vault, you must enter a license as follows:

- Your license may be a single license for the base NetBackup product and all NetBackup add-ons that you install, including Vault. If you have already installed NetBackup and entered the license, Vault is already licensed.
- You may have a separate license specifically for the Vault option. If so, you must enter the Vault license before you can use Vault.
  See "Adding a Vault license on a Windows system" on page 18.

If you install a Vault in a cluster environment, you must license Vault on all systems in the cluster on which NetBackup primary servers are installed.

For more information about Administering NetBackup licenses, see the *NetBackup Web UI Administrator's Guide*.

Adding a Vault license on a Windows system

When preparing to license NetBackup Vault on a Windows system, the NetBackup primary server must be installed and running on the Windows computer. Vault cannot be installed on a NetBackup media server or on a NetBackup client. In addition, you must have a valid NetBackup Vault license.

Note: If the license for NetBackup Vault was included in the license for the base NetBackup product, you do not have to perform this procedure.

To add a Vault license on a Windows system

1. Select **Help > License management**.
2. Select **Add license**.
3. Select the license option and follow the prompts.

4 Select **Add**.

5 To complete a new installation, you must configure the NetBackup attributes that Vault uses. You must also identify which NetBackup policies you want to use with Vault (or create new ones to use with Vault). Be sure to configure an email address for notification of sessions status and enter alternate media server names, if appropriate.

   See "About configuring Vault Management Properties" on page 40.

About upgrading NetBackup Vault on a Windows system

On Windows systems, NetBackup Vault is upgraded at the same time NetBackup is upgraded. To upgrade NetBackup Vault, follow the upgrade installation procedures for NetBackup.

See the *NetBackup Installation Guide*.

Removing a Vault license

The NetBackup Vault software is not uninstalled. Rather, you deactivate NetBackup Vault by removing the license from the list of current NetBackup licenses. Then Vault is no longer available for use. You can remove the license only if Vault was licensed with its own license, separate from the base NetBackup product license.

Before you remove the NetBackup Vault license, remove all Vault-specific configuration items. This action ensures that NetBackup does not include anything that was configured for Vault, such as volume pools.

To remove a Vault license

1 Select **Help > License management**.

2 Locate the Vault license from the list and select **Actions > Remove**.

   If NetBackup Vault was included as part of the base product license, performing the following step removes your base license and you cannot use NetBackup. If you do not want to remove the NetBackup license, do not continue.

Chapter 3

Best Practices

This chapter includes the following topics:

- About best practices
- About vaulting paradigms
- About preferred vaulting strategies
- About how to ensure that data is vaulted
- About not Vaulting more than necessary
- About preparing for efficient recovery
- About media ejection recommendations
- About scratch volume pools
- About organizing reports
- About generating the lost media report regularly

About best practices

You can configure Vault to support how your computing environment or datacenter environment is set up and how it operates. A best-practice recommendation that may provide benefit for one environment may not provide the same benefit for another. You should evaluate and implement any recommendations based on the benefit to your environment.

About vaulting paradigms

How you set up and name your vaults and profiles depends on your operations. For example, if you maintain a customer database and a payroll database, you may choose to organize your vaults by data usage and your profiles by time periods.

Example vaults and profiles that are organized by location and data type are as follows:

CustomerDB vault	Weekly
	Monthly
Payroll vault	Biweekly
	Monthly
	Yearly

Alternatively, if your operations are organized geographically, you can set up your vaults by location and your profiles by data type.

Example vaults and profiles that are organized by location and data type are as follows:

London vault	`CustomerDB`
	Payroll
Tokyo vault	`CustomerDB`
	Payroll

About preferred vaulting strategies

Several strategies can help you reduce resource and time contention when you back up your data and when you vault your backup media. Although these strategies may not be advantageous for all situations, they can be beneficial in many environments.

Cohesity recommends that you use one of the following strategies:

- Vault the original NetBackup backup media. Because you can produce multiple copies of images during a NetBackup policy job, fewer drives and less time may be required to create multiple original copies than duplicating media.

- Use disk staging. Send your backups to disk and then copy the data from disk to removable media. This strategy reduces the time that the backup process uses.

About Vault original backups

Cohesity recommends that you use a NetBackup policy to produce multiple, original backup images. You should then use a Vault profile to eject and transfer one or more of the original images off site.

In most situations, vaulting originals has the following advantages:

- Uses less drive-time than duplicating backup images from the original tapes. For example, a backup job that creates two originals of a backup image uses two drives: two units of drive time. Conversely, a backup job that creates one original image uses one drive, and a vault job that creates one duplicate of the original uses two drives: three units of drive time. Over time, duplicating backup images consumes more drive time than writing multiple originals during a backup job.
- Avoids configuring for duplication. In complex environments (such as with multiple media servers, multiple robots, or multiple retention period requirements), it can be difficult to configure the duplication steps of Vault profiles. It is possible to send large amounts of data over the network without careful configuration, although in storage area network (SAN) environments network traffic may not be an issue.
- Use VTL tapes. You can send your backups to VTL tapes with minimum retention period required for your recovery. You can then duplicate to physical tapes from VTL tapes and expire the VTL tape copy using the **Expire original tape backup images after xxx hour(s)** setting.

See the following information before you configure Vault, if you decide to create and vault original backups:

See “About vaulting original backups in a 24x7 environment” on page 26.

See “About avoiding vaulting partial images” on page 24.

About how to ensure that data is vaulted

When you set up NetBackup Vault, make sure that you configure it to vault all of the information that you want transferred off-site.

About overlapping the time window in the profile

To ensure that all data is vaulted, overlap the time window in the profile.

A Vault profile uses a time range as one of the criteria for choosing the backup images to be vaulted. Vault does not duplicate or eject a backup image that already has a copy in the off-site Volume Group; therefore, Vault does not process images that are already vaulted by a previous session. Perhaps more importantly, backups that were not processed if a previous session failed are processed when the profile runs again if the time window is long enough.

Therefore, configure the time window to be the sum of the following:

- The longest expected downtime for a server or robot
- Twice the length of the frequency at which the profile runs

If a robot fails and requires three days to repair, the next time the profile runs, it selects backup images that were not vaulted during the three-day downtime. Configuring the window to be longer, such as seven days, provides even more resiliency. A longer time window forces Vault to search a larger list of images for vault candidates. Although that consumes more processing time, the extra time may not be a problem in your environment because Vault is a batch process that does not demand immediate system response.

About the consequences of not overlapping the time window

When a vault session is delayed, some backup images may be missed if the time window does not allow Vault to select images from a wider time range. For example, suppose the time window for your daily profile extends from one day ago to zero days ago. On Tuesday, the robot has mechanical problems and the Vault profile fails. Consequently, Monday night's backups are not vaulted. On Wednesday, the robot is fixed. When the next Vault session begins on Wednesday, it only selects backup images that were created during the previous 24 hours. So Monday night's backups still are not vaulted. If the profile's time window had spanned more than one day, the session would have picked up both Monday night's and Tuesday night's backups.

About resolving multiple names for a single server

For every media server, you should add an entry on the **Alternate Media Server Names** tab of the **Vault Management Properties** dialog box. At a minimum, there should be, for each media server, an entry that contains both the abbreviated name and the fully qualified name. Also add any other names by which a media server has ever been known. Taking this action avoids a number of problems. For example, if you do not list alternate names for media servers, some images may not be recognized as a match for the criteria entered in the **Choose Backups** tab of the **Profile** dialog box and may therefore not get vaulted.

If you have multiple NIC cards in your server, make sure that the server name associated with each NIC card is listed in the **Alternate Media Server Names** tab when you configure a profile.

See "Alternate Media Server Names tab (Vault Management Properties)" on page 41.

Note: Alternate media servers apply to NetBackup Enterprise Server only.

About specifying a robotic volume group when configuring a Vault

Volumes are ejected only if they are in a robotic volume group and in one of the off-site volume pools that are specified on the profile **Eject** tab. If you want a volume to be ejected, ensure that it is in a robotic volume group and in one of the off-site volume pools that are specified on the profile **Eject** tab.

About not Vaulting more than necessary

When you set up NetBackup Vault, do not select and transfer off-site more data than is necessary.

About sending only the intended backups off-site

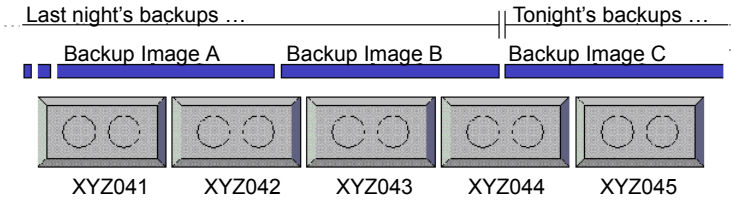
When configuring your backup policies, do not assign backup images that are not intended to be moved off-site to volumes in an off-site volume pool. In some circumstances, Vault ejects a volume if it contains images that are not intended for off-site storage. For example, if volume ABC123 has three images from policy1 and three images from policy2, and policy1 is specified on the profile **Eject** tab, volume ABC123 is ejected even though it contains images from policy 2.

Use different volume pools for backup images you want to keep on site and for backup images you want to send to the vault. If you use the same volume pool for both, you vault the backup images that should remain on-site. Also, if you use the same volume pool for both, a deadlock situation may result if your Vault profile is duplicating images. It may attempt to read a backup image from the same tape to which it tries to write the image.

About avoiding vaulting partial images

Figure 3-1 shows how original backup tapes often begin and end with partial images.

Figure 3-1 Original backup media



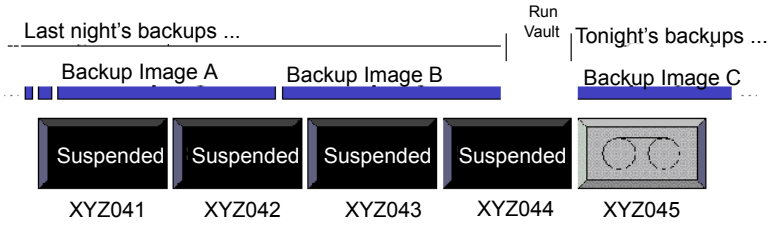
If you eject and vault original backup media, that media may contain partial images.

To avoid vaulting partial images, use one of the following methods:

- Stop backup activity long enough to run Vault.
- If backup jobs are running, use the **Suspend Media for the Next Session** option on the profile **Eject** tab to suspend all media on which backups were written within the last day and then vault only those backups that are older than one day. No more backup images are written to that media, and that media is ready to be ejected.

Figure 3-2 shows what occurs during NetBackup and Vault operations when **Suspend Media for the Next Session** is used.

Figure 3-2 Suspending original backup media



Only use the **Suspend Media for the Next Session** option if you eject original backup media and want to avoid vaulting partial images. You should carefully consider whether to use the **Suspend Media for the Next Session** option. It uses extra CPU cycles because it queries all of the databases again and applies all of the Choose Backups filters again, prolonging the length of time that is required to suspend the media. Therefore, some partial images on vaulted media may be acceptable. If you use this option, it is possible that the original backup media vaulted will not be full.

This option does not suspend media that is in use, such as media to which NetBackup is writing backup images.

Note: Vault only suspends media in off-site volume pools that are specified on the profile **Eject** tab.

About vaulting original backups in a 24x7 environment

If you use Vault in an environment in which backups can occur 24 hours a day, seven days a week, a profile may try to eject media to which backups are written. Because Vault cannot suspend media on which backups are currently written, an error occurs and partial images may be vaulted. The rest of the image is vaulted the next time the profile runs if that tape is not busy and the choose backups time window is large enough to select the image again.

To avoid such problems when vaulting originals, choose backups that were created a day or more ago and suspend the media to prevent writing to the media. (This recommendation assumes that your backups are complete by the time the Vault session runs.)

About preparing for efficient recovery

Preparing in advance can help you restore your data more quickly and easily. The following can help you prepare for recovery.

About Vault NetBackup catalog requirements and guidelines

Use Vault to vault the NetBackup catalogs. A current catalog backup is a critical component of an effective disaster recovery plan. Although you can rebuild the catalog by importing all of your backup media manually, it is a time-consuming process.

Vault requirements and guidelines are as follows:

- Perform the catalog backup step in Vault. Vault creates a new catalog backup with up-to-date information, it does not duplicate an existing NetBackup catalog backup. A NetBackup catalog backup is not a substitute for a Vault catalog backup. It does not include the latest information about duplicated media and media location.
- Use only one vault to do Vault catalog backup.
- Use a dedicated volume pool for Vault catalog backups.
- If you have a robot attached to the primary server, use it for the Vault catalog backup. In most circumstances that primary server creates the NetBackup catalog that remains on site.

See the discussion of NetBackup catalog backups in the *NetBackup Administrator's Guide, Volume I*.

- Retain the three most recent catalog backups. In most circumstances, you do not need to retain vaulted catalog backups for the same length of time that you retain other vaulted backup media. Although you only need one catalog backup in your off-site vault, maintaining the three most recent catalog backups in your off-site vault is a good practice for extra protection. The Recovery Report for Vault lists only the three most recent catalog backups in the off-site vault regardless of how many actually reside in the vault.
- To retain only the three most recent catalog backups, specify an appropriate retention level. Specify a level that dictates that older catalog backups expire and are recalled from off-site storage and only the three most recent catalog backups remain in off-site storage.

About naming conventions for volume pools and groups

How you name pools and groups can help you (and others) organize and more easily identify media if you have to recover data after a disaster.

Use the conventions as follows:

- For volume pools, try to identify the purpose or data in the pools. For example, Vaulted_Payroll, Vaulted_CustomerDB, 1_month_vault, and 7_year_vault are descriptive volume pool names.
- For Vault catalog backups, use an easily identified name for the catalog volume pool (such as Vault_Catalog_Backups).
- For off-site volume groups, use names that indicate the physical location of the data, such as offsite_volume_group.

About matching volume pools to data usage

Volumes are assigned to volume pools. To assist with recovery, create and use off-site volume pools that match your data usage (that is, the type of data). For example, if you maintain a customer database, you may want to restore all of your customer database at the same time when you recover from a disaster. Assign all of your customer database backup data to an off-site volume pool specifically for that data. Assign only backup images of the customer database to that off-site volume pool.

This volume pool (for example, Vaulted_CustomerDB) can correspond to all profiles within a logical vault or to a single profile, depending on your Vault environment configuration.

About the primary copy

The first (or only) original backup image is the primary backup copy. NetBackup always uses the primary copy for restore operations. Vault uses the primary copy for duplication operations (unless the primary copy is on removable media and another copy exists on disk). Ensure that primary copies on removable media remain on site in your robot. If the primary copy is off site, a user-initiated restore operation waits indefinitely for a mount of the off-site media.

If you create multiple original backups during a NetBackup policy job, do not assign the primary copy to an off-site volume pool unless you intend to send it off site. If you assign the primary copy to an off-site volume pool, it is ejected and is not available for restore or duplication operations.

About suspending vaulted media

Suspend unexpired media that is recalled and injected back into the robot so NetBackup does not write images to it. Suspending media before it is ejected also helps to prevent errors from ejecting media that is in use. Vault profile **Eject** tab options let you suspend the media that is ejected so you do not have to suspend it if it is recalled. You also can choose to suspend media before it is ejected so that partial images are not written to that media.

Suspend options available on the Vault profile **Eject** tab are as follows:

Suspend this Session's Media

To suspend media in the profile eject list for the current session. If you select **Immediately**, no more images are written to the media. If you select **At Time of Eject**, images may be written to the media until the media are ejected. Select **At Time of Eject** if you want the media sent off-site to be full.

Because **Suspend this Session's Media** operates on media in the eject list, it does not use more CPU cycles selecting media to suspend.

Suspend Media for the Next Session

To prevent partial images from being written onto media that contains images to be vaulted. Use this option only if you vault original images and want to avoid vaulting partial images on backup media.

You should carefully consider whether to use this option. It uses extra CPU cycles because it queries all of the databases again and applies all of the Choose Backups filters again. Also, this option does not suspend media that is in use, such as media to which NetBackup is writing backup images. However, Vault does enable you to narrow the image search by entering a time window on **Eject** tab.

This option suspends duplicate media created by Vault; however, the **Suspend this Session's Media** option is a better choice for suspending duplicate media because it does not use CPU cycles to select media to suspend.

See "About avoiding vaulting partial images" on page 24.

Note: Vault only suspends media in off-site volume pools that are specified on the **Eject** tab.

About revaulting unexpired media

You should always revault media that was recalled from off-site storage and injected into the robot (for example, if you recall a volume to use for a restore operation). If you do not eject the media and transfer it to your off-site vault location, it is not available if media at your site is damaged.

About media ejection recommendations

Although Vault queues jobs, you can reduce the chances of error conditions from busy robots and reduce potential problems by doing the following:

- Eject media during a dedicated time period when no other inject or eject operations occur.
- Do not inject or eject other media while Vault is ejecting media.
- Do not inventory a robot while Vault is ejecting media.

About scratch volume pools

A scratch pool is an optional volume pool that you can use to ensure that volumes are allocated to the volume pools that need them. Media Manager moves volumes

from a scratch pool to other pools that do not have volumes available, including Vault pools. Expired volumes are returned to the scratch pool automatically.

You can set up a scratch pool in two ways, as follows:

- Create a scratch pool and add all your volumes to it. Then create all the other volume pools but do not allocate any volumes to them. Media Manager then moves volumes from the scratch pool to the other volume pools as needed and returns the expired volumes to the scratch pool.
- Create your volume pools and allocate volumes to them. Then create a scratch pool and allocate volumes to it. Media Manager moves volumes between the scratch pool and the other volume pools as needed and returns the expired volumes to the scratch pool. This method may be the best option if you decide to add a scratch pool to an existing NetBackup configuration.

The scratch pool feature can affect reports for media coming on site. If you use a scratch pool, the Picking List for Vault, the off-site Inventory, and the All Media Inventory reports may include volumes from other profiles or vaults that have expired and moved back into the scratch pool even though the reports may be for a specific Vault profile or session.

For information about configuring scratch pools, see the *NetBackup Administrator's Guide*.

About organizing reports

You should determine whether you want your Vault reports to group media by robot, by vault, or by profile. Your decision affects how you use your volume groups and volume pools.

Vault searches the off-site volume group for the media to include in the reports. It also uses the off-site volume pools for the same purpose. Therefore, you can use either the off-site volume group or the off-site volume pool(s) to organize media for each robot, vault, or profile.

About organizing reports by robot

To ensure that reports are organized by robot, all the vaults within each robot should use the same off-site volume group. That is, each robot has its own off-site volume group. This arrangement organizes reports by robot and maximizes the reuse of tapes. Media from one robot do not appear on the reports for another robot.

Reports do not seem consistent for an individual logical vault, but this strategy maximizes the frequency with which tapes are returned for reuse. Every time the Picking List for Vault report is generated for any profile within any vault for the robot,

tapes from all profiles and logical vaults for that robot can be recalled for reuse (depending on how profiles share off-site volume pools).

About organizing reports by Vault

To ensure that the Vault reports include media for each vault, specify a separate off-site volume group for each vault within a robot (that is, each vault has its own off-site volume group) and a common off-site volume pool for all profiles within each vault (that is, all profiles in the vault use the same off-site volume pool). Doing so ensures that each report contains media from one vault.

About organizing reports by profile

If you want the reports to include only media for a single profile, use a separate off-site volume pool for each profile.

About the consequences of sharing an off-site volume group across multiple robots

If profiles from multiple robots share both an off-site volume group and one or more off-site volume pools, your vault vendor returns a group of tapes (for a single Picking List for Vault report) that were ejected from multiple robots. The operator needs to identify which tapes should be injected into each of the robots. If mistakes are made identifying and injecting tapes, you can inject the incorrect media and possibly the incorrect number of media into your robots.

About generating the lost media report regularly

You should generate the Lost Media Report regularly so you can recall media that has not been returned from the off-site vault vendor but which should have been returned.

Media can get stranded at the off-site vault for the following reasons:

- Frozen backup tapes never expire. A backup tape that does not expire does not appear on the Picking List for Vault and is not recalled from the vault.
- A backup tape appears on the Picking List for Vault and Distribution List for Robot only once. If a tape from that report is missed and is not returned to the robot, it never again is listed for recall.
- You change off-site volume group or pool names. For example, if you begin to use a new media type, you have to use a new volume pool name. If you change names, media may be stranded off-site because the Picking List for Vault is

based on off-site volume pools and off-site volume groups. Media associated with the old names are not listed.

Cohesity recommends that you do not change or rename group or pool names. See "About changing volume pools and groups" on page 127.

How often you generate the Lost Media Report depends on your operations. Weekly or monthly may be often enough.

Chapter 4

Configuring NetBackup Vault

This chapter includes the following topics:

- About configuring NetBackup Vault
- About off-site volume pools
- About creating catalog backup schedules for Vault
- About setting primary server properties for Vault

About configuring NetBackup Vault

Before you configure Vault, you must do the following in NetBackup:

- Create off-site volume pools.
- Create a Vault catalog backup schedule.

You should review the best practices information. It can help you determine how to set up and configure Vault.

See "About best practices" on page 20.

You should be familiar with basic NetBackup concepts, such as volume pools and groups, policies, and storage units.

See the *NetBackup Administrator's Guide, Volume I*.

About off-site volume pools

Volume pools identify logical sets of volumes by usage. Vault uses volume pools to determine if a volume should be ejected. Volume pools for images to be

transferred off site are known as off-site volume pools. When you create the images that you want to send off site, write them to media in an off-site volume pool. During a Vault job, Vault searches a robot for the images that match the selection criteria. If the media that the images reside on are in an off-site volume pool, Vault ejects that media.

You need at least two dedicated volume pools such as the following:

Off-site Volume Pool	Vault ejects media from off-site volume pools. Assign the data that you want to transfer off site to media in an off-site volume pool. You can assign either original backup images that are created as part of a NetBackup policy job or duplicate images that are created by a vault job to the off-site volume pool. How many off-site volume pools you use depends on your operations.
Vault Catalog Backup Volume Pool	If you write the Vault catalog to removable media, you should use a volume pool that is dedicated for Vault catalog backups. When you configure the volume pool in Media Manager, ensure that the Catalog Backup attribute is set. You should use only one Vault catalog backup volume pool. Vault does not require a dedicated volume pool for its catalog backups. However, if you do not use one, regular NetBackup media or catalog media may be ejected.

Do not use the NetBackup volume pool for Vault media. Because the NetBackup volume pool is the default volume pool, if you use it for Vault you can send more data off-site than you intend.

See “Creating a volume pool” on page 34.

See “About naming conventions for volume pools and groups” on page 27.

See “About matching volume pools to data usage” on page 27.

See “About scratch volume pools” on page 29.

Creating a volume pool

Ensure that the volume pools you create have sufficient volumes allocated to them (or to a scratch pool if one exists).

After a volume is assigned to an off-site volume pool, it remains in that pool and is used for rotation within that same pool. (Unless a scratch pool exists, in which case it is returned to the scratch pool).

See the *NetBackup Web UI Administrator’s Guide* > *Configuring tape media* > *Managing volume pools* section for more information about volume pools and allocating volumes to them.

About creating catalog backup schedules for Vault

NetBackup uses a special backup policy of type NBU-Catalog to perform catalog backups. To perform a Vault catalog backup, Vault uses a special schedule of type Vault Catalog Backup in an NBU-Catalog policy.

Before you can configure the catalog backup step in Vault, you must create a Vault Catalog Backup schedule in an NBU-Catalog policy.

See "Creating a Vault catalog backup schedule in an existing policy" on page 35.

See "Catalog backup tab (Profile dialog box)" on page 55.

See "About Vault NetBackup catalog requirements and guidelines" on page 26.

Creating a Vault catalog backup schedule in an existing policy

You can create a schedule in an existing backup policy or create a new backup policy and schedule. You can create more than one Vault schedule per policy, and your NetBackup environment may have more than one policy.

You must specify the storage unit and, if the storage unit uses removable media, a volume pool for the Vault catalog backup.

If creating one copy of the catalog, you must do the following:

- Override the policy's storage unit and select a storage unit.
- Override the policy's volume pool and select the dedicated Vault catalog volume pool (for removable media only).

If making multiple copies, select the storage unit and the dedicated Vault catalog volume pool (removable media only).

You do not have to specify a volume pool for disk storage units.

Prerequisites are as follows:

- Create a Vault of backup policy type
  See the *NetBackup WebUI Administrator's Guide* > *Configuring backups* > *Managing classics policies* section.

About setting primary server properties for Vault

Several NetBackup primary server properties control some aspects of Vault.

Setting the maximum number of Vault jobs

Vault uses the **Maximum vault jobs** property as a threshold for queueing jobs. This property is configured on the NetBackup primary server. For more information see *NetBackup Web UI Administrator's Guide*.

The **Maximum Vault Jobs** property is configured on the NetBackup master server.

See "About running multiple sessions simultaneously" on page 72.

To set the maximum number of Vault jobs

1. On the left, select **Hosts > Host properties**.
2. Select the primary server and select **Edit primary server**.
3. Select **Global attributes**.
4. Specify the maximum number of vault jobs that can be active on the primary server.

   The greater the maximum number of vault jobs, the more system resources are used.

See the **Maximum Vault Jobs** property in the *NetBackup Administrator's Guide, Volume I*.

Chapter 5

Configuring Vault

This chapter includes the following topics:

- About configuring Vault
- About Vault configuration
- About configuration methods
- About configuring Vault Management Properties
- Configuring robots in Vault
- Vault Robot dialog box options
- About creating a vault
- Media access ports dialog box
- About creating profiles
- Creating a profile
- Configuring a profile

About configuring Vault

When you configure Vault, you configure robots, vaults, and profiles. However, before you can configure Vault, you must first configure volume pools and a catalog backup schedule that Vault uses.

See “About configuring NetBackup Vault” on page 33.

Then, after you configure Vault profiles, you configure the policies to schedule when a Vault job runs.

See “About scheduling a Vault session” on page 70.

Before configuring NetBackup and Vault, review the best practices information. It can help you determine how to set up and configure Vault.

See "About best practices" on page 20.

About Vault configuration

Information about the general configuration for NetBackup is required so you can set up and use NetBackup Vault. Collect and record the appropriate information about the primary servers and media servers, storage units, and robot information. That way the information is available when you begin to configure Vault.

Configuration information about primary servers, media servers, and storage units

Collect the following information about primary servers, media servers, and robotic devices, which are used in various configuration options in Vault:

Table 5-1 Configuration information

Property	Description
Primary server host name	The name of the host server on which the NetBackup primary server and Vault are installed.
Operating System level of primary server	The release of the operating system residing on the system on which the NetBackup primary server is installed.
Number of media servers	The number of media servers that are associated with the primary server.
Media server name	The name of each media server that controls the drives you want to use for the vault process. This server should also be bound to a storage unit within the NetBackup configuration. For NetBackup, all drives (of a given media type) that are attached to a server are defined as one storage unit, which is the recommended configuration for NetBackup. For every media server, configure alternate media server names. See "Adding alternate media server names" on page 43.
Operating System level of media servers	The release of the operating system on the host machines on which the NetBackup media server or servers are installed.
Types of Robotic Devices	The robotic devices that are associated with each media server. Use the appropriate NetBackup terminology to identify the devices (for example, TLD and ACS) or specify the actual hardware manufacturer and model names for each device.

Table 5-1 Configuration information *(continued)*

Property	Description
Storage unit name	The NetBackup storage units that are associated with each media server. Consider how many drives in each storage unit you want to use for vault sessions. You may choose to keep some drives available for restores or backups while duplication is running.
Number of drives	The number of drives in each storage unit. Tape to tape duplication requires drives in pairs: one to read and one to write.

Robot information

Collect the following information for each robot. Although the following information is not required to configure a robot for Vault, it may help you plan your configuration so that you use resources efficiently.

The robot properties are as follows:

Table 5-2 Robot information

Property	Description
ACSLS Server	The name of the ACSLS server. StorageTek only.
ACS Number	The corresponding ACS number for this robot. You can obtain this information by using the Media Manager `tpconfig` or by using the ACSLS console commands such as `query acs all` or `query lsm all`. StorageTek only.
LSM Number	The corresponding LSM number for this robot. You can obtain this information by using the Media Manager `tpconfig` command or by using the ACSLS console commands such as `query acs all` or `query lsm all`. StorageTek only.
MAP Capacity	The capacity of the media access port (also known as cartridge access port). On StorageTek systems, you can obtain this information by using the ACSLS command `query cap all` from the ACSLS console.
MAP Numbers	The identifiers for the media access port. On StorageTek systems, you can obtain this information by using the ACSLS command `query cap all` from the ACSLS console.

About configuration methods

The NetBackup Vault Manager manages Vault activity and arbitrates access to the Vault robot, vault, and profile configuration information. The NetBackup Vault Manager must be running at all times so Vault functions correctly.

About configuring Vault Management Properties

Vault Management Properties specify email addresses for event notification, alternate media server names, report properties for all vaults, and retention level mappings for all vaults.

Configure **Vault Management Properties** using the following tabs in the dialog box:

- See "General tab (Vault management settings)" on page 40.
- See "Alternate Media Server Names tab (Vault Management Properties)" on page 41.
- See "Reports tab (Vault Management Properties)" on page 43.

General tab (Vault management settings)

The options on the **General** tab are described as follows:

Table 5-3 General tab configuration options

Property	Description
Email address for notification of session status	An email notification is sent at the end of each vault session. It provides a summary of the vault session, in the form of a `summary.log` file, and the status of the operation. The subject line of the email message is formatted as follow: Vault Status *status_code* [*robot_number/vault/profile*] *(PrimaryServer)* By default, the email is sent to the root or administrator user account on the system on which the NetBackup primary server is installed. If you enter email addresses in the E-mail address for notification of session status field, email is sent to those addresses rather than to the root user. You cannot disable notification of session status. To enter more than one address, separate the addresses with commas.
Email address for eject notificationP	An eject notification is sent to the email addresses entered in the **Email address for eject notification** field when the eject begins (includes a list of the media to be ejected) and when the eject is completed. Eject notification is configured for each profile on the **Eject** tab, for each robot on the **Vault Robot** dialog box, and globally for Vault on the **Vault Management Properties** dialog box **General** tab. Vault sends the notification to the first email addressesthat are found in that order. You can configure different addresses in each place. To enter more than one address, separate the addresses with commas.
Eject media, sort by	You can select whether to eject media alphabetically or by expiration date. By default, Vault ejects media alphabetically.

Table 5-3 General tab configuration options *(continued)*

Property	Description
Lookback days for media going offsite reports	You can enter the number of days before the day a profile runs to search for images to include in media going off-site reports. This setting reduces the amount of time to generate reports because Vault searches fewer image database records to determine which images are on the ejected media. By default, Vault searches the entire image database. Specifying a value does not affect whether media are ejected and vaulted. However, if a volume is ejected that has an image on it older than the period you specify, that image is not listed on the media going off-site reports.

For procedures related to configuring the **General** tab options on the **Vault management settings** dialog, see the following topics.

See "Configuring Vault Management Properties on the General tab" on page 41.

Configuring Vault Management Properties on the General tab

In the **Vault Management Properties** dialog, use the **General** tab to configure the following:

- The email address for session status notification.
- The email address for eject notification for all profiles.
- The sort order for ejected media.
- The reporting period for media going off-site reports.
  See "About setting up email" on page 125.

To configure general Vault management properties on the General tab

1. From within Vault Management, select **Vault Management Properties** on the **Actions** menu.
2. In the **Vault Management Properties** dialog, select the **General** tab.
3. Enter information or select options as appropriate.

See "General tab (Vault management settings)" on page 40.

Alternate Media Server Names tab (Vault Management Properties)

Use the **Alternate Media Server Names** tab (Vault Management Properties) to add alternate names of NetBackup media servers.

Adding alternate names for media servers simplifies configuration and helps ensure that all images eligible to be vaulted are chosen. Vault expands any occurrence of one of the names in a server name group to include all of the names in the group.

For every media server, add the fully qualified name, the short name, every name that is used by storage units that refer to it, and any other names by which a media server has been known. If you have multiple network interface cards (NICs) in the server, all server names associated with each NIC.

You also can create a server name group that includes different servers. Then, in the **Media Servers** field in the **Choose Backups** tab of the **Profile** dialog box, you only have to specify the server name group rather than the individual servers. This use of the **Alternate Media Server Names** dialog box lets you use one name to specify more than one server. This name is useful if you want to duplicate images from multiple servers.

If you use the default, all media servers, for all of your vaults, you do not have to specify alternate media server names.

About alternative media server names

A media server can have more than one name. For example, a server can have a fully qualified name, a short name, and more than one network interface card, each of which has its own name. If a media server has more than one storage unit, each storage unit can use a different name for that media server.

If a media server has more than one name, images backed up by it can be identified by an alternate name. If you specify only one of the names of that media server, images that are identified by the other names are not vaulted.

The Choose backups configuration is simplified if you specify media servers (that is, specify something other than the default: all media servers). If you add alternate media server names, you only have to specify one of those names in the **Media Servers** field of the **Profile** dialog box **Choose Backups** tab. If you do not add alternate media server names, you must specify all the names that are associated with each media server on the **Choose Backups** tab.

About alternate media server names considerations

Be aware of the following concerns associated with alternate media server names:

- You must have enough drives in the specified destination storage unit to keep up with the demand for duplication. If you do not, you risk a deadlock situation.
- The specified media servers must have access to the destination storage unit. If not, you risk a deadlock situation and your Vault job fails. To prevent this situation, use the **Media Servers** criterion on the **Choose Backups** tab to ensure that only backups from certain media servers are selected.

- If multiple duplication rules use different media server names that are part of a server name group, Vault processes only the first duplication rule. Successive rules do not get processed. Also, because the media server name for the duplication rule is expanded to include all media server names in the group, all images written by all storage units that use those media server names are processed by the first duplication rule that uses any name from the group. All images are processed, but by the first duplication rule only.
- Your configuration can send data over the network, depending on the media server(s) in use.

Cohesity recommends that you specify only one destination storage unit per server. If you specify more than one, you may create a problem because Vault does not have a mechanism to choose to which destination storage unit to send the duplicate images.

Adding alternate media server names

Use the following procedure to add alternate media server names.

To add alternate media server names

1. Select **Vault management** and then select **Vault management settings** on the top right corner of the portal's page.
2. Select **Alternate media server** names tab.
3. In the field below the **Media Server Names** window, enter all the alternate names for the media server, separated by commas. Then click **Add**.
   - To remove a media server name group you previously added, select it and click **Delete**.
   - To change a name group you previously added, select it and then click **Edit**.

   Each server name group should occupy one line in the **Media Server Names** window.
4. Click **Save**.

Reports tab (Vault Management Properties)

Use the **Reports** tab (Vault Management Properties) to configure the following items:

- Each report that you want generated when a profile runs.
- Customize report titles.
- The destinations for each report (email, printer, and location to save).

The values that are configured on this tab are propagated to the **Reports** tab of each profile. You can override the values you configure on this tab for any report on any profile.

See "Changing report properties" on page 44.

Changing report properties

Use the following procedure to change report properties on the **Change Report Properties** dialog.

To change report properties

1. Click kebab menu of the desired report and then select **Edit**.
2. In the Edit report properties dialog box, specify the required information.

   If you consolidate your reports and also change titles, use the same title for all profiles whose reports are consolidated. The title is printed on the reports and appears in the email subject line if you email the reports.

Configuring robots in Vault

Use the **Vault Robot** dialog box to specify and configure the robots from which Vault ejects media. Vault robots contain the media that has images to be stored off-site. That media is ejected so it can be transferred to the vault. The images can be original images that are created during a backup job.

You can select any robots that are recognized by NetBackup and that have storage units associated with them. NetBackup assigns a number to each robot that it recognizes, and eligible robots are recognized by Vault.

To configure a robot in Vault

1. Log into NetBackup Web UI
2. On the left pane, select **Storage > Vault management**.
3. Select **Actions** drop-down and then click **Add vault robot**.
4. In the **Add vault robot** dialog box, select the **Robot name** from the drop-down. **Robot control host** is displayed.

   Note: Robot control host is the name of the host that controls the robot. This value is auto-populated based on the API response.

Vault Robot dialog box options

Table 5-4 contains the field descriptions of the **New Vault Robot** dialog box.

Table 5-4 Robot configuration information

Property	Description
Robot Name	The name of the robot. The name is configured in Media Manager, and Vault uses that information to populate the **Robot Name** field.
Robot Control Host	The name of the host that controls the robot. Enter the name of the media server that controls the robot.
Use email address from Vault Management Properties for eject notification	Select to use the global eject notification email address or enter email addressees, separated by commas, semicolons, or spaces, that receive notification when eject begins and ends. Eject notification is configured for each profile on the **Eject** tab, for each robot on the **Vault Robot** dialog box, and globally for Vault on the **Vault Management Properties** dialog box **General** tab. Vault sends the notification to the first email addresses found in that order. You can configure different addresses in each place.

See "Configuring robots in Vault" on page 44.

About creating a vault

After you configure robots, you can create and configure vaults with the **Vault** dialog box.

- See "Creating a Vault" on page 45.
- See "About configuring Vault dialog box attributes" on page 46.

See "About how Vault uses volume groups and pools" on page 13.

Creating a Vault

The following are the requirements for creating a vault:

- At least one robot must be configured already in Vault.
- A robot may contain multiple vaults, but a vault cannot span robots. Therefore, if you configured three TLD robots for Vault (not connected with pass-through devices), you must define at least three logical vaults, one for each TLD robot.

- Volumes in a vault must have the same density. If a robot has volumes of different density and you want to use all of those volumes for Vault, that robot must have a separate vault for each volume density.

Use the following procedure to create a vault.

To create a vault

1. In the NetBackup Web UI, select **Storage > Vault management**. Expand **Vault management**.
2. Select a robot in the **Vault management** tree.
3. From the **Actions** drop-down, select **Add vault**.
4. In the **Add vault** dialog box, enter or select the values for each fields.

   See "About configuring Vault dialog box attributes" on page 46.
5. Click **Add**.

About configuring Vault dialog box attributes

A vault is a logical entity that refers to a collection of removable media drives (usually tape drives) within a robot. You can use vaults to organize the data that is going off-site.

For example, you can use one vault for payroll data and another vault for customer data.

You can configure a vault by specifying the following values in the dialog box:

- **Vault Name**: The name of the vault. The name should reflect its purpose. For example, if you are creating a vault primarily to duplicate and vault records from the finance department, you might call the vault Finance. The vault name may contain up to 25 characters.
  Vault names are case sensitive.

  Note: Directory names are not case sensitive on Microsoft Windows systems. Therefore, session directories are created in the same `vault\sessions\vault_name` directory for two or more vaults that have names that differ only in case

- **Vault robot**: Select the appropriate robot from the drop-down.

  Note: If the required robot does not exists in the drop-down, select Add vault robot. See See "Configuring robots in Vault" on page 44.

- **Vault vendor**: The name of your off-site vault vendor (for example, Iron Mountain). If you select Iron Mountain, you also can configure Vault to put media lists into a file formatted in compliance with Iron Mountain's electronic processing specification. You can then send this file to Iron Mountain for electronic processing of the media lists.
- **Customer ID**: Your customer identification if you selected Iron Mountain as your vault vendor. You may have a separate customer ID for each logical vault.
- Select anyone of the following option **When vaulting, use**:
  - **Slots for individual media**: Select if your media is stored in slots at your off-site storage location. If you select slots, you must complete the **First Off-site Slot ID** field.

    The ID of the first slot in the off-site vault. This usually is provided by your vault vendor. Off-site slot IDs are often used by the vault vendor to track media. If your vendor does not use these identifiers, you can use the default first off-site slot ID of 1. Off-site slot IDs are unique only within a given vault.

    Slot IDs are assigned consecutively from the starting slot number. Ensure that the number of media in the vault does not exceed the range of slot IDs assigned by the vault vendor. With every session, Vault starts with the off-site slot ID and counts upward, looking for slots that are no longer in use. Vault always fills in the gaps with newly vaulted media.

    If multiple vaults are defined for the same vault vendor, divide the range of assigned slots between the various vaults. For example, if the vault vendor assigned the range 1-2000 and you defined three vaults for this vault vendor, then you can assign range 1-499 to vault 1, 500-999 to vault 2, and 1000-2000 to vault 3, assuming that vault 3 has the maximum number of tapes to vault.
  - **Containers of many media**: Select if your media is stored in containers at your off-site storage location.
- **Robotic volume group**: The name of the volume group associated with the robot for this vault. The Robotic Volume Group is the group that indicates that media resides in a robot. Usually, NetBackup creates a robotic volume group when media are added to a robot. A robotic library can contain volumes from more than one volume group, so a robot can have more than one robotic volume group name associated with it.
- **Off-site volume group**: The name of the off-site volume group. The Off-site Volume Group indicates that media are in off-site storage. The name should describe the data, the vault vendor, the vault location, or a combination thereof so you can easily identify the volume group. Vault moves each piece of ejected media from the Robotic Volume Group into a standalone volume group (that is, a volume group that is not under the control of the robot). If the Off-site Volume

Group does not exist, it is created during the vault session. The off-site volume group name may contain up to 25 characters.

If the off-site volume group does not exist, it is created during the vault session.

Vault Attributes tab options (Vault dialog box)

If you are configuring a vault in an ACS robot, you also can configure the media access ports (MAPs) to use for eject operations.

See "About ACS MAP" on page 61.

See "About vaulting paradigms" on page 21.

See "About preferred vaulting strategies" on page 21.

See "About naming conventions for volume pools and groups" on page 27.

Table 5-5 lists the **Vault** dialog box configuration options that you can configure in the **Vault** dialog box.

Table 5-5 Vault dialog box configuration options

Property	Description
Containers of Many Media	Select if your media is stored in containers at your off-site storage location.
First Off-site Slot ID	The ID of the first slot in the off-site vault. This usually is provided by your vault vendor. Off-site slot IDs are often used by the vault vendor to track media. If your vendor does not use these identifiers, you can use the default first off-site slot ID of 1. Off-site slot IDs are unique only within a given vault. Slot IDs are assigned consecutively from the starting slot number. Ensure that the number of media in the vault does not exceed the range of slot IDs assigned by the vault vendor. With every session, Vault starts with the off-site slot ID and counts upward, looking for slots that are no longer in use. Vault always fills in the gaps with newly vaulted media. If multiple vaults are defined for the same vault vendor, divide the range of assigned slots between the various vaults. For example, if the vault vendor assigned the range 1-2000 and you defined three vaults for this vault vendor, then you can assign range 1-499 to vault 1, 500-999 to vault 2, and 1000-2000 to vault 3, assuming that vault 3 has the maximum number of tapes to vault.
Media Access Ports to Use	For ACS robots only, the media access ports (MAPs) to use for media ejection for the current vault. To select or change MAPs to use, click **Change**. In the **About the media access ports** dialog box, select the MAPs to use.

Table 5-5 Vault dialog box configuration options *(continued)*

Property	Description
Off-site Volume Group	The name of the off-site volume group. The Off-site Volume Group indicates that media are in off-site storage. The name should describe the data, the vault vendor, the vault location, or a combination thereof so you can easily identify the volume group. Vault moves each piece of ejected media from the Robotic Volume Group into a standalone volume group (that is, a volume group that is not under the control of the robot). If the Off-site Volume Group does not exist, it is created during the vault session. The off-site volume group name may contain up to 25 characters. If the off-site volume group does not exist, it is created during the vault session.
Robotic Volume Group	The name of the volume group associated with the robot for this vault. The Robotic Volume Group is the group that indicates that media resides in a robot. Usually, NetBackup creates a robotic volume group when media are added to a robot. A robotic library can contain volumes from more than one volume group, so a robot can have more than one robotic volume group name associated with it.
Slots for Individual Media	Select if your media is stored in slots at your off-site storage location. If you select slots, you must complete the **First Off-site Slot ID** field.
Vault Name	The name of the vault. The name should reflect its purpose. For example, if you are creating a vault primarily to duplicate and vault records from the finance department, you might call the vault Finance. The vault name may contain up to 25 characters. Vault names are case sensitive. **Note:** Directory names are not case sensitive on Microsoft Windows systems. Therefore, session directories are created in the same `vault\sessions\vault_name` directory for two or more vaults that have names that differ only in case.
Vault Vendor	The name of your off-site vault vendor (for example, Iron Mountain). If you select Iron Mountain, you also can configure Vault to put media lists into a file formatted in compliance with Iron Mountain's electronic processing specification. You can then send this file to Iron Mountain for electronic processing of the media lists. See "Reports tab (Profile dialog box)" on page 65.

Media access ports dialog box

This dialog box applies to ACS robots in NetBackup Enterprise Server only. Use it to configure the media access ports (MAPs) to use for eject operations.

About creating profiles

After you configure vaults, you can create and configure profiles with the **Profile** dialog box.

See the following to create and configure Vault profiles:

- See "Profile dialog box" on page 50.
- See "About the number of profiles required" on page 50.
- See "Creating a profile" on page 51.

Profile dialog box

A Vault profile is a template for a vault job; it contains the rules for selecting, and ejecting media. A profile is associated with a specific vault, and at least one profile must exist for every vault. A vault can contain multiple profiles, although two profiles within the same vault cannot run simultaneously. Two different profiles can run simultaneously if each profile is in a different vault and if each profile uses a different off-site volume pool.

All profiles select images (that is, Choose Backups).

You must select at least one of the following profile options when you create a new Vault profile:

- **Catalog Backup**
- **Eject**
- **Reports** (mandatory)

The other options are optional so you can separate the Vault tasks into separate jobs if desired, using different jobs to accomplish different tasks. For example, you can use one job to select and duplicate images daily, and another job to eject media and generate reports weekly.

You can select or deselect any of these profile options at any time during the configuration process.

After you create a profile, use a Vault policy to schedule when it should run.

See "About scheduling a Vault session" on page 70.

About the number of profiles required

The number of profiles that are required depends on your operations. If you have more than one Vault, you have more than one profile.

To determine the number of profiles that you need, use the following criteria:

- If you vault original images, you may require only one profile to choose backups, eject media, and generate reports.

Creating a profile

Once you have determined the number of profiles needed to accommodate the vault operations, you are ready to create the first profile using the **New Profile** dialog box.

To create a profile

1. Select a vault in the NetBackup Web UI. From the **Actions** menu, choose **Add profile**.
2. In the **Add profile** dialog box, specify / select the required configurations.

   Profile name is case-sensitive.
3. Select the steps you want this profile to perform.

   You must select at least one step. However, you can change the selections when you configure the profile. Because you must always configure the choose backups step, it is not displayed on this dialog box.
4. Click **Save**.

Configuring a profile

The **New Profile** dialog box includes the following five tabs:

Table 5-6 New Profile dialog box options

Property	Description
Choose backups tab	Enables you to specify the criteria for selecting backup images.
Catalog backup tab	Enables you to choose which catalog backup policy and schedule to use for creating a Vault catalog backup. For efficient disaster recovery, vault a new catalog backup each time you vault data.
Eject tab	Enables you to choose in which off-site volume pools Vault should look for the media you want to eject.
Reports tab	Enables you to choose which reports to generate.

A profile must select images (Choose Backups). The other steps are optional so you can separate the tasks into separate jobs if you want, using different jobs to accomplish different tasks. For example, you can use one profile to select and another profile to eject media and generate reports weekly.

About configuring a profile using the Choose Backups tab

Use the **Choose Backups** tab to configure the search for images to be vaulted. The most basic criterion you can set is the time frame. To refine the search for images to vault, the default setting of these two criteria is for the check boxes to be unselected, which means all criteria in that particular field is included in the search for an image to vault.

Vault compares images in the NetBackup database with the criteria defined in the **Choose Backups** tab and generates a list of images that match the criteria. The image selection process chooses all images in the NetBackup catalog that match the criteria.

See "Choose Backups tab configuration options" on page 52.

See "About the list of images to be vaulted" on page 75.

See "About overlapping the time window in the profile" on page 22.

Choose Backups tab configuration options

Table 5-7 describes the options that you can use in the **Choose Backups** tab to configure a profile.

Table 5-7 Choose Backups tab configuration options

Property	Description
Attribute	A filter enabling you to choose which logical attributes you want to use when searching for an image to vault. By default, if the check box is not checked, all criteria in this field are included in the search.
Backup Policies	A list of policies to use to select backup images. Enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. To change the backup policies, click **Change** and then choose the backup policies you want to include in the profile. Policies are based on the storage unit that is used for backups. Because storage units are related to a specific robot number, choose the policies by robotic device.

Table 5-7 Choose Backups tab configuration options *(continued)*

Property	Description
Backups Started	The period of time from which the profile selects backups relative to the start time of the session. Time is expressed in terms of days and hours, relative to the time of the session. For example, assume the following settings: ■ between 8 day(s) 0 hour(s) ago ■ and 1 day(s) 0 hour(s) ago If the session is started on October 12 at 1:00 P.M., count backward from October 12. The vaulted backups are those started between October 4 at 1:00 P.M. (eight days before) and October 11 at 1:00 P.M. (one day before). If you select original backup images to send off site, the default time range is between eight days and one day before the session runs. If you duplicate images, the default time range is between seven days and zero days.
Basic disks	A list of basic disk paths, in the form of <server>:<path>. Selecting Basic disks refines your search to those paths that are selected. An image is selected for duplication or vaulting if its primary copy resides in any of the selected basic disk paths. **Note:** An individual basic disk from this list would also display the storage unit name in parenthesis, for example, <server>:<path> (storage unit). This option is enabled if you select this criteria in the **Location** field, or by default if the **Location** check box is not checked. To change the basic disks, click **Change** and then choose the basic disks that you want to include in this profile. By default, the **Include all basic disks** is selected. An image is selected for duplication or vaulting if its primary copy resides in any of the specified basic disks.
Change	Option used to display a dialog box to change any of the criteria selected in the **Attribute** or **Location** fields.
Clients	The clients for which to select backup images. Enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. To change the clients, click **Change** and then choose the clients you want to include in this profile.
Disk pools	A list of disk pools that you can choose search for an image to duplicate or vault. Enabled if you select this criteria in the **Location** field, or by default if the **Location** check box is not checked. To change the disk pools, click **Change** and then choose disk pools that you want to include in this profile. By default, the Include all disk pools is selected. An image is selected for duplication or vaulting if its primary copy resides in any of the specified disk pools. **Note:** An individual disk pool from this list would also display the storage unit name in parenthesis, for example, disk pool (storage unit).

Table 5-7 Choose Backups tab configuration options *(continued)*

Property	Description
Location	A filter enabling you to choose which physical location you want to search for an image to vault. By default, if the check box is not checked, all criteria in this field are included in the search.
Media servers	The media servers from which to select backup images. This option is enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. (Applies to NetBackup Enterprise Server only.) An image is selected for duplication or vaulting if the media server of the primary copy matches any of the values selected in the list. To change the media servers, click **Change** and then choose the media servers you want to include in this profile.
Retention levels	A list of retention levels that you can use to further refine your search criteria. An image is selected for duplication or vaulting if the retention level of the primary copy matches any of the values selected in the list. Enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. To change the retention level, click **Change** and then choose the level or levels that you want to include in this profile. By default, the **Include all retention levels** is selected.
Schedules	A list of schedules to use to select backups. Enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. To change the default, click **Change** and then choose the schedules you want to include in this profile. Schedules are based on the storage unit used for backups. Because storage units are related to a specific robot number, choose the schedules by robotic device.
Source Volume Groups	This selection criterion contains a list of **Volume Groups** from which to select backup images. Enabled if you select this criteria in the **Location** field, or by default if the **Location** check box is not checked. To change the default, click **Change** and then choose the volume groups you want to include in this profile. Selecting **Source Volume Groups** restricts the search for images to those in either all volume groups or the specific volume groups that you choose to include in your search. Usually, a **Source Volume Group** is specified if your primary server has access to multiple robots and you want to duplicate the images that reside on media in one robot to media in another robot. The images that are read are in the **Source Volume Group** in one robot. The images are written to media in the **Robotic Volume Group** in another robot. An image is selected for duplication or vaulting if any fragment of its primary copy is found in a media that is from any of the selected volume groups. **Note:** If you want to exclude all tape images from this profile, select the **Exclude All** check box. This means there is no effect of the selection from **Volume Pools** criterion as both of them apply to tape images. So, if you select **Exclude All** for "source volume groups," it automatically means **Exclude All** for "volume pools" as well.

Table 5-7 Choose Backups tab configuration options *(continued)*

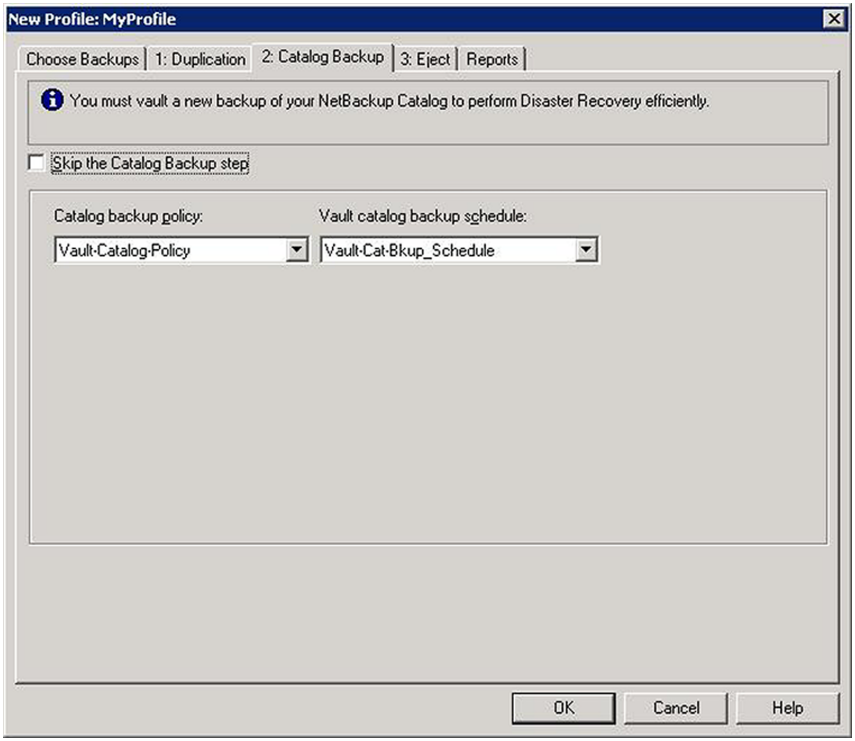
Property	Description
Backup Types	The types of backups (full, incremental, and so on) the profile captures. Enabled if you select this criteria in the **Attribute** field, or by default if the **Attribute** check box is not checked. To change the default, click **Change** and then choose the backup types you want to include in this profile. Depending on the different types of backups you configured in NetBackup policy management, you can choose the backup type. Only those types for which you configured policies are available for selection. If you want to vault all types of backups, accept the default. This criterion is optional.
Volume pools	A list of volume pools that you can choose to include in your search for an image to duplicate or vault. Enabled if you select this criteria in the **Location** field, or by default if the Location check box is not checked. To change the volume pools, click **Change** and then choose the volume pool or pools that you want to include in this profile. By default, the **Include all Volume pools** option is selected. To change the default, click **Change** and then choose the volume pools you want to include in this profile. Selecting Volume pools restricts the search for images to those in either all volume pools or just the volume pools that you choose to include in your search. An image is selected for duplication or vaulting if any fragment of its primary copy is found in a media that is from any of the selected volume pools. **Note:** To exclude all tape images from this profile, select **Exclude All** check box. This means there is no effect of the selection from "Source Volume Groups" criterion as both of them apply to tape images. So, if you select **Exclude All** for "volume pools" it automatically means **Exclude All** for "Source Volume Groups" as well.

Catalog backup tab (Profile dialog box)

Use the **Profile** dialog box tab to specify the catalog backup policy and schedule that performs the Vault catalog backup. At least one Catalog policy that includes a Vault Catalog Backup schedule must exist so you can specify them on the **Catalog Backup** tab.

Vault uses the online, hot catalog backup method, which can back up the catalogs even when other NetBackup or Vault activity is occurring. (NetBackup provides two types of catalog backup; the other type is an offline, cold catalog backup that cannot occur when regular backup activity is occurring.)

You must add the Vault catalog backup volume pool to the eject list on the **Eject** tab.



See "About off-site volume pools" on page 33.

See "About creating catalog backup schedules for Vault" on page 35.

The following topics provide additional information about Vault catalog backups:

- See "About Vault catalog backups" on page 56.
- See "Catalog backup policy settings" on page 57.
- See "About critical policies " on page 58.
- See "Catalog backup tab configuration options" on page 58.

About Vault catalog backups

NetBackup catalogs are databases that contain information about the NetBackup configuration and backups, including the files that are backed up and the media on which they are stored. Vault creates a new catalog backup with up-to-date information. It does not duplicate an existing NetBackup catalog backup. A NetBackup catalog backup is not a substitute for a Vault catalog backup because it does not include the latest information about duplicated media and media location. Therefore, you should perform a catalog backup in Vault.

To perform a Vault catalog backup, Vault uses a special schedule of type Vault Catalog Backup in an Catalog policy. (NetBackup uses a special backup policy of type Catalog to perform catalog backups.)

A Vault catalog backup occurs when a profile that performs catalog backup runs. It does not occur on the schedule that is defined in the NBU-Catalog policy. A Vault Catalog Backup schedule always performs a full backup of the entire NetBackup catalog.

You can create multiple copies concurrently of a Vault catalog backup.

Vault does not duplicate existing catalog images, but it ejects the media on which those images are stored if both of the following are true:

- Those images are selected during the choose backups step.
- The media is assigned to the dedicated Vault catalog volume pool.

If the catalog backup fails but the remainder of the Vault job succeeds, the session ends with a status 294 (vault catalog backup failed). Data is vaulted with no associated catalog backup. Cohesity believes that it is better to vault the data without a catalog backup than to fail the job and vault nothing at all for that session.

The Recovery Report for Vault shows the three most recent Vault catalog backups. If you vault your regular NetBackup catalog backups, they do not appear on the Recovery Report but do appear on other reports.

Catalog backup policy settings

Although you configure only two options on the **Catalog Backup** tab, settings in the catalog backup policy affect the Vault catalog as follows:

Table 5-8 Catalog backup tab configuration options

Property	Description
Job priority	The catalog backup job competes for resources with other backup jobs. You can specify the priority for the job, either on the policy Attributes tab (single catalog backup) or on the **Configure Multiple Copies** dialog box of the Vault Catalog Backup schedule.
Destination	You can send the catalog backup to any storage unit, including disk and removable media storage units. Specify the destination in the Vault Catalog Backup schedule.
Volume pool	If you use removable media storage units, you must specify a volume pool for the catalog backup in the Vault Catalog Backup schedule. You also must specify the same volume pool on the **Eject** tab of the profile.

Table 5-8 Catalog backup tab configuration options *(continued)*

Property	Description
Number of copies	You can create multiple copies of the catalog, and you can send them to any storage unit that is attached to the destination media server. Specify multiple copies on the **Vault Catalog Backup** schedule **Attributes** tab and then specify the number of copies on the **Configure Multiple Copies** dialog box.
Critical policies	Beginning with NetBackup 6.0, you do not specify the catalog files to include in the Vault catalog backup, and you cannot add other files to the catalog backup. A new NetBackup catalog policy option, critical policies, lets you select policies that should be recovered before backups from other policies are recovered. Specify critical policies on the policy **Disaster Recovery** tab.

About critical policies

A new NetBackup catalog policy option, critical policies, lets you select policies that should be recovered before backups from other policies are recovered. The media that contains the backup images from those critical policies are listed in the new NetBackup disaster recovery report. (Vault does not include critical policy data in its catalog backups.)

The media from those critical policies also is listed in the Vault Recovery Report so you can recall the media from those policies and recover that data before you recover data that is not as critical.

You can even recover the critical policies data before you recover the entire catalog. During catalog recovery, partial recovery of the catalog is possible. Partial recovery means you can choose which parts of the catalog backup to restore and in what order. Partial recovery lets you restore part of the catalog, then restore data from critical policies, and finally restore the remainder of the catalog.

If you want to include certain critical policies in your Vault catalog backup but not your regular NetBackup catalog backup, you need a separate NBU-Catalog policy for Vault.

For information about specifying critical policies in an NBU-Catalog policy, see the *NetBackup Administrator's Guide, Volume I*.

Catalog backup tab configuration options

The following are the configuration options for the **Catalog Backup** tab:

Table 5-9 Catalog backup tab configuration options

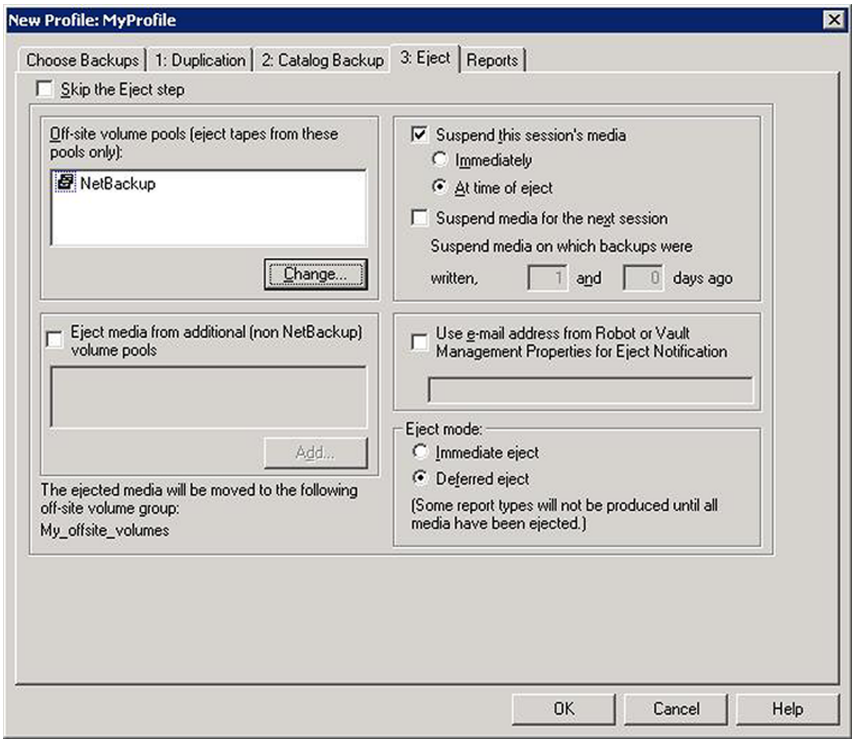
Property	Description
Catalog Backup Policy	The catalog backup policy to use. The drop-down list includes all catalog backup policies that have a Vault Catalog Backup schedule.
Vault Catalog Backup Schedule	The schedules available for the catalog backup policy. The drop-down list includes all Vault Catalog Backup schedules for the policy selected in **Catalog Backup Policy** field.
Skip the Catalog Backup Step	Select if you do not want to back up and vault the NetBackup and Media Manager catalogs.

Eject tab (Profile dialog box)

Use the **Profile** dialog box **Eject** tab to specify the following:

- Volume pools from which to eject media.
- Suspend option. By default, Vault suspends media when it is ejected. Vault only suspends the volumes in volume pools specified in the off-site volume pools list.
- When to eject the media (immediately when the profile runs or later).
- Email addresses for eject notification.

If you create catalog backup media in a profile in which you eject media, you must add the appropriate catalog volume pool to the off-site volume pools eject list.



About media ejection

During media ejection operations, Vault moves the media to be ejected into the default media access port (MAP) of the robotic library. You must extend the MAP, remove the media, and then retract the MAP. If more media is ejected, Vault continues to fill the MAP until all media are ejected. For libraries that have separate MAP doors such as libraries connected by pass-through mechanisms, NetBackup treats all doors as one continuous MAP. In other words, each time you are prompted by NetBackup, open all the doors, empty all the MAPs, and then close all the doors.

For ACS robots that have multiple MAPs, you can specify the MAPs to eject media to when you configure the robot in Vault.

If you use a library that does not have a MAP, you must remove the media from the library slots manually. You also have to perform the eject operation in Vault so that the appropriate database entries are completed. Although you can use automatic eject, Cohesity recommends that you use deferred eject to avoid resource contention with other NetBackup activity and you do not neglect to remove the media from the robot. The manual eject operation serves as a reminder to remove the media.

To use deferred eject for a library that does not have a MAP, do the following:

- Configure the profiles for deferred eject.
- Eject the media manually.
  See "About ejecting media" on page 75.
- Remove the media from the library slots.

Do not inventory the robot until you remove the media from the MAP or library slots. If you do, you have to revault the media.

About ACS MAP

The following applies to NetBackup Enterprise Server only.

Automated cartridge system (ACS) robots can have multiple library storage modules (LSMs), each with multiple media access ports (MAPs). When you configure a vault that uses an ACS robot, you can specify any MAP or a subset of MAPs to use for media ejection. Vault ejects media to as few of the configured MAPs as possible based on a nearest MAP algorithm. The algorithm considers the volumes to be ejected, the MAPs configured for ejecting in the vault, and the configuration of the LSMs. The algorithm assumes that the LSMs are connected in a line.

The **Any MAP** option does not mean all MAPs; media are not ejected to all MAPs, media are ejected to the nearest MAP in each LSM.

If you specify any MAP:

- MAPs that have only one element are not used.
- Vault selects from MAPs that are on-line when the eject begins; MAPs that are offline are not considered for eject operations.
- If only a subset of MAPs are used during ejection, all MAPs are busy and unavailable. For example, if the media are ejected to only two MAPs in one LSM, all MAPs are still busy.

For all other robot types that have MAPs, media are ejected to the default MAP. NetBackup does not support ejecting to multiple MAPs for other robot types.

About eject mode (immediate or deferred)

You can eject media immediately when the profile runs or defer ejection. If you defer eject, you also should defer reports.

If you select deferred eject, other actions are required to eject the media for the session. After the session ends, you can eject media for one session, for multiple sessions, or for all sessions.

Eject for one session only, as follows:

- Eject media for the session.

- Use the Vault Operator Menu to eject media for the session.
- Use the `vlteject` command to eject media for the session.
- Create a Vault policy and enter the appropriate `vlteject` command and options in the file list.

Eject for multiple sessions for a specific profile, as follows. (This method for duplicating and ejecting media provides the added benefit of consolidated reports that are not organized by session.)

- Configure a Vault profile to do the catalog backup and eject steps. Configure a Vault policy to run this profile on the day you want the media ejected.

Eject for all sessions for a specific vault or for all sessions for all vaults (consolidated eject) by doing one of the following:

- Use the NetBackup Web UI.
- Use the Vault Operator Menu.
- Use the `vlteject` command.
- Create a Vault policy and enter the appropriate `vlteject` command and options in the file list.

If you defer eject operations, you also should defer reports until you eject media.

About media ejection timeout impact

The media ejection timeout period is the amount of time the eject process waits for the removal of the ejected media from the media access port (MAP) before an error condition occurs. The timeout period varies depending on the capability of each robot.

Table 5-10 shows the ejection timeout periods for robots.

Table 5-10 Media ejection timeout period for Vault

Robot	Timeout period	Note
Automated Cartridge System (ACS)	One week	Applies to NetBackup Enterprise Server only
Tape Library DLT (TLD)	One week	
Robots that do not have MAPs	None	

For robots that do not have timeout periods or do not have MAPs, select deferred eject and then eject the media manually. When you eject the media, ensure that

the media are removed from the library in a timely manner so that other operations can occur.

Status messages that are displayed provide information about the status of inject, eject, or inventory operations.

Note: If media are not removed and the timeout period expires, the Vault reports do not accurately show the status of the media. To recover, you should use the Vault Operator Menu (`vltopmenu`) or `vlteject` to eject the media that was not removed from the library and generate the reports.

Eject tab configuration options

Table 5-11 lists the configuration options for the **Eject** tab.

Table 5-11 Eject tab configuration options

Property	Description
Select off-site volume pools	The option that is used to add a volume pool to the eject list. If you click **Select off-site volume pools**, the **Select a volume Pool** dialog box appears, in which you can add or remove volume pools from the eject volume pool list.
At Time of Eject (Suspend this Session's Media)	Suspend the media when it is ejected. If you also select deferred eject, images can be written to the media until it is ejected. Select this option if you want the media sent off-site to be full. Suspend at time of eject is the default.
Deferred (Eject Mode)	Defer media ejection until a later time. The reports that are marked with an asterisk (*) on the **Reports** tab are generated only when all media selected by the profile have been ejected.
Immediate (Eject Mode)	Eject media immediately as part of the current Vault job. The reports that are marked with an asterisk (*) on the **Reports** tab are generated only when all media selected by the profile have been ejected.
Immediately (Suspend this Session's Media)	Suspend the media during the current session. No more images are written to the media even if ejection is deferred.

Table 5-11 Eject tab configuration options *(continued)*

Property	Description
Use Email Address from Robot or Vault Management Properties for Eject Notification	Select to send the eject notification email to the email addresses configured on the **Vault Robot** dialog box or **Vault Management Properties** dialog box. Eject notification is sent when the eject process begins and ends. To send the notification email to different address, enter the email addresses in the field below the **Use Email Address...** checkbox. Eject notification is configured for each profile on the **Eject** tab, for each robot on the **Vault Robot** dialog box, and globally for Vault on the **Vault Management Properties** dialog box **General** tab. Vault sends the notification to the first email addresses found in that order. You can configure different addresses in each place.
Off-site Volume Pools	The names of the volume pools from which to eject media. Only the media in the pools that contain images that meet the selection criteria are ejected. If you create catalog backup media in a profile in which you eject media, you must add the appropriate catalog volume pool to the off-site volume pools eject list. If you use a `vlt_ejectlist_notify` script to eject media that is not created by NetBackup or Vault, you must add the volume pool in which that media resides to the **Off-site Volume Pools** list of the profile that you run to eject that media. See "About using notify scripts" on page 96.
Skip the Eject Step	Select if you do not want to eject media with this profile.
Suspend Media for the Next Session (Suspend Media on Which Backups Were Written)	Select to suspend original backup media. Then enter the number of days before the Vault job to suspend media. Use this option only if you vault original images and want to prevent NetBackup from writing partial images on backup media. Carefully consider whether to use this option. It uses extra CPU cycles because it queries all of the databases again and applies all of the Choose Backups filters again to select media to suspend. Also, this option does not suspend media that is in use, such as media to which NetBackup is writing backup images. This option suspends duplicate media that is created by Vault. However, the **Suspend this Session's Media** option is a better choice for suspending duplicate media because it does not use CPU cycles to select media to suspend. See "About avoiding vaulting partial images" on page 24.
Suspend this Session's Media	Select to suspend media in the eject list, then select either **Immediately** or **At Time of Eject**. Suspend at time of eject is the default.

Reports tab (Profile dialog box)

Use the **Reports** tab to select which reports to generate for the profile, where to distribute them, and when to generate them (immediately when the profile runs or deferred until later).

You and your off-site storage vendor can use the reports to determine which media should be moved between your site and the off-site storage location and the timing of the moves.

Reports can be generated for one session or for multiple sessions (known as consolidating your reports and ejections).

Note: You must specify a destination so that reports are generated.

By default, the report files are stored in the following path:

- UNIX

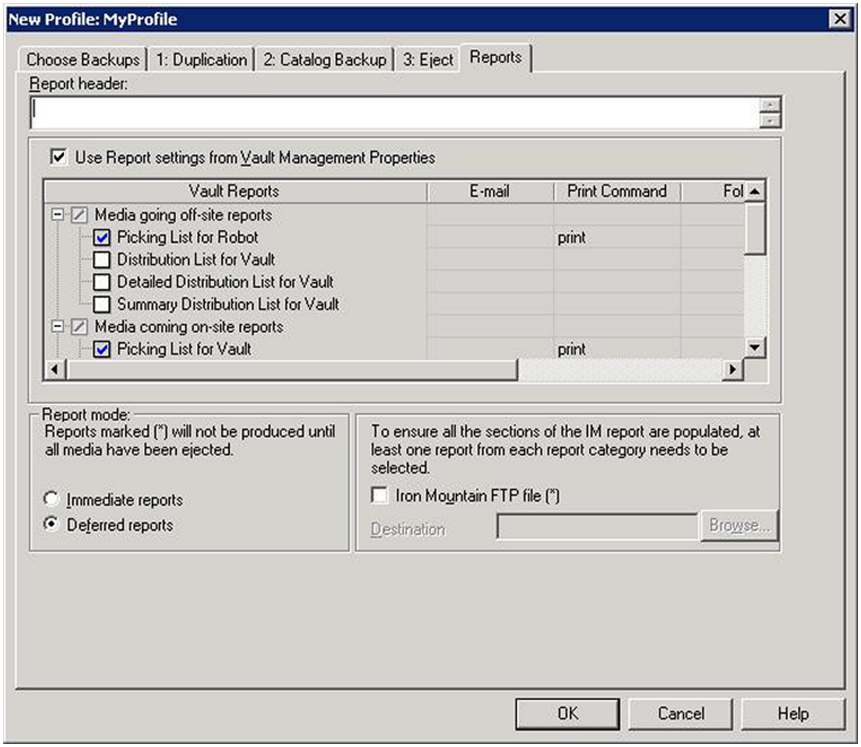
  `/usr/openv/netbackup/logs/user_ops/vault/vault-xxx`

- Windows

  install_path`\NetBackup\logs\user_ops\vault\vault-`*xxx*

If you specify a different directory other than the default directoy for saving the report, the report files are saved as per the following applicable naming rules:

- `picklist_robot_sidXX_XXXXXXXXX.rpt`
- `picklist_vault_sidXX_XXXXXXXXX.rpt`



See “Changing report properties” on page 68.

Generating reports is optional.

See “About report mode (immediate or deferred)” on page 66.

See “Reports that depend on eject” on page 67.

See “Reports tab configuration options” on page 67.

See “Changing report properties” on page 68.

About report mode (immediate or deferred)

Similar to the eject mode, you can specify whether reports should be generated immediately when the profile runs or deferred until later. If you defer eject, you should also defer reports. If you defer reports, you must perform or schedule another action to generate the reports.

Because some reports are generated only when media are ejected, you may choose to defer reports until the media are ejected. For example, if you duplicate images

daily and eject media weekly, you can defer reports for the profile that duplicates images and use the profile that ejects media to generate reports.

If the corresponding eject process has completed when you generate reports, all pending reports are generated and distributed. Those reports are not regenerated if you run deferred reports again. If eject has not completed, the subset of reports that do not depend on completion of eject are generated. Those reports are generated again if deferred reports are ran again.

If you defer reports from multiple sessions and then generate them together, the progress is known as consolidating reports.

Reports that depend on eject

Reports can be generated from on the **Reports** tab of the **Profile** dialog box. Reports marked with an asterisk (*) on the **Reports** tab are generated only when all media that is selected by the profile are ejected. The reports for media coming on-site are not dependent on the media being ejected before they are generated.

Reports that you can generate from the **Profile** dialog box **Reports** tab are as follows:

- Reports for media coming on-site
  - Picking List for Vault
  - Distribution List for Robot
- Inventory reports
  - Vault Inventory
  - Off-site Inventory
  - All Media Inventory)
- Recovery Report for Vault

Reports tab configuration options

The following are the **Reports** tab configuration options.

Table 5-12 Reports tab configuration options

Property	Description
Deferred Reports	Defer generating the reports until after the session has completed (for example, if you run Vault sessions daily and eject media weekly). Deferred is the default. Reports marked with an asterisk (*) are generated only when all media that is selected by the profile are ejected.
Immediate Reports	Generate the reports immediately as part of the current vault session. Reports that are marked with an asterisk (*) are generated only when all media that is selected by the profile are ejected.
Iron Mountain FTP File	If you selected Iron Mountain as your Vault vendor (in the **New Vault** dialog box), Iron Mountain FTP file and Destination folder items appear. To generate a file that you can send by FTP to Iron Mountain, select Iron Mountain FTP file and enter the name or browse to choose the Destination folder to which the file is written. Sending the file to Iron Mountain is not part of the vault process.
Report Header	If you want certain text to appear at the top of every report, enter it in the **Report Header** box. The header appears on all reports.
Use Report Settings from Vault Management Properties	Select to use the report settings configured in the **Vault Management Properties Reports** tab.

Changing report properties

Use the following procedure to change report properties (title, email destination, printer to use, and directory to save it to).

To change report properties

1. Select the required report.
2. Click kebab menu and select **Edit**. **Edit report properties** dialog box is displayed. Modify the required parameters and click **Save**.

Chapter 6

Vaulting and managing media

This chapter includes the following topics:

- About Vault sessions
- About previewing a Vault session
- Stopping a Vault session
- About resuming a Vault session
- About monitoring a Vault session
- About the list of images to be vaulted
- About ejecting media
- About injecting media
- About using containers
- Revaulting unexpired media
- About tracking volumes not ejected by Vault
- About notifying a tape operator when an eject begins
- About using notify scripts
- About clearing the media description field
- Restoring data from vaulted media

About Vault sessions

A Vault session or vaulting job is the process of running the steps that are specified in a Vault profile. Before you can run a Vault session, you must configure at least one robot, one vault, and one profile.

For additional information about Vault sessions, refer to the following:

- See "About scheduling a Vault session" on page 70.
- See "About running a session manually" on page 72.
- See "About running multiple sessions simultaneously" on page 72.

You also can run a vault session by using the Vault Administration menu interface (UNIX systems only).

See "About the Vault administration interface" on page 131.

About scheduling a Vault session

To run a vault session automatically at a specific day and time, use a Vault policy. A Vault policy is a NetBackup policy that is configured to run Vault jobs; a Vault policy does not back up client systems. The policy includes the schedule for when the Vault session should run (day or date and time window) and the command to run a Vault profile.

How you schedule your sessions depends on how you conduct operations as follows:

- A Vault policy can run a profile that ejects media containing the original images that were created during a backup job. If you create multiple original backup images concurrently, you can assign one or more of the original images to an off-site volume pool. A separate Vault policy can run a Vault job that ejects the media on which those images are stored.
- A Vault policy can run a profile that selects images and ejects the media on which those images are stored. That policy can perform both operations daily or at some other interval that meets your requirements. If your vault vendor arrives daily to pick up media or you remove the off-site media from your robot immediately, you may need only one policy for that vault.

See "About media ejection recommendations" on page 29.

See "Creating a Vault policy" on page 70.

Creating a Vault policy

Setting up a Vault policy differs from setting up a regular policy in NetBackup, as follows:

- First, you must specify Vault as the policy type.
- Second, you do not specify clients for Vault policies.
- Third, rather than specifying files to back up on the **Backup Selections** tab, you specify one of two Vault commands to run.
  - Use the `vltrun` command to run a Vault session. You specify the robot, vault name, and profile for the job. The `vltrun` command accomplishes all the steps necessary to vault media. If the profile is configured for immediate eject, media are ejected and reports are generated. If the vault profile name is unique, use the following format:

    ```
    vltrun profile_name
    ```

    If the vault profile name is not unique, use the following format:

    ```
    vltrun robot_number/vault_name/profile_name
    ```

  - Use the `vlteject` command to eject media or generate reports for sessions that are completed already and for which media have not been ejected. The `vlteject` command can process the pending ejects or reports for all sessions, for a specific robot, for a specific vault, or for a specific profile. For example:

    ```
    vlteject -vault vault_name -eject -report
    ```

Note: Include one Vault command only in a Vault policy. If you use more than one command, the first command is initiated and the successive commands are interpreted as parameters to the first command. Failure may occur and images may not be duplicated or vaulted.

See "Ejecting media by using a Vault policy" on page 80.

For more information about the `vlteject` and the `vltrun` commands, see the *NetBackup Commands Reference Guide*.

Note: If you create a vault policy by copying a regular NetBackup policy that has a client list configured, delete all the clients in the client list before you run the policy. If you do not, Vault creates one vault job for every client in the list even though the client is not used by the Vault job. The first vault job operates as a normal vault session; the rest terminate with a status 275 (a session is already running for this vault).

To create a Vault policy, navigate to *Protection* > *Policies*. Click **Add** and specify the required parameters.

For more information about creating NetBackup Vault policies, see the *NetBackup Web UI Administrator's Guide*.

About running a session manually

You can run a Vault session manually either by using the NetBackup Web UI to initiate the session or by invoking the veteran command from the command line.

See "Running a session from a command line" on page 72.

Running a vault from the NetBackup Web UI

To run a Vault session from the NetBackup Web UI, you either run the policy manually or run the profile manually.

To manually run the policy, navigate to *Protection* > *Policies*. Select the appropriate policy and click **Manual backup**.

Running a session from a command line

Use the following procedure to run a vault session from a command line.

To run a vault session from a command line

1. Add the path in which the NetBackup executable files are installed to your `PATH` environment variable
2. Run `vltrun` from a command line, specifying the robot number, vault, and profile as in the following example:

```
vltrun robot_number/vault_name/profile_name
```

Alternatively, you can specify only the profile if it has a unique name.

See the *NetBackup Commands Reference Guide*.

About running multiple sessions simultaneously

Multiple Vault sessions can run at the same time. Vault uses a global setting **Maximum Vault Jobs** as a threshold for queuing jobs from any vault. A Vault job runs if resources are available and the maximum number of Vault jobs has not been reached. If resources are not available to run jobs, Vault queues jobs until the resources are available.

Vault queues jobs as follows:

- If **Maximum Vault Jobs** is reached, any subsequent vault job is queued and its status is shown as Queued in the Activity Monitor.
- If a job needs to eject media and another job from any vault is ejecting media in the same robot, the job is queued and shown as Active in the Activity Monitor.

Queued jobs are scheduled or run when the resources that are required for them become available.

For jobs that run simultaneously, the following restrictions exist:

- Vaults should not share on-site and off-site volume pools. Profiles within the same vault can use the same volume pools, but profiles from one vault cannot use the same volume pools as profiles from another vault.
- Vaults should not share off-site volume groups. Profiles within the same vault can use the same off-site volume groups, but profiles from one vault cannot use the same off-site volume groups as profiles from another vault.

About previewing a Vault session

Before you run a Vault session, you can preview the session to verify that the profile selects the appropriate images for off-site storage. To preview a session, use the `vltrun` command with the `-preview` option, specifying the robot number, vault, and profile as in the following example:

```
vltrun robot_number/vault_name/profile_name -preview
```

Alternatively, you can specify only the profile if it has a unique name.

The `vltrun -preview` option starts a new vault job and performs a search on the image catalog based on the criteria that is specified on the profile **Choose Backups** tab. Then `vltrun -preview` writes the names of the images to a `preview.list` file and exits. Vault does not act on the images selected.

After you run the preview option, examine the `preview.list` file, which is located in:

- UNIX:

  `/usr/openv/netbackup/vault/sessions/vault_name/sidxxx`

- Windows:

  `install_path\NetBackup\Vault\sessions\vault_name\sidxxx`

Under certain circumstances, the `preview.list` file may contain more backup images than are vaulted:

- If the profile is configured to duplicate only disk images, selected images on removable media are not vaulted.
- If images in the list do not have a copy on media in one of the Off-site Volume Pools listed for the eject step, they are not vaulted.

Stopping a Vault session

You can use Activity Monitor to stop a Vault session. The Activity Monitor must be configured to show the Vault fields.

To stop a vault session

1. In the Activity Monitor, select the vault session you want to stop.
2. From the **Action** menu, select **Cancel Job**.

   If a vault session fails, you cannot run a new session until the old session ends. Use **Cancel Job** to end the failed session.

About resuming a Vault session

If a Vault job fails, refer Activity monitor or the notification of the session status. If enough information cannot be determine the cause of the problem, examine the other log files.

See "Debug logs" on page 139.

After you determine the cause, you can do one of the following:

- If the session reached the Eject step or attempted to generate reports before encountering problems, you can use `vltopmenu` (or `vlteject`) to finish the eject or reporting for the session.

About monitoring a Vault session

If you configure the NetBackup Web UI Activity Monitor to display the Vault fields, you can use the Activity monitor to monitor the progress of Vault jobs. For a Vault job that is initiated by the NetBackup scheduler, the **Policy** field displays the policy name. If the Vault job is run by any means other than the NetBackup scheduler, the Policy field is empty.

For more information, refer *Monitoring and notifications* section in *NetBackup Web UI Administrator's Guide*.

About the list of images to be vaulted

During a Vault session, Vault builds a list of images that are candidates for ejection.

The `preview.list` file, which resides in the session directory for the current Vault session, includes all images that match the criteria specified on the profile **Choose Backups** tab except for the following:

- If a copy of an image already is in the Off-site Volume Group, that image is not be included in the `preview.list` file. Because the images that have a copy in an Off-site Volume Group are already vaulted, Vault does not select them as candidates for vaulting.
- If the Source Volume Groups criteria in the **Locations** field on the **Choose Backups** tab is set to a specific volume group and if no copy of that image exists in that volume group, the image is not added to the `preview.list` file.

After the `preview.list` file is generated, Vault evaluates the images in it to determine if they should be ejected. Because several filters (other profile configuration options) can exclude an image from ejection, the `preview.list` file can be a superset of the images that are eventually duplicated by the session.

About ejection exclusions

Vault ejects media that are listed in the `eject.list` file. If the profile skips the duplication step and an image in `preview.list` has no copy in an off-site volume pool (configured on the **Eject** tab), it is not ejected.

About Vault resiliency

The functionality that Vault uses to build the list of images to be ejected allows Vault to do the following:

- Eject images that were not processed because of a problem during the previous run of the profile.
  See "About overlapping the time window in the profile" on page 22.

One Vault profile can vault original backup images from some NetBackup backup policies and also duplicate and vault images from other backup policies.

About ejecting media

If you configure a profile to defer ejection, you must perform or schedule another action to eject media.

You can use one of the following actions to eject media that was not ejected by a profile that selected or duplicated images:

- Manually by using the Vault management node in the NetBackup Web UI
- Manually by using the Vault Operator Menu
- Manually by using the `vlteject` command
- Automatically by creating and scheduling a Vault policy and entering the appropriate `vlteject` command and options in the file list

---

Note: You must use one of the Vault methods to eject media. If you use a NetBackup or Media Manager option to eject media, the correct database entries are not made and the Vault reports are not accurate.

For information about Vault methods to eject media, refer to the following:

- See "Previewing media to be ejected" on page 76.
- See "Ejecting media by using NetBackup Web UI" on page 77.
- See "Ejecting media by using the Vault operator menu" on page 78.
- See "Ejecting media by using the vlteject command" on page 79.
- See "Ejecting media by using a Vault policy" on page 80.
- See "Consolidating ejects and reports" on page 81.

For other related information see the following:

- See "About media ejection" on page 60.
- See "About ACS MAP" on page 61.
- See "About eject mode (immediate or deferred)" on page 61.
- See "About media ejection timeout impact" on page 62.

Previewing media to be ejected

Before you eject media, you can preview the media to be ejected. To preview that media, you can user NetBackup Web UI or the `vlteject` command.

To preview media to be ejected

1. Select **Actions > Deferred Eject**.
2. In the **Deferred Eject** dialog box, if necessary, select a vault, profile, or session ID. The options that are selected in the dialog box depend on whether you are ejecting for all vaults, for a single vault, or for a profile.
3. Click **Get Preview** and then select one or more of the profiles in the **Eject Preview** window.

To preview media to be ejected using the vlteject command

- From a command prompt, enter the `vlteject` command in the following format, specifying the robot, vault, or session for which you want to preview ejected media:

```
vlteject -preview [-vault vault_name [-profile profile_name]]
[-profile robot_no/vault_name/profile_name]
[-robot robot_no]
[-sessionid id]
```

Ejecting media by using NetBackup Web UI

Use the NetBackup Web UI to eject media and generate reports for all vaults, for a single vault, or for a profile for which media have not yet been ejected.

When you select **Deferred Eject**, the default selections on the **Deferred Eject** dialog box depend on whether you are ejecting for all vaults, for a single vault, or for a profile. From the dialog box, you can initiate the eject operation or preview the media to be ejected. The preview shows the session IDs for which the deferred eject occurs and the media IDs for each session selected. You also can select whether to generate the reports after the ejection.

To eject media using NetBackup Web UI

1. Select the vault or profile for which you want to eject media.
2. Select **Actions > Deferred Eject**.

3 In the **Deferred Eject** dialog box, select or change any of the options. The options that are selected in the dialog box depend on whether you are ejecting for all vaults, for a single vault, or for a profile.

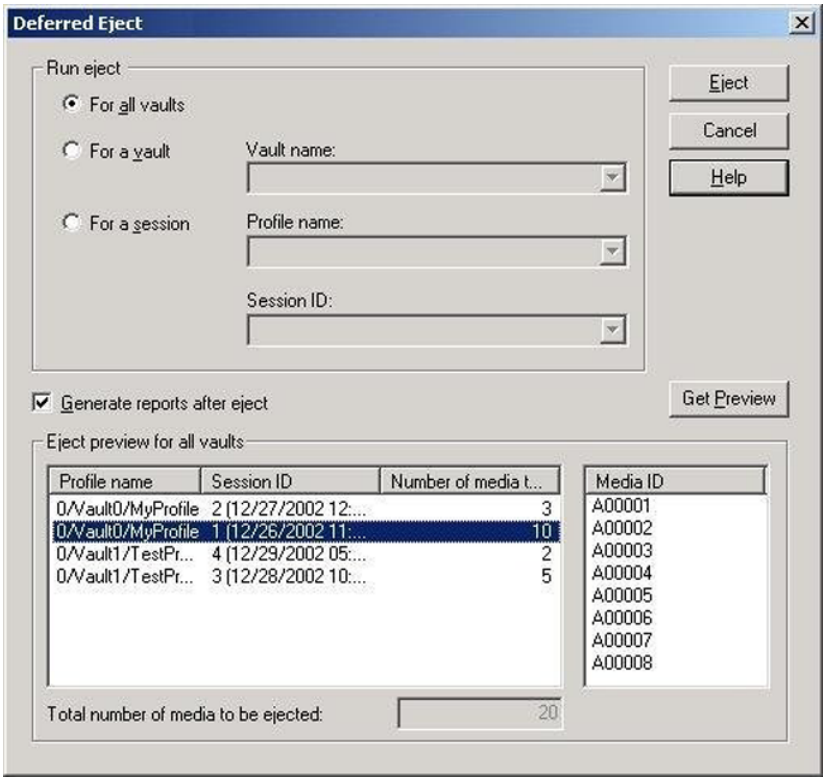
4 Click **Eject**.

To preview the media to be ejected, click **Get Preview**, and then select one or more of the profiles in the **Eject Preview** window.

To monitor the progress of or cancel the eject operation, use NetBackupWeb UI Activity monitor.

Figure 6-1 shows the Deferred Eject dialog box with all vaults selected and previewing the media that is ejected for the selected session.

Figure 6-1 Deferred Eject dialog box



Ejecting media by using the Vault operator menu

Use the **Vault Operator Menu** to eject media and generate reports for Vault sessions for which media are not yet ejected (the reports must be configured in the profiles).

The **Vault Operator Menu** calls the `vlteject` command to accomplish the media ejection. You also can use the **Vault Operator Menu** to preview the media to be ejected.

See "Vault operator menu interface " on page 132.

To eject media by using the Vault operator menu

1. Start the **Vault Operator Menu** by running the `vltopmenu` command.
2. If necessary, select a profile.
3. Select one of the following options:
   - **Eject Media for This Session**
     See "Ejecting media by using the vlteject command" on page 79.
     See "Ejecting media by using a Vault policy" on page 80.
   - **Consolidate All Ejects**
   - **Consolidate All Reports and Ejects**
     See "Consolidating ejects and reports" on page 81.

Ejecting media by using the vlteject command

Use the `vlteject` command to eject media and generate reports for Vault sessions for which media are not yet ejected (the reports must be configured in the profiles). The `vlteject` command can process the pending ejects or reports for all robots (all sessions for all vaults), for all sessions for a single vault, or for a specific Vault session.

The following is the format of the `vlteject` command:

```
vlteject -eject -report -preview [-vault vault_name]
[-vault vault_name [-profile profile_name]]
[-profile robot_no/vault_name/profile_name]
[-legacy][-robot robot_no] [-auto y|n]
[-eject_delay seconds][-sessionid id]
```

The vlteject command resides in the following directory:

- UNIX

  ```
  /usr/openv/netbackup/bin
  ```

- Windows

  ```
  install_path\NetBackup\bin
  ```

The following is a `vlteject` command example that ejects media for all robots that have sessions for which media has not yet ejected and that generates the reports:

```
vlteject -eject -report
```

The following example ejects all media that has not yet ejected for all sessions for the CustomerDB vault and generates reports:

```
vlteject -vault CustomerDB -eject -report
```

The following is a `vlteject` command example that previews the media to be ejected for the CustomerDB vault:

```
vlteject -vault CustomerDB -preview
```

See the *NetBackup Commands Reference Guide* for more information about the `vlteject` command.

To eject media by using the vlteject command

1. In a terminal window or command window, change to the directory in which the `vlteject` command resides.
2. Run the command, using the appropriate options and parameters.

Ejecting media by using a Vault policy

Use a Vault policy to eject media or generate reports for the Vault sessions that have completed already and for which media have not ejected. In the Vault policy, specify Vault as the policy type, do not specify clients, and specify the `vlteject` command on the **Backup Selections** tab.

The following is the format of the `vlteject` command:

```
vlteject -eject -report -preview [-profile profile_name]
[-profile robot_no/vault_name/profile_name]
[-robot robot_no] [-vault vault_name [-sessionid id]]
[-auto y|n] [-eject_delay seconds] [-legacy]
```

The vlteject command resides in the following directory:

- UNIX

  ```
  /usr/openv/netbackup/bin
  ```

- Windows

  ```
  install_path\NetBackup\bin
  ```

The following is an `vltejct` command example that ejects media for all robots that have sessions for which media has not yet ejected and generates the reports:

```
vlteject -eject -report
```

The following example ejects all media that has not yet ejected for all sessions for the CustomerDB vault and generates reports:

```
vlteject -vault CustomerDB -eject -report
```

See the *NetBackup Web UI Administrator's Guide*, for more information about creating NetBackup policies.

See the *NetBackup Commands Reference Guide* for more information about the `vlteject` command.

To create a Vault policy that ejects media

1. On the **NetBackup Web UI**, select **Protection** and then select **Policies**.
2. Specify the required parameters for the **Attributes** and **Schedule** tabs.
3. Select **Backup selections** tab, click **Add**. Add backup selection dialog box is displayed.
4. Specify the path and `vlteject` command and then click **Add**.
5. Click **Save**.

Consolidating ejects and reports

You can eject media from more than one vault session, which is known as consolidating ejects. For example, you may use one vault policy to duplicate media daily but eject media only at the end of the week.

If you consolidate ejects, you should also consolidate reports. Some restrictions may apply if you consolidate reports. By default, you cannot consolidate reports between vaults that use slots and vaults that use containers.

See “About consolidating reports” on page 108.

See “Eject tab (Profile dialog box)” on page 59.

See “Reports tab (Profile dialog box)” on page 65.

To consolidate ejects and reports for a profile

1. Select **Deferred Eject** on the profile **Eject** tab.

   This action ensures that tapes are not ejected automatically for each Vault session.

2. Select **Deferred Reports** on the profile **Reports** tab.

   This action ensures that reports are not generated automatically for each Vault session.

3. Eject media and generate reports by using one of the methods that are described in Ejecting media.

   See "About ejecting media" on page 75.

About injecting media

In a normal volume rotation, you have to inject media back into a robot after media expires and is returned from your off-site storage location so that it is available for reuse. You also may need to inject unexpired media for restore or disaster recovery operations.

Injecting media updates the NetBackup and Media Manager catalogs so that the correct location of the media is recorded. If the robot does not have a barcode reader to identify the media being injected, you still must use an inject option so the location of the media is updated in the databases.

How you accomplish the process of injecting the media depends on the robot library as follows:

- If your library has a media access port (MAP), you insert the media to be injected into the MAP. Then use one of the injecting options that is discussed in this topic to move that media from the MAP to the library slots. If the library has a barcode reader, the appropriate database changes are made automatically.
- If the library does not have a MAP, you insert the media into the library slots or into a cartridge which is then placed into the robot. If the library has a barcode reader, the appropriate database changes are made automatically.
- If your library does not have a barcode reader, you must use the **Move media** option so the databases are updated.

You can inject media as follows:

- See "Injecting media for libraries with and without barcode readers" on page 83.
- See "Injecting media by using the Vault Operator Menu" on page 84.
- See "Injecting media by using the vltinject command" on page 84.

The vault fields in the Media Manager database are cleared when the media are unassigned while in a robotic volume group or moved into a robotic volume group and then unassigned (that is, injected back into the robot).

The following are the Media Manager database fields dedicated to Vault information:

`vltcid`	The ID of the container (container vaulting only).
`vltname`	The name of the vault.
`vltreturn`	The date the volume or container should be returned from the off-site vault.
`vltsent`	The date the volume or container was sent off-site.
`vltsid`	The ID of the session that vaulted the volume or container.
`vltslot`	The ID of the slot in which the volume resides in the off-site vault (slot vaulting only).

Volume pool, volume group, and media description fields are used for all volumes, not only the volumes that Vault uses. So, they are not cleared when media are injected back into a robot. You can, however, configure NetBackup so that the media description field is cleared.

See "About clearing the media description field" on page 99.

Injecting media for libraries with and without barcode readers

Inject the media for the libraries that have barcode readers and libraries that do not have barcode readers.

To inject media for libraries with barcode readers

1. Insert the media into the robotic library slots or media access port.
2. On the left, select **Tape storage** and then click **Robots** tab.
3. Select the robotic library where you inserted the volume.
4. Select **Inventory robot**.
5. In the Inventory operation section, select **Update volume configuration**.
6. To configure advanced options, click **Advanced options**.
7. If your robot has a media access port into which you placed the media, select **Empty media access port prior to update**.
8. Select **Start** to start the update.
9. Repeat as necessary until all media are injected.

To inject media for libraries without barcode readers

1. Insert the media into the robotic library slots (or into the cartridge and then inject the cartridge into the robot).
2. On the left, select **Tape storage** and then click **Volumes** tab.
3. Select the volume to be injected into the library.
4. Select **Move**.
5. Select or enter the robot, volume group, and slot number.

   Use the **First slot number** field to enter the slot into which you placed the volume.
6. Select **Move** to move the volume.
7. Repeat as necessary until all media are injected.

Injecting media by using the Vault Operator Menu

You can use the Vault Operator Menu to inject media. The Vault Operator Menu calls the `vinject` application programming interface (API) to inject the media.

Note: Ensure that all the media in the MAP are from the current vault (that is, the vault for the currently selected profile in `vltopmenu`). If they are not, inject fails.

To inject media by using the Vault Operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. If necessary, select a profile.
3. If necessary, select a session.
4. Load the media in the robot's media access port.
5. Select **Inject Media into Robot**.
6. Repeat until all media are injected into the robot.

   See "Vault operator menu interface " on page 132.

Injecting media by using the vltinject command

The `vltinject` command injects volumes into a robot and updates the Media Manager volume database. It requires as an option the name of a profile (if unique) or a robot number, vault, and profile name.

The following is the format of the `vltinject` command:

```
vltinject profile|robot/vault/profile
```

The following example command injects volumes that were vaulted by the Payroll profile and that were returned from the off-site vault:

```
vltinject Payroll
```

Note: If you use the same profile name across vaults in your vault configuration, then you should specify the *robot/vault/profile* attributes.

The following example injects volumes that were vaulted by the Weekly profile in the Finance vault and that were returned from the off-site vault:

```
vltinject 8/Finance/Weekly
```

See the *NetBackup Commands Reference Guide* for more information about the vltinject command.

To inject media by using the vltinject command

1. In a terminal window or command window, change to the directory in which the vltinject command resides, as follows:
   - UNIX

     ```
     /usr/openv/netbackup/bin
     ```

   - Windows

     ```
     install_path\NetBackup\bin
     ```

2. Load the media to be injected into the robot's media access port.
3. Run the command, using the appropriate options and parameters.
4. Repeat until all media are injected.

About using containers

A container is a box in which you can place media and then transfer that box to your off-site storage location. When you configure a vault, you select whether the media are stored in containers or slots at your off-site storage location. Vault tracks, reports, and recalls your media regardless of how the media are transferred and stored off site.

After the media are ejected from your robot, you must add the media logically to containers by using either the Vault Operator Menu or the `vltcontainers` command.

The options available for adding media to containers are as follows:

- Enter the container ID and media IDs by typing them in with the keyboard. Using this method, you can add media to more than one container.
- Scan the container ID and media IDs by using a keyboard interface barcode reader. (Keyboard interface readers are also known as keyboard wedge readers because they connect, or wedge, between the keyboard and the keyboard port on your computer.) Using this method, you can add media to more than one container.
- Read an input file that contains the IDs or numeric equivalents of barcodes of all the media to be added to one container. If you have a barcode reader that can write to a file, you can scan media barcodes and use that output file as input for the `vltcontainers` command.
- Add all the media that is ejected by a specific session to one container.

The default return date of a container is the date of the volume in the container that is returned the latest. You can change the return date during the container ID and media ID entry process or at any time thereafter before a container is recalled.

You also can delete a container from the NetBackup and Media Manager databases. The following describes when you should delete an empty container:

- If a container becomes empty due to moving media to other containers, Vault deletes that empty container.
- If a container becomes empty due to a media inject, the empty container remains and the user will have to manually delete it using the `vltcontainers` command. The following example shows you how to delete container ABC123 from the NetBackup and Media Manager catalogs.

  ```
  vltcontainers -delete -vltcid ABC123
  ```

  Note: The container must be empty before it can be deleted.

If you use containers, Vault reports on the containers and media outside the context of a profile or session.

See "About vaulting media in containers" on page 87.

See "About managing containers and media" on page 89.

See "Generating a Container Inventory Report" on page 91.

About vaulting media in containers

You can use either the Vault Operator Menu or the `vltcontainers` command to add media IDs to containers.

See "Vaulting container media by using the Vault operator menu" on page 87.

See "Vaulting container media by using the vltcontainers command" on page 87.

Vaulting container media by using the Vault operator menu

After the media eject from your robot, you can use the Vault Operator Menu to enter the container ID and media IDs.

See "Vault operator menu interface " on page 132.

To vault media in containers by using the Vault operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. Eject the media to be added to the containers.
3. Select **Container Management**.
4. Select one of the following options:

Move media into one or more containers	Select if you want to use the keyboard to enter media IDs and container IDs or use a barcode scanner to scan the barcodes on the volumes and containers.
Move all media ejected by this session, into one container	Select if you want to add all media that are ejected by a session to a container.
Move all media listed in a file, into one container	Select if you want to add all media that are listed in an input file to a container.

5. Follow the prompts to complete the process of logically moving media into containers.

Vaulting container media by using the vltcontainers command

After the media eject from your robot, you can use the `vltcontainers` command to enter the container ID and media IDs. The following is the format of the `vltcontainers` command:

```
vltcontainers -run [-rn robot_number]
vltcontainers -run -usingbarcodes [-rn robot_number]
vltcontainers -run -vltcid container_id -vault vault_name -sessionid
session_id
vltcontainers -run -vltcid container_id -f file_name [-rn
robot_number] [-usingbarcodes]
vltcontainers -view [-vltcid container_id]
vltcontainers -change -vltcid container_id -rd return_date
vltcontainers -delete -vltcid container_id
vltcontainers -version
```

The following examples show how to use the vltcontainers command to add media to a container:

- To add the volumes that were ejected from robot number 0 to containers and enter the IDs by typing them in, use the following command:

  ```
  vltcontainers -run -rn 0
  ```

- To add the volumes that were ejected from robot number 0 to containers and use a barcode reader to scan the container ID and media IDs, use the following command:

  ```
  vltcontainers -run -usingbarcodes -rn 0
  ```

- To change the return date of container ABC123 to December 07, 2004, use the following command:

  ```
  vltcontainers -change -vltcid ABC123 -rd 12/07/2004
  ```

- To delete container ABC123 from the NetBackup and Media Manager catalogs, use the following command:

  ```
  vltcontainers -delete -vltcid ABC123
  ```

- To add all media that were ejected by session 4 of vault MyVault_Cntrs to container ABC123, use the following command:

  ```
  vltcontainers -run -vltcid ABC123 -vault MyVault_Cntrs
  -sessionid 4
  ```

- To add media that were listed in file `C:\home\jack\medialist` that are ejected from robot number 0 to container ABC123, use the following command:

```
vltcontainers -run -vltcid ABC123 -f C:\home\jack\medialist -rn
0
```

- To add media to container ABC123 that was ejected from a robot that is attached to the primary server and read the barcodes for that media from file `C:\home\jack\medialist`, use the following command:

```
vltcontainers -run -vltcid ABC123 -f C:\home\jack\medialist
-usingbarcodes
```

See the *NetBackup Commands Reference Guide* for more information about the `vltcontainers` command.

To vault container media by using the vltcontainers command

1. Eject the media to be added to the containers.
2. Run the `vltcontainers` command, using the appropriate options and parameters.
3. Follow the prompts to move the media logically into containers.

About managing containers and media

After the media and containers are sent to your off-site storage location, you can still perform tasks to manage the containers and media. You can view and change return dates of containers. If a container is recalled and is empty of media, you can delete the information about a container from the NetBackup and Media Manager databases.

See “Managing container media by using the Vault operator menu” on page 89.

See “Managing container media by using the vltcontainers command” on page 90.

Managing container media by using the Vault operator menu

You can use the Vault Operator Menu to change a container return date and to delete the information about a container from the NetBackup databases.

See “Vault operator menu interface ” on page 132.

Note: (This note applies to Iron Mountain users.) To change a container return date, change the date using the Vault Operator Menu or the `vltcontainers` command. Then resend the Container Inventory Report or the Iron Mountain FTP file to Iron Mountain. Do not use the Iron Mountain account management facilities to change a container return date. If you do, the Vault reports do not match the report information that is maintained by Iron Mountain.

To view a container return date by using the Vault operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. Select **Container Management > View a container's return date**.
3. Follow the prompts to enter a container name.

To change a container return date by using the Vault operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. Select **Container Management > Change a container's return date**.
3. Follow the prompts to enter container names and change dates.

To delete a container by using the Vault operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. Select **Container Management > Delete a container**.
3. Follow the prompts to enter a container name and delete the records of a container.

   If a container becomes empty after it is recalled and all media that reside in it are either injected back into the robot or assigned to another container, it is deleted from the NetBackup and Media Manager databases.

Managing container media by using the vltcontainers command

You can use the `vltcontainers` command to view and change a container return date and to delete the information about a container from the NetBackup and Media Manager databases.

See the *NetBackup Commands Reference Guide* for more information about the vltcontainers command.

Note: (This note applies to Iron Mountain users.) To change a container return date, change the date using the Vault Operator Menu or the `vltcontainers` command. Then resend the Container Inventory Report or the Iron Mountain FTP file to Iron Mountain. Do not use the Iron Mountain account management facilities to change a container return date. If you do, the Vault reports do not match the report information that is maintained by Iron Mountain.

To view a container return date by using the vltcontainers command

- Run the `vltcontainers` command by using the `-view` option. For example, to view the return date of container ABC123, use the following command:

```
vltcontainers -view -vltcid ABC123
```

To change a container return date by using the vltcontainers command

- Run the `vltcontainers` command by using the `-change` option and specifying the `-vltcid` parameter and argument and `-rd` parameter and argument. For example, to change the return date of container ABC123 to December 07, 2004, use the following command:

```
vltcontainers -change -vltcid ABC123 -rd 12/07/2004
```

To delete a container by using the vltcontainers command

- Run the `vltcontainers` command by using the `-delete` option and specifying the `-vltcid` parameter and argument. For example, to delete container ABC123 from the NetBackup and Media Manager catalogs, use the following command:

```
vltcontainers -delete -vltcid ABC123
```

  To be deleted, a container must be empty.

Generating a Container Inventory Report

The Container Inventory Report shows all the containers that are 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.

If you are using containers, all of the other Vault reports list the ID of the container in which the volume resides rather than a slot number. Reports do 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.

You also can generate the Container Inventory Report by using the Vault Operator Menu (Run **Individual Reports > Container Inventory**).

Note: You must specify a directory path where the report is generated.

See "Vault operator menu interface " on page 132.

To generate a container inventory report

1. In the NetBackup Web UI, select **Detection and reporting > Reporting**.
2. Select **Vault reports** from **Report type** drop-down.
3. Select **Container inventory** from the **Vault reports** drop-down.
4. Click **Run Report**.

Revaulting unexpired media

When you inject unexpired media from off-site storage back into a robot (for example, to perform a restore), you should revault the media. If you have to revault many tapes, you should create a new profile to revault them. If only a few tapes are to be revaulted, revaulting them manually may be the easiest and fastest option.

To revault unexpired media by creating a new profile

1. Copy the original Vault profile that was used to eject the media.
2. In this new profile, change the **Choose Backups** time window to shift it far enough back in time so that it selects the images on the volumes that you want to revault.
3. Start a session using this new vault profile.

   Vault recognizes that copies of images eligible to be vaulted exist and does not duplicate the images even if the duplication step is configured. The profile ejects the volumes to be revaulted.
4. If you are vaulting containers, logically add the volumes to containers. The container ID field is cleared when media that was vaulted in containers is injected back into the robot, so you must add the media to containers.

   See "About using containers" on page 85.

   If you are vaulting media in slots, Vault assumes that the media are returned to the same slots in off-site storage from which they were recalled.
5. Delete the new profile you created to do the revaulting.

6 If you froze your media during the data restore process, use the `bpmedia` command to unfreeze it.

If you froze the media, you have to unfreeze it so it is recalled and returned to volume pool rotation when it expires. Vaulted media that are suspended are unsuspended automatically when they expire and are recalled.

7 Return the media to your vault vendor so that all backups on that media will be available for future disaster recovery.

8 Run the Recovery Report to ensure that media are available in off-site storage for future use.

See the *NetBackup Commands Reference Guide* for information about the `bpmedia` command.

To revault media manually

1 Manually eject the media, using one of the following methods:

- Use the `vmchange` command.
- In the NetBackup Web UI, select the media ID from **Tape storage** and then select the **Eject from robot**.

`vlteject` and `vltopmenu` do not work for this purpose.

2 Manually transfer the media to the off-site volume group, using one of the following methods:

- Use the `vmchange` command.
- In the NetBackup Web UI, select the media ID from **Tape storage** and then select the **Change Volume Group**.

3 If you are vaulting containers, logically add the volumes to containers. The container ID field is cleared when media vaulted in containers is injected back into the robot, so you must add the media to containers.

See "About using containers" on page 85.

If you are vaulting media in slots, Vault assumes that the media are returned to the same slots in off-site storage from which they were recalled.

4 If you froze your media during the data restore process, use the `bpmedia` command to unfreeze it.

If you froze the media, you have to unfreeze it so that it is recalled and returned to volume pool rotation when it expires. Vaulted media that are suspended are unsuspended automatically when they expire and are recalled.

5. Return the media to your vault vendor so that all backups on that media are available for future disaster recovery.
6. Run the Recovery report to ensure that the media are available for future disaster recovery operations.

   See the *NetBackup Commands Reference Guide* for information about the `vmchange` command.

About tracking volumes not ejected by Vault

Eject is the event that Vault uses to update the NetBackup database for the location of volumes and to recall volumes. In normal operation, Vault must eject volumes so they are tracked and recalled from off-site storage after they expire.

If you ejected volumes or removed them from your robot without using a Vault eject method, it is still possible to use Vault to track them if they are in a volume pool you are using for off-site media. Using commands, you can change the attributes for volumes that were not ejected by Vault so they appear in the Vault reports and are recalled when they expire.

Note: This process works only if the volumes already are in a volume pool on the **Eject** tab of a profile. You cannot change the pool of an assigned volume.

To track volumes not ejected by Vault do the following:

- Use the `vmchange` command to change the volume group of the volumes, which Vault uses to track their location. For example, the following `vmchange` command changes the volume group of volume A00001:

  ```
  vmchange -new_v offsite_volgrp -m A00001
  ```

- Use the `vltoffsitemedia` command to change the Vault-specific attributes. The following `vltoffsitemedia` example changes the vault attributes of volume A00001:

  ```
  vltoffsitemedia -change -m A00001 -vltname offsite_vault -vltsent
  07/03/2004 -vltreturn 0 -vltslot 99 -vltsession 33
  ```

A catalog volume is processed the same except the return date is set to the date the volume should be recalled.

If you are adding the volumes to slots at your off-site storage location, you can use the `vltoffsitemedia` command with the `-list` option to find empty slots into which you can add the volumes.

If you are placing the volumes in containers, use the `vltcontainers` command to add the volumes logically to containers after you specify the off-site volume group and the vault attributes.

See "About using containers" on page 85.

The default return date of a container is the date of the volume in the container that is returned the latest. You may have to change the container return date if the volume you add expires later than any volume already in the container.

The following are the `vltoffsitemedia` options you can use to set the necessary volume attributes:

`-vltname` *`vault_name`*	The name of the vault.
`-vltreturn` *`date`*	Set the return date to 0. Vault uses the latest expiration date of the images on the volume as the return date. Exception: if the volume is a NetBackup catalog backup volume, set the date the volume should be recalled from off-site.
`-vltsent` *`date`*	Set the sent date to the date the volume was ejected. The format of the date depends on your locale setting. For the C locale, the date syntax is mm/dd/ yyyy [hh[:mm[: ss]]].
`-vltsession` *`session_id`*	The ID of the session that vaulted the volume or container. Set it to a nonzero number that is different from existing session IDs
`-vltslot` *`slot_id`*	The ID of the slot in which the volume resides in the off-site vault. Ensure that this is an empty slot at your off-site storage location. If you are placing the volume in a container, do not specify this option.

About notifying a tape operator when an eject begins

Vault can send an email notification when the eject process begins. Eject notification is configured for each profile on the **Eject** tab, for each robot on the **Vault Robot** dialog box, and globally for Vault on the **Vault management settings** dialog box. Vault sends the notification to the first email addresses that are found in that order.

To configure eject email notification, see the following:

- See "About configuring Vault Management Properties" on page 40.
- See "Configuring robots in Vault" on page 44.
- See "Eject tab (Profile dialog box)" on page 59.

- See "About setting up email" on page 125.

About using notify scripts

A Vault job can call notify scripts at specific points during the execution of the job. Vault includes template notify scripts that you can customize for your use. You can use a script for a robot, a vault, or a profile.

The template notify scripts are in the following directory:

- UNIX

  `/usr/openv/netbackup/bin/goodies`

- Windows

  install_path`\NetBackup\bin\goodies`

On Windows systems, the names of the scripts include a `.cmd` extension. They include instructions that can help you edit them for your needs.

To call and run a script, it must be copied to the NetBackup `bin` directory. A script must return a normal status (0) for the Vault job to continue processing. In case of failure, the script must return a nonzero status code to cause the Vault job to stop. On UNIX systems, the return status is communicated to the Vault job through the exit call. On Windows systems, the scripts communicate the return status in a file that is defined by the `EXIT_STATUS` environment variable, which is set by Vault.

The following scripts are provided with Vault:

`vlt_start_notify`	Called by the Vault session after it starts. For example, you can use it to send notification when the Vault job begins.
`vlt_ejectlist_notify`	Called by the Vault session before the list of media to be ejected (the `eject.list`) is built. Use this script to add media managed by Media Manager but not created by NetBackup or Vault to the eject list. The script writes media IDs to the `addon_medialist` file. Vault reads the `addon_medialist` file and ejects the media that is listed in that file during the current Vault session if the volume pool in which that media resides is in the **Off-site Volume Pools** list on the **Eject** tab of the **Profile** dialog box.

`vlt_starteject_notify`	Called by the Vault session after the `eject.list` file is built and before the automatic eject process begins. Use this script to send notification when the eject process begins or perhaps to suspend the media in the eject list. If the eject step is not configured for the profile, the `vlt_starteject_notify` script is not called.
`vlt_endeject_notify`	Called at the end of eject processing. Use this script to send notification when the eject process ends. If the eject step is not configured for the profile, the `vlt_endeject_notify` script is not called.
`vlt_end_notify`	Called by the Vault session immediately before it exits. One use for this script is to start another vault job. Then run Vault jobs in succession and avoid resource contention.

Before you use a notify script, ensure that your systems are set up properly for email.

See "About setting up email" on page 125.

For information on how to use the notify script, see the following:

- See "About notify script for a specific robot" on page 97.
- See "About notify script for a specific Vault" on page 98.
- See "About notify script for a specific profile" on page 98.
- See "Notify script order of execution" on page 98.

About notify script for a specific robot

You can use a notify script to create a unique, customized script for each robot in your configuration. To create a notify script for a specific robot, append the robot number to the script name and copy the script to the NetBackup `bin` directory.

For example, a `vlt_start_notify` script for a specific robot appears as follows:

```
vlt_start_notify.robot_number
```

The script is run for all profiles that are created for the robot.

Use the same methodology to create other notify scripts.

About notify script for a specific Vault

You can use a notify script to create a unique, customized script for each vault in your configuration. To create a notify script for a specific vault, append the robot number and vault name to the script name and copy the script to the NetBackup `bin` directory.

For example, a `vlt_start_notify` script for a specific robot or vault combination appears as follows:

`vlt_start_notify.`*`robot_number`*`.`*`vault_name`*

The script is run for all profiles that are created for a specific vault.

Use the same methodology to create other notify scripts.

About notify script for a specific profile

You can use a notify script to create a unique, customized script for each profile in your configuration. To create a notify script for a specific profile, append the robot number, vault name, and profile name to the script name and copy the script to the NetBackup `bin` directory.

For example, a `vlt_start_notify` script for a specific robot or vault or profile combination appears as follows:

`vlt_start_notify.`*`robot_number`*`.`*`vault_name`*`.`*`profile_name`*

This script is run for a specific profile that is defined for a specific vault.

Use the same methodology to create other notify scripts.

Notify script order of execution

The notify scripts run in specific to general order, as follows:

1. *script_name.robot_number.vault_name.profile_name*
2. *script_name.robot_number.vault_name*
3. *script_name.robot_number*
4. *script_name*

About clearing the media description field

When media are returned from the off-site vault during a typical volume rotation, they are expired and ready for reuse. To avoid confusion, it may be helpful to clear the media description information when an expired volume is returned to the robot.

You can configure NetBackup so that the media description field is cleared when media are returned to the robot. To do so, use the `nbemmcmd` to set the `VAULT_CLEAR_MEDIA_DESC` parameter. The media description field clears when other Vault information clears from the database.

See the *NetBackup Commands Reference Guide* for information about the `nbemmcmd` command.

Restoring data from vaulted media

You may need to restore images from the media that is stored in your off-site vault. The high-level procedure in this section describes how to restore data from vaulted media.

To restore data from vaulted media

1. Recall the media.
2. Change the images to be recovered to primary (NetBackup restores from the primary image).

   Use the `bpchangeprimary` command to promote a copy to primary.

   See the *NetBackup Commands Reference Guide*.
3. If the media is not suspended or frozen, suspend the media.

   Use the `bpmedia` command to suspend the media.

   See the *NetBackup Commands Reference Guide*.
4. Inject the media into the robot.

   See "About injecting media" on page 82.

   Injecting the media moves it into the robot and also changes the off-site volume group attribute of the media to the robotic volume group so NetBackup knows that the media are in the robot.
5. Using the Backup, Archive, and Restore interface, restore the data.

   See the *NetBackup Backup, Archive, and Restore Getting Started Guide*.
6. After restoring all the data, revault the media.

   See "Revaulting unexpired media" on page 92.

Chapter 7

Creating originals or copies concurrently

This chapter includes the following topics:

- About concurrent copies
- About the continue or fail for concurrent copies
- Creating multiple original images concurrently

About concurrent copies

You can create up to four copies of the same backup image concurrently. Those copies are created concurrently by the Inline Tape Copy feature. If the images are created during a NetBackup policy job, all are considered original images.

You must configure NetBackup to allow a sufficient number of copies in the **Maximum Backup Copies** field for the NetBackup primary server. (Configured in **Hosts > Host properties > Global attributes** for the primary server.) By default, the value is two.

All storage units must be connected to the same media server. Also, you must configure the storage unit to allow a sufficient number of concurrent jobs to support the concurrent copies (**Maximum Concurrent Jobs** or **Maximum Concurrent Drives Used for Backup** setting).

You can write images concurrently to the following storage units:

- Media Manager storage units. If the Media Manager storage unit has more than one drive, the source storage unit and destination storage unit can be the same.
- Disk storage units.
- Disk staging storage units.

If you create multiple original images concurrently during a NetBackup policy job, the backup time that is required may be longer than for one copy. Also, if you specify both Media Manager and disk storage units, the duration of disk write operations match that of slower removable media write operations.

You cannot create images concurrently using the following:

- Storage unit groups
- Quarter-inch cartridge (QIC) devices
- Third-party copies

About the continue or fail for concurrent copies

When making multiple copies of images concurrently, you can choose how an operation behaves if one of the copies fails. Your choice also can determine whether copies are ejected, depending on the success or failure of the copy operation. It is possible for a duplication operation to succeed but no ejection to occur.

In NetBackup, your continue or fail choice affects only the current image copy. In Vault, your choice affects all copies of that image.

By default, the option is configured to **Continue in NetBackup** and to **Fail All Copies in Vault**.

- See "About continue copies" on page 101.
- See "About fail all copies" on page 102.

About continue copies

If you choose **Continue for all copies**, the concurrent copy job is considered successful if any of the copies succeed. However, it is possible that a copy of the image may never get vaulted. It is probable that at least one copy will succeed, but it may not be the copy that is assigned to the off-site volume pool for ejection.

To ensure that media are ejected even if a concurrent copy operation fails during a NetBackup policy backup, do one of the following:

- Configure a Vault profile to duplicate the image, assign the copy to the off-site volume pool, and select **Fail All Copies**. If the copy fails during the original NetBackup backup job, the Vault profile subsequently duplicates it. If the copy succeeds during the original backup job, the Vault profile does not duplicate it. Either way, a copy is ejected for transfer off site.
- Monitor the Activity Monitor for a failed status for the copy that is assigned to the off-site volume pool. If that copy fails, duplicate that image and assign it to the off-site volume pool so it is ejected.

About fail all copies

The behavior of the fail option and the default settings depend on whether the concurrent copies operation was configured in Vault or in NetBackup:

- In Vault, if you choose **Fail All Copies**, all copies of that image fail, independent of the success or failure of other image copy operations. The next time the Vault profile runs, Vault again tries to duplicate the image if the following conditions are true:
  - The image is selected.
  - The Vault profile did not eject the primary backup.
- In NetBackup, if you choose **Fail All Copies**, the entire backup job fails and no copies are made. In this case, normal NetBackup behavior ensures that a successful backup for this policy eventually occurs. That is, NetBackup automatically retries the backup if time permits and, the next time the backup window for the policy opens, NetBackup again tries to run the backup (regardless of the frequency of the schedule). NetBackup retries until the backup succeeds, although one or more backup windows may pass before the backup is successful.

Creating multiple original images concurrently

In a NetBackup policy job, you can create multiple original backup images concurrently. Vaulting original images has many benefits, including easier configuration of Vault, fewer chances for resource contention, and possibly fewer drives required.

To create multiple backup images concurrently

1. In the **NetBackup Web UI**, in the left pane, expand **Protection > Policies**.
2. Select the **Schedules** tab.
3. In the Backup schedules, click **Add**.
4. In the **Add schedule** dialog-box, select **Multiple copies** and specify the parameters in the **Configure multiple copies** section of the dialog-box.
5. Specify the priority of the duplication job for each copy, from 0 to 99999.

   A larger number is higher priority. All copies are duplicated at the same priority.
6. Specify the storage unit where each copy is stored.

   If a Media Manager storage unit has more than one drive, it can be used for both the source and the destination. Network Data Management Protocol (NDMP) storage units are not supported when creating multiple copies during a NetBackup policy job.

7 Specify the volume pool to which each copy is assigned.

8 Select the retention level for each copy.

If you select **No Change**, the expiration date is the same for the duplicate copies and original copies.

If you select a different retention period, the expiration date of the copy is the backup date plus the retention period. For example, if a backup was created on November 14, 200x, and its retention period is one week, the new copy's expiration date is November 21, 200x.

9 Select whether to **Continue** the other copies if a copy operation fails or to **Fail All Copies**.

10 Specify who should own the media onto which NetBackup writes the images:

Any	NetBackup chooses the media owner, either a media server or server group.
None	Specifies that the media server that writes to the media owns the media. No media server is specified explicitly, but you want a media server to own the media.
A server group	All media server groups that are configured in your NetBackup environment appear in the drop-down list. Specifying a media server group allows only those media servers in the group to write to the media on which backup images for this policy are written.

11 Click **OK**.

12 Configure other schedule criteria as appropriate.

Chapter 8

Reporting

This chapter includes the following topics:

- About reports
- About generating reports
- About consolidating reports
- Viewing Vault reports
- Vault report types

About reports

The reports for each profile are configured on the**Reports** tab in the **Profile** dialog box. When you configure a Vault profile, you specify which reports should be generated, when they should be generated, and how and to whom they should be distributed.

After reports are generated and distributed, you can view and print them until the Vault logs for that session are deleted.

To view sample Vault reports and log files for this release, refer to the following file on the Cohesity Support Web site.

About generating reports

If the reports for a profile are configured as immediate, the reports are generated when the profile runs.

If the reports for a profile are deferred, use one of the following methods to generate the reports after the profile runs:

- Select the **Deferred Eject** option and then selecting **Generate Reports After Eject**.
- Use the **Vault Operator Menu** interface.
- Use the `vlteject` command.
- Use a Vault policy that runs the `vlteject` command.

When you generate reports, the reports that are selected on the **Profile** dialog box **Reports** tab are generated and distributed to the destinations specified.

Reports can be generated for one session or for multiple sessions. Generating reports and ejecting media from more than one vault session is known as consolidating your reports and ejections. For example, you may duplicate images daily but eject media and generate reports only at the end of the week.

- See "Generating reports by using the Vault operator menu" on page 105.
- See "Generating reports by using the `vlteject` command" on page 106.
- See "Creating a Vault policy to generate reports" on page 106.
- See "Ejecting media by using NetBackup Web UI" on page 77.
- See "Reports tab (Profile dialog box)" on page 65.
- See "Reports that depend on eject" on page 67.

Generating reports by using the Vault operator menu

You can use the Vault Operator Menu to generate reports.

To generate reports by using the Vault operator menu

1. Start the Vault Operator Menu by running the `vltopmenu` command.
2. If necessary, select a profile.
3. Select one of the following options:
   - **Run Reports for This Session**
   - **Run Individual Reports**
   - **Consolidate All Reports**
   - **Consolidate All Reports and Ejects**
     Consolidating reports and ejects also ejects media.
4. Continue as prompted by the Vault Operator Menu.

Generating reports by using the `vlteject` command

You can use the `vlteject` command with the `-report` option to generate reports from the command line. The following is the syntax for the command that generates all reports that are not yet generated:

```
vlteject -report
```

You also can specify a robot, vault, profile, or session for which to generate reports.

If the corresponding eject process has completed, pending reports from the selected sessions are generated and distributed. The reports are not generated again if `vlteject` is run again. If the ejection has not been completed, the subset of reports that do not depend on completion of eject are generated. These reports are generated again if `vlteject -report` is run again after eject has been completed.

The following is the format of the `vlteject` command:

```
vlteject -eject -report -preview [-profile profile_name]
[-profile robot_no/vault_name/profile_name]
[-robot robot_no] [-vault vault_name [-sessionid id]]
[-auto y|n] [-eject_delay seconds] [-legacy]
```

The `vlteject` command resides in the following directory:

- UNIX: `/usr/openv/netbackup/bin`
- Windows: *install_path*`\NetBackup\bin`

See the *NetBackup Commands Reference Guide*.

To generate reports by using the `vlteject` command

1. In a terminal window or command window, change to the directory in which the `vlteject` command resides.
2. Run the command, using the appropriate options and parameters.

Note: In case of non-administrative users using NBAC, a specially privileged user in **Vault Operator** group is authorized to run the command `vlteject -report`. This privileged user only can generate the reports for detail.log and session.log files, on demand.

Creating a Vault policy to generate reports

You can use a Vault policy to generate reports for the Vault sessions that have completed already and for which reports have not been generated. On the **Backup**

Selections tab, in the Vault policy, specify Vault as the policy type, do not specify clients, and specify the `vlteject` command with the `-report` option.

You also can specify a robot, vault, profile, or session for which to generate reports.

If the corresponding eject process has completed, pending reports from the selected sessions are generated and distributed. The reports are not generated again if `vlteject` is run again.

If the eject operation has not been completed, the subset of reports that do not depend on completion of eject are generated and distributed. These reports are generated again if `vlteject` is run again.

The following is the format of the `vlteject` command:

```
vlteject -eject -report -preview [-profile profile_name]
[-profile robot_no/vault_name/profile_name]
[-robot robot_no] [-vault vault_name [-sessionid id]]
[-auto y|n] [-eject_delay seconds] [-legacy]
```

The `vlteject` command resides in the following directory:

- UNIX

  `/usr/openv/netbackup/bin`

- Windows

  install_path`\NetBackup\bin`

  See the *NetBackup Commands Reference Guide*.

To create a Vault policy to generate reports

1. Navigate to **Protection > Policies**.
2. Click Add and specify the required parameters.
3. On the **Attributes** tab, select **Vault** as the policy type.
4. On the **Schedules** tab, click **New** to create a new schedule.

   The type of backup defaults to Automatic Vault.
5. Complete the schedule.
6. Bypass the **Client** tab (clients are not specified for Vault jobs).
7. On the **Backup Selections** tab, enter the `vlteject` command with the `-report` option and any other appropriate options.
8. Click **Save**.

About consolidating reports

You can generate reports and eject media from more than one vault session, which is known as consolidating your reports and ejections. For example, you may duplicate images daily but eject media and generate reports only at the end of the week. To do so, specify deferred reports on the **Reports** tab and deferred eject on the **Eject** tab for each profile for which you want to consolidate reports. Then, eject the media and generate the reports.

Note: If you consolidate reports, you should also consolidate ejects.

See "About ejecting media" on page 75.

When you generate the reports, you select the robot, vault, or profile sessions for which reports were deferred (that is, for the reports that are pending).

You can consolidate the following:

- All sessions for a profile
- All sessions for a vault
- All sessions for a robot
- All sessions for all vaults

A consolidated report includes information from all sessions in which that report is specified in the profile. For example, a consolidated Picking List for Robot includes the appropriate media from all sessions whose profile has Picking List for Robot selected on the **Reports** tab.

Table 8-1 defines the elements of a consolidated report.

Table 8-1 Consolidated reports elements

Report element	Description
Report Header	Includes the following: ■ Identifies the report as a consolidated report. ■ The robots, vaults, or profiles that are included in the report. ■ The sessions that are included in the report.
Report Body	Shows the media from all sessions that are included in the consolidation in which the report is selected on the profile **Reports** tab. If media applies to more than one session, only the information from the most recent session is included. Similarly for containers, only the container information from the most recent session appears.

Table 8-1 Consolidated reports elements *(continued)*

Report element	Description
Summary	Shows the same information as in a nonconsolidated report.

In the Recovery Report, the earliest date range among the consolidated sessions is the end date. The Recovery Report is generated from the current date and time to that end date. Time ranges specified in individual profiles are used to generate the reports. Each time range is calculated based on the start time of the individual sessions participating in the consolidated report.

If the ejection has not completed, the subset of reports that do not depend on completion of eject are generated. These reports are generated again if deferred reports are run again.

If you consolidate reports and also rename reports, use the same customized report title for all profiles whose reports are consolidated. The customized report title is printed on the report and appears in the email subject line if you email the reports.

Note: Reports cannot be consolidated between the vaults that use slots and the vaults that use containers.

About consolidated reports in previous Vault releases

Consolidated reports in previous releases of Vault concatenated the same reports from each session together. One advantage of that style is that you can consolidate reports from slot and container-based vaults, which you cannot do with the new style of consolidated report.

If you prefer the previous style of consolidated reports, use the `vlteject` command `-report` and `-legacy` options to consolidate the reports in that old style. If you currently do immediate reports, you have to change to deferred reports and either run the `vlteject` command manually or create a Vault policy to schedule the `vlteject -report -legacy` job. If you currently do deferred reports, you can add the `-legacy` option to the `vlteject` command you use to generate reports.

Viewing Vault reports

You can view and print reports for Vault sessions for which reports are already generated. You can only view reports if the session directory for that vault still exists. Only some of the reports are valid. For example, the picking list reports are only valid on the date they were generated.

To view Vault reports

1. Navigate to **Detecting and reporting > Reporting**.
2. Select one of the Vault reports or report types.

   When you select a report or a report type, the **Reports** window appears. The **Reports** window includes a **Report Settings** area and a report contents window.
3. Enter or select the appropriate values for the report you want to generate.

   Usually, you must specify a profile and a session ID. You also may have to specify a date range or time period.
4. Click **Run Report**.
5. To print the report, click **File > Print**.

Vault report types

This topic introduces and describes a variety of Vault reports as well as Vault report types.

Reports for media going off site

The reports for media going off-site show media that have ejected from the robot and are transported off-site. They vary in the amount of detail that is included in each report. Media on these reports are from the `eject.list` file for the session or, from consolidated reports, the combined `eject.list` files of all unreported vault jobs. An unreported vault job is one that ejects media but does not generate reports.

Picking List for Robot report

The **Picking List for Robot** report shows the volumes that are 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 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.

Column descriptions in the **Picking List for Robot** report are as follows:

IMAGES	The number of images on the volume. For Vault catalog backup media from releases earlier than NetBackup 6.0, the column displays zero.
CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)

EJECTED	**Yes** or **No**.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup media, displays the date that is calculated as a return date during the volume assignment.
MBYTES	The size in megabytes of images on the volume. For Vault catalog backup media from releases earlier than NetBackup 6.0, the field is empty.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Old NBU CTLG**. Catalog backup media from NetBackup releases earlier than 6.0 ■ **Add-on**. Media not managed by NetBackup.
MEDIA	The ID of the media.
ROBOT	The number of the robot from which the media was ejected. (Consolidated report only.)
SLOT ID	The ID of the slot in which the volume will reside at the off-site vault. (Slot vaulting only.)

Distribution List for Vault report

The **Distribution List for Vault** report shows the volumes that have ejected from the robot and are transported off-site. This report is sorted by off-site slot number or container 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.

Column descriptions in the **Distribution List for Vault** report are as follows:

IMAGES	The number of images on the volume.
CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
EJECTED	**Yes** or **No**.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup media, displays the date that is calculated as a return date during the volume assignment.

MBYTES	The size in megabytes of images on the volume. For Vault catalog backup media from releases earlier than NetBackup 6.0, the field is empty.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media not managed by NetBackup.
MEDIA	The ID of the media.
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. (Slot vaulting only.)
IMAGES	The number of images on the volume.

Detailed Distribution List for Vault report

The **Detailed Distribution List for Vault** report shows the volumes that have ejected from the robot and are transported off-site. This report is similar to the **Picking List for Robot** and **Distribution List for Vault** reports except that it includes detailed information about the images on each volume. Because backup jobs can span volumes, fragments of a backup image may appear on more than one volume. If two or more fragments of the same image are on one volume, they are reported on one line rather than on a separate line for each fragment. That is, each image is listed once for every media its fragments reside on.

This report is useful at a disaster recovery site. Cohesity recommends that you send this report off-site.

Column descriptions in the **Detailed Distribution List for Vault** report are as follows:

BACKUP ID	Identifier that NetBackup assigns when it performs the backup.
CLIENT	Name of the client that was backed up.
CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
EJECTED	**Yes** or **No**.

EXPIRATION	Date when the images on the volume expire. For Vault catalog backup media, displays the date that is calculated as a return date during the volume assignment.
IMAGES	The number of images on the volume.
KBYTES	The size in kilobytes of the complete backup image. The size of the complete image is listed even if the image is a fragment. For Vault catalog backup volumes, the field is empty.
MBYTES	The size in megabytes of all images on the volume. For Vault catalog backup media from releases earlier than NetBackup 6.0, the field is empty.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media not managed by NetBackup.
MEDIA	The ID of the media.
PARTIAL	Partial images on the volume. The field displays: ■ **COMPLETE** if all fragments reside on that volume. ■ **PARTIAL** if some fragments reside on other volumes. ■ **EXTRA** if the images do 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. (Slot vaulting only.)
VAULT	The name of the vault to which the volume's profile belongs. (Consolidated report only.)
WRITTEN	The date the image was written.

Summary Distribution List for Vault report

This report is similar to the **Detailed Distribution List for Vault** report, except that the entry for each piece of media lists 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 prints on this report. The **Detailed Distribution List** would show each of these backup jobs as a separate entry, which

can generate a long report. The **Summary Distribution List for Vault** report summarizes the information and presents it in a more compact form. This report is also useful for disaster recovery situations; we recommend that you send this report off-site.

Column descriptions in the **Summary Distribution List for Vault** report are as follows:

IMAGES	The number of images on the volume.
BACKUP TIME	When the backup occurred.
CLIENT	Name of the client that was backed up.
CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
EJECTED	**Yes** or **No**.
EXPIRATION	Date when the images on the volume expire. For Vault catalog backup media, displays the date that is calculated as a return date during the volume assignment.
MBYTES	The size in megabytes of images on the volume. For Vault catalog backup media from releases earlier than NetBackup 6.0, the field is empty.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media not managed by NetBackup.
MEDIA	The ID of the media.
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. (Slot vaulting only.)
VAULT	The name of the vault to which the volume's profile belongs. (Consolidated report only.)

Reports for media coming on-site

The reports for media coming on-site show the volumes that are requested back from the off-site vault. These reports can be generated before or after media has ejected for the current Vault session.

To appear in these reports, media must:

- Be in a Vault off-site volume group.
- Be in an eject volume pool for a profile in the current vault or in a scratch pool.
- Be in any vault if the media is in a scratch pool.
- Have a non-null return date which has passed when the report is generated (Catalog backup only).
- Have a vault container value that is non-null (container vaulting only).
- Be unassigned (NetBackup media only).

Picking List for Vault report

The **Picking List for Vault** report shows the volumes that are 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 **Return Date** field for the media and adds the media ID and date requested to this report.

Expired media appear on this report only once: either on the date the media expire or the next time the report is generated (if the report is not generated on the date a volume expires). If media appear on the report but are not recalled, they appear on the **Lost Media** report.

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

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

Column descriptions in the **Picking List for Vault** report are as follows:

CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
DENSITY	Density of the volume.

LAST MOUNT	The date the volume was last mounted. (Session report only; does not appear for consolidated report.)
LAST SID	The session ID of the Vault session that recalled the media.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media that NetBackup does not manage.
MEDIA	The ID of the media.
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. (Container vaulting only.)
SLOT ID	The ID of the slot in which the volume resides in the off-site vault. (Slot vaulting only.)
VAULT	The name of the vault to which the volume's profile belongs. (Consolidated report only.)

Distribution List for Robot report

The **Distribution List for Robot** report shows the volumes to be requested back from the off-site vault. This report is identical to the **Picking List for Vault**, except that it includes the robot to which the media should be returned. Retain this report to use as a checklist for the media that are 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.

Column descriptions in the **Distribution List for Robot** report are as follows:

CONTAINER ID	The ID of the container in which the volume resides in the vault. (Container vaulting only.)
DENSITY	Density of the volume.
LAST MOUNT	The date the volume was last mounted. (Session report only; does not appear for consolidated report.)
LAST SID	The session ID of the Vault session that recalled the media.

CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media that NetBackup does not manage.
MEDIA	The ID of the media.
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. (Container vaulting only.)
ROBOT	The number of the robot in which the media resided. (Consolidated report only.)
SLOT ID	The ID of the slot in which the volume resides in the off-site vault. (Slot vaulting only.)

Inventory reports

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

See "Vault Inventory report" on page 117.

See "Off-site Inventory report" on page 118.

See "All Media Inventory report" on page 119.

To view 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 report

The **Vault Inventory** (or **Inventory List for Vault**) report shows media that are off-site at the vault vendor and media being sent off-site (outbound media in transit to the vault).

To appear in this report, media must be:

- In the off-site volume group.
- In the current vault or in any vault if the media is in a scratch pool.
- In an eject volume pool for a profile in the current vault, in a scratch pool, or in the catalog volume pool.

Cohesity 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.

Column descriptions in the **Vault Inventory** report are as follows:

ASSIGNED	The date that NetBackup Media Manager assigned the volume.
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.
CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media that are not managed by NetBackup.
MEDIA	The ID of the media.
SLOT ID	The ID of the slot in which the volume resides in the off-site vault. (Slot vaulting only.)
VAULT	The name of the vault to which the volume's profile belongs. (Consolidated report only.)

Off-site Inventory report

The **Offsite Inventory** (or **Full Inventory List for Vault**) report includes the information in the Vault Inventory report and also includes any volumes that were requested back from the off-site vault vendor (that is, inbound media 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.

Column descriptions in the **Offsite Inventory** report are as follows:

ASSIGNED	The date when the volume was assigned by NetBackup Media Manager.
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.

CATEGORY	The type of media: ■ **NBU**. NetBackup media that contains backup images. ■ **New NBU CTLG**. Catalog backup media from NetBackup 6.0 and later releases. ■ **Add-on**. Media that are not managed by NetBackup.
MEDIA	The ID of the media.
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.)
VAULT	The name of the vault to which the volume's profile belongs. (Consolidated report only.)

All Media Inventory report

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

To appear in this report, media must be:

- In the robotic volume group or off-site volume group.
- In the current vault or in any vault if the media is in a scratch pool.
- In an eject volume pool for a profile in the current vault or in a scratch pool.

If you use a scratch pool, this report can include volumes from other profiles or vaults that 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 do not appear on this report.

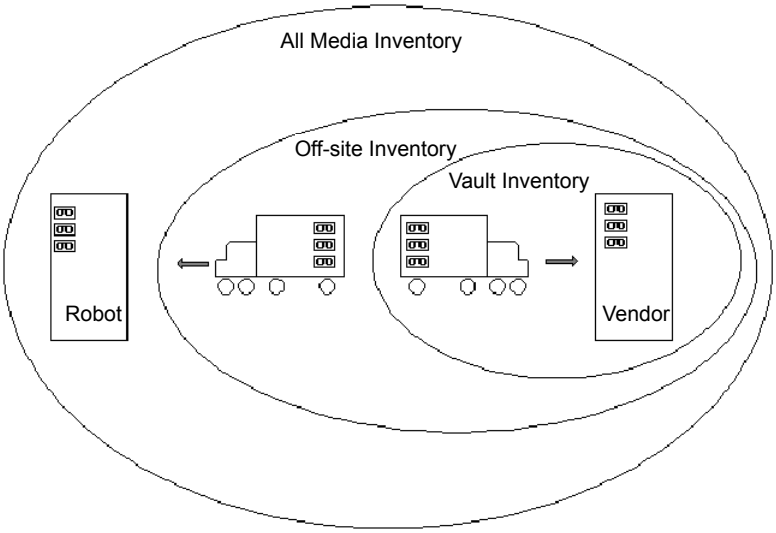
Column descriptions in the **All Media Inventory** report are as follows:

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.
LOCATION	Shows where the volume resides. For a session report, shows Robot or Vault. For a consolidated report, shows the robot number if the volume is in the robot or the vault name if the volume is off-site.

MEDIA	The ID of the media.
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. (Slot vaulting only.)

Figure 8-1 shows the different scopes of the reports:

Figure 8-1 Graphical representation of inventory reports scope



Container Inventory report

The **Container Inventory** report shows all the containers that are 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 do 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.

Column descriptions in the **Container Inventory** report are as follows:

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 that are in the container.
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 report

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

This report also includes the following:

- The three most recent Vault catalog backups in the vault's off-site volume group. Only Vault catalog backups appear on this report. NetBackup catalog backups do not appear even if they are ejected and transferred off site.
- The information from the disaster recovery file that is generated by the catalog backup policy.

In a consolidated **Recovery** report, the earliest date range among the consolidated sessions is the end date. The **Recovery** report is generated from the current date and time to that end date. Time ranges specified in individual profiles are used to generate the reports. Each time range is calculated based on the start time of the individual sessions participating in the consolidated report.

Sending the **Recovery** report to the vault vendor on a regular basis helps with disaster recovery efforts. If a disaster destroys the primary server, you cannot generate a **Recovery** report to determine which volumes to request from the vault vendor. Therefore, it is very important that the vault vendor has a copy of the Recovery report.

Field descriptions in the **Recovery Report for Vault** report are as follows:

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.
CLIENT	Name of the client that was backed up. (Excluding catalog backup media.)

MEDIA	The ID of the media. (Vault catalog backup media only.)
MEDIA ID	The ID of the media. (Excluding catalog backup media.)
WRITTEN	The date the catalog backup was written to the volume. (Vault catalog backup media only.)
VAULT	The off-site vault at which the media are stored.
SLOT/CONTAINER	The ID of the slot or container in which the volume resides in the off-site vault.

Lost Media report

The **Lost Media** report lists expired media that has not been returned from the off-site vault vendor.

Media that appear on the Lost Media report have the following:

- An assigned date of 0 or are frozen.
- A robot number value of null.
- A vault sent date value that is non-null.
- A non-null return date.

Media can get lost for various reasons, as follows:

- 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 never again is listed for recall.
- Frozen backup media never expires. Media that does not expire does not appear on the **Picking List for Vault** and is not recalled from the vault.
- You change or rename your off-site volume groups and pools. For example, if you begin using a new media type, you have to use a new volume pool name. Cohesity recommends that you do not change or rename group or pool names.

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, the media that are 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).

Column descriptions in the **Lost Media** report are as follows:

DENSITY	Density of the volume.

LAST MOUNT	The date the volume was last mounted.
MEDIA ID	The ID of the media.
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 Exception** report shows images and media that were not vaulted when the Vault session was run. When a **Non-vaulted Images Exception** report for a given session is generated, the current status of images (in the preview.list of the session) and the media they reside on is checked for those that were not vaulted. This report lists the images (from the preview.list file) and the media that match the Choose backups criteria, and were not vaulted at the time the report was generated.

If you generate the report after a session runs, images that expired since the session ran are not on the report even though they were not vaulted. Therefore, to use the **Non-vaulted Images** report effectively, generate it when a session runs and save it so you can refer to it later.

You can save the report by specifying a directory to save the report to on the **Reports** tab (**Profile** dialog box).

See "Reports tab (Profile dialog box)" on page 65.

Reports also are saved in the session directory.

Column descriptions in the **Non-vaulted Images** report are as follows:

ASSIGNED	The date when NetBackup Media Manager assigned the volume.
BACKUP ID	Identifier that NetBackup assigns when it performs the backup.
CREATED	The date the volume was created (original backup or duplicated).
EXPIRATION	Date when the images on the volume expire.
MEDIA	The ID of the media.
POLICY	Name of the policy that was used to back up the client.
ROBOT	The number of the Vault robot in which the volume resides. (Consolidated report only.)
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 robot. (Slot vaulting only.) (Session report only; does not appear for consolidated report.)
VOLUME GROUP	The group to which the volume is assigned.
VOLUME POOL	The pool to which the volume is assigned.

About the 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 (the "P" section)
- Distribution List for Vault (the "D" section)
- Vault Inventory report (if you are vaulting in slots) (the "I" section)
- Container Inventory report (if you are vaulting containers) (the "C" section)
- Recovery report (the "R" section)

The reports that are included in the file depend on your selections on the **Reports** tab of the **Profile** dialog box. You must select a report so that it appears in the Iron Mountain report file.

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

Before you send the report to Iron Mountain, verify that the volumes that were ejected match the **Distribution List for Vault**. Contact Iron Mountain to determine where and when to send the report.

Chapter 9

Administering Vault

This chapter includes the following topics:

- About setting up email
- About administering access to Vault
- Copying a profile
- About moving a vault to a different robot
- About changing volume pools and groups
- About NetBackup Vault session files

About setting up email

Depending on your computing environment, you may have to configure NetBackup or your computing environment so that notification email from NetBackup functions properly.

On UNIX systems, NetBackup uses the `sendmail` mail transfer agent to send email. If `sendmail` is not installed, you must install it and configure your environment so it functions correctly.

On Windows systems, NetBackup uses the `nbmail.cmd` script (in *install_path*`\VERITAS\NetBackup\bin\goodies`) on the NetBackup primary server to send email. For email notifications, NetBackup passes the email address, subject, and message to the script. NetBackup then uses the mail program that is specified in the script to send email. For instructions on configuring the script, see the comments in the `nbmail.cmd` script. Default NetBackup behavior: `nbmail.cmd` does not send email.

Note: If you use the Blat email client to deliver email on Windows systems, include the `-mime` option on the `blat` command in the `nbmail.cmd` script. That ensures the Vault reports are mailed correctly.

See the *NetBackup Administrator's Guide, Volume I*.

About administering access to Vault

NetBackup provides two mutually exclusive methods for controlling user access:

- Role Based Access Control (RBAC). lets you control access to NetBackup by defining user groups and granting explicit permissions to these groups. Configuring user groups and assigning permissions is done using RBAC in the NetBackup Web UI.

  Note: See *NetBackup Web UI Administrator's Guide*, *Managing security* section.

- Enhanced Authorization and Authentication. Enhanced authentication allows each side of a NetBackup connection to verify the host and user on the other side of the connection. By default, NetBackup runs without enhanced authentication. Enhanced authorization determines if authenticated users (or groups of users) have NetBackup administrative privileges. By default, NetBackup gives administrative privileges to UNIX root administrators or Windows system administrators on NetBackup servers.

If both RBAC and Enhanced Authorization and Authentication is configured, RBAC takes precedence.

Copying a profile

If you want to create a profile that is similar to another profile, you can copy the existing profile, rename it, and then change the attributes.

Note: The new profile must belong to the same robot as the original profile.

To copy a profile

1. Select the profile you want to copy.
2. Open the **Actions** menu and select **Copy Profile**.
3. In the **Copy a Profile** dialog box, from the drop-down list under the **Vault** field, choose the vault in which to place the new profile.

4 Enter a new name for the profile.

5 Click **OK**.

About moving a vault to a different robot

A vault is associated with (that is, belongs to) a specific robot. However, you can change the robot to which the vault belongs. To do so, right-click the robot and select **Change**. Then complete the dialog box, specifying another robot for the vault, and click **OK**.

Note: All vaults that were associated with the previous robot are now associated with the new robot chosen in the dialog box. Some profile configurations may be invalid under the new robot. For example, if the previous robot was associated with a media server that the new robot is not associated with, the configuration is invalid.

Robots are configured in NetBackup through Media Manager. The action that is described in this topic does not change the configuration of a robot in Media Manager.

About changing volume pools and groups

If you change to a new off-site volume group or off-site volume pool(s), you can ensure that media are recalled by configuring a profile that only generates the reports needed to recall media, as follows:

- Configure a vault that uses the old off-site volume group.
- Configure a profile in that vault that does the following:
  - Selects no images (that is, configure the **Choose Backups** step so that no backup images are selected).
  - Skips the Duplication step and Catalog Backup step.
  - Specifies the old volume pools in the volume pool list on the Eject step.
  - Generates only the Picking List for Vault and Distribution List for Robot reports.
- Schedule the profile to run on a regular basis.

Media in the old off-site volume group and in the old volume pool(s) are recalled from off-site storage as they expire. After each volume is recalled and injected back into the robot, change its volume pool and group to the new ones. If a volume is

returned to a scratch volume pool from which all media are allocated, you do not have to change the volume pool.

After all media in those volume pools and groups are recalled, you can delete the vault, volume group, and volume pools.

Note: If you have media in your off-site vault, Cohesity recommends that you do not change or rename your off-site volume group(s) or off-site volume pool(s). If you begin using new volume pools and groups in your Vault profiles, the reports that recall expired media do not include the old groups and pools.

About NetBackup Vault session files

The directory that is generated for each vault session collects information for the session in 2 log files. The `detail.log` file contains a record of each action that is performed for the session. Some of the information in `detail.log` is also recorded in the NetBackup log files. The `summary.log` file contains a brief description of the vault session, and the results of the session. If email notification is enabled, the information in this file is appended to the email.

The `detail.log` has information about the number of images that are selected by a particular session. In addition, it should record information (during the duplication step) about the total number of images and the number of images duplicated. If these numbers do not match, it means that some images were not duplicated. The log should contain information about which images were not duplicated, either because they were duplicated in a previous session or because the duplication failed for some reason. The actual images that are selected by the session show only if a higher debug level (level 5) is used.

The session log files are located in the following path:

- UNIX

  `/usr/openv/netbackup/vault/sessions/`*`vault_name`*`/sid`*`xxx`*

  `/usr/openv/netbackup/vault/sessions/vault_name/sidxxx/logs`

  On a NetBackup cluster, the `vault/sessions` directory is present in the shared location:
  Example: `/opt/VRTSnbu/netbackup/vault/sessions/vault_name/sidxxx/`

- Windows

  `install_path``\NetBackup\vault\sessions\vault_name\`*`sidxxx`*

On a NetBackup cluster, the vault\sessions directory is present in the shared location.

Example: <shared-path>\NetBackup\vault\sessions\vault_name\sidxxx\

The name of the vault is *vault_name* and it is used for the session. The unique session identifier *xxx* is the identifier that Vault assigns to each vault session. The session ID starts at 1 the first time that Vault runs and increments by 1 for each new session. The session identifier for a Vault session can be found by viewing the Activity Monitor entry for that session.

By default, the session log files are created using the following naming convention, on Windows and UNIX platforms.

- `/usr/openv/netbackup/logs/vault/<vault>/<session-id>/logs/<username>.detail.log`
- `/usr/openv/netbackup/logs/vault/<vault>/<session-id>/logs/<username>.session.log`

For Windows administrative users, the user name **ALL_ADMINS** gets appended in the log file name. In case of UNIX administrative users, the user name **root** gets appended in the log file name. For non-administrative users, only for the NBAC, with a specially privileged user in **Vault_Operator** group who is authorized to run `vlteject -report`, generates the session logs on demand. For more information on legacy logging, refer to the **Legacy Logging** section in *NetBackup Logging Reference Guide*.

Note: Directory names are not case-sensitive on Microsoft Windows systems. Therefore, session directories are created in the same `vault\sessions\vault_name` directory for two or more vaults that have names difference only in the letter-case.

Table 9-1 describes the Vault session logs.

Table 9-1 Vault session log names

Name	Purpose
`preview.list`	Summary of images to be duplicated if Duplication step is configured or ejected if Eject step is configured and Duplication step is not.
`image.list`	Lists all images and partial images for a session.
`detail.log`	Summary of each action that is performed for a Vault session.
`summary.log`	Brief description of the Vault session and its results. If email notification is enabled, data in this log file is appended.

About setting up Vault session log files

Vault generates session logs and debug logs. The session logs can help you keep track of Vault processes.

See "About NetBackup Vault session files" on page 128.

See "Setting the duration of Vault session files" on page 130.

See "Debug logs" on page 139.

Setting the duration of Vault session files

Vault's session files are stored in the following directory:

- UNIX

  `/usr/openv/netbackup/vault/sessions`

- Windows

  install_path`\NetBackup\vault\sessions`

You can configure the length of time NetBackup retains these files.

To set the duration of Vault session files

1. On the left, select **Hosts > Host properties**.
2. Select the primary server and select **Connect**.
3. Select **Clean-up**.
4. In the **Delete vault logs** field, set the length of time after which to delete the Vault working files.

   When the set time has elapsed, the entire `sid`*xxx* directory is deleted.

   You should plan to retain each `sid`*xxx* directory at least as long as the period of time over which you plan to span consolidated ejects. We suggest that you keep these directories at least a week longer than the consolidation span. If the `sid`*xxx* directory has been deleted, Vault is unable to eject tapes or generate reports from that session.

Chapter 10

Using the menu user interface

This chapter includes the following topics:

- About using the menu interfaces
- About the Vault administration interface
- Vault operator menu interface
- Vault fields in bpdbjobs output

About using the menu interfaces

Vault also includes the following two menu user interfaces (MUIs) that you can use in a terminal window:

- The Vault Administration interface, which lets you configure Vault. It provides the same functionality as Vault Management.
- The Vault Operator Menu interface, which provides a way to eject media and print reports for one or more Vault sessions.

About the Vault administration interface

The information in this section applies to UNIX and Linux systems only.

The Vault Administration interface lets you configure and run Vault from a text-based menu. You can perform the same actions in the **Vault Administration** menu.

You can use the Vault Administration interface from any character-based terminal (or terminal emulation window) that has a termcap definition or terminfo definition. Use the `vltadm` command to start the Vault Administration interface, and run the

`vltadm` command only from the UNIX system on which the NetBackup primary server resides. You must have root privileges to run the `vltadm` command.

The `vltadm` command and interface are available on UNIX systems only.

The `vltadm` command resides in the following directory:

```
/usr/openv/netbackup/bin
```

When you run the `vltadm` command, the following menu appears in the terminal window:

```
Vault Administration
--------------------
       Robot Name:  <none>
       Vault Name:  <none>
       Profile Name:  <none>
r)  Browse all configured robots
v)  Browse all configured vaults for selected robot
p)  Browse all configured profiles for selected vault
n)  Robot management...
t)  Vaults for selected robot...
f)  Profiles for selected vault...
c)  Copy selected profile...
s)  Start session for selected profile...
a)  Vault properties...
h)  Help
q)  Quit
ENTER CHOICE:
```

To browse through specific robots, vaults, or profiles already configured in Vault, press `r`, `v`, or `p`. When the correct robot, vault, or profile appears, type the letter of the action you want to perform.

You can configure different criteria in the Vault Administration interface.

See "About configuring Vault" on page 37.

For help on the currently displayed menu, select the **help** option on that menu. Help includes a tutorial for learning and using the Vault Administration interface.

Vault operator menu 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 run the `vltopmenu` command).

The `vltopmenu` command, which starts the Vault Operator Menu, resides in the following directory:

- UNIX: `/usr/openv/netbackup/bin`
- Windows: *install_path*`\NetBackup\bin`

When you run the `vltopmenu` command, the NetBackup Vault Operator menu appears in the terminal window.

```
                     NetBxxxackup 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  e) Eject Media for This Session

ce) Consolidate All Ejects  re) Consolidate All Reports and Ejects

c) Container Management...

q) Quit

Selection-->
```

Upon startup, the menu displays the current profile, session, and report destinations.

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`

See the *NetBackup Vault Operator's Guide*.

Vault fields in bpdbjobs output

The NetBackup activity monitor utility, `bpdbjobs`, displays Vault jobs by default.

Table 10-1 shows the Vault-specific fields that you receive if you run the `bpdbjobs` command and use the `-vault` option.

Table 10-1 Vault fields in bpdbjobs output

Field	Description
Robot	The name of the robot with which the vault is associated.
Vault	The name of the vault under which the session is running.
Profile	The name of the profile that holds the configuration information for the vault session.
Session ID	The session ID is a unique numeric value for the vault job. Session ID assignment starts at 1 the first time a vault job is run after vault has been installed. The value increments by 1 every time a new vault job runs.
Tapes to Eject	The number of tapes to be ejected for a vault session. If the profile is configured for deferred eject, the tapes may not be ejected yet.
Operation	For Vault jobs, the field contains one of the following values. These values progress from the first value to the last as the Vault job progresses as follows: ■ **Choosing Images** ■ **Choosing Media** ■ **Catalog Backup** ■ **Eject and Report** ■ **Done**

If a Vault job completes successfully (with exit status = 0), the **State** field and the **Operation** field both contain the value **Done**. If a vault job fails, the Operation field contains the operation occurring at the time the job failed.

Chapter 11

Troubleshooting

This chapter includes the following topics:

- About troubleshooting Vault
- About printing problems
- About errors returned by the Vault session
- About media that are not ejected
- About media that is missing in robot
- About the tape drive or robot offline
- About stopping bpvault
- About ejecting tapes that are in use
- About tapes not removed from the MAP
- Revaulting unexpired tapes
- Debug logs

About troubleshooting Vault

This topic contains information about how to diagnose potential problems or errors that you may encounter. Some of these areas include printing problems, missing media issues, no duplicate messages, to how to stop bpvault.

About printing problems

Problems with printing reports that appear to be Vault problems often are problems with the print command configured on the profile **Reports** tab. Therefore, you should

test print commands from a command line on the server on which Vault is installed to ensure that they work correctly.

In some rare cases with Microsoft Windows, the print command works correctly when tested from a command prompt but does not work when configured on the profile **Reports** tab. The issue may be with how Windows calls the print command. If you experience such a problem, from a command prompt on the primary server on which Vault is installed, enter the following command (use the appropriate server and printer names):

```
NET USE lpt1 \\servername\printername PERSISTENT:YES
```

This problem can also occur in mixed environments of UNIX and Windows.

About errors returned by the Vault session

Every Vault session writes a detailed error status to `stderr`, as follows:

- If the error generated by the Vault session is less than or equal to 255, it returns the actual error code. Error codes less than or equal to 255 (except 252) map to standard NetBackup error codes and are documented in the *NetBackup Troubleshooting Guide*.
- If the Vault session fails with an error code greater than 255, it returns error code 252 and the actual error code is written to `stderr`. Codes greater than 255 are called NetBackup Extended Error Codes and are not supported by all operating systems.

The format of the error text written to `stderr` is:

EXIT status = *error code*

See the *NetBackup Troubleshooting Guide*.

About media that are not ejected

If no media are ejected, it may be because of the following:

- All images have already been vaulted, so no images were selected. Vault determines that a backup image has already been vaulted if a copy of the image is already on a volume in an off-site volume group.
- The media to be vaulted are in a volume group other than the robotic volume group specified for the vault to which the profile belongs.

About media that is missing in robot

Duplication may fail if NetBackup does not know that a requested piece of media is in the robot. For example, a tape may have been moved to the off-site volume group inadvertently even though it remains in the robot.

If the tape is not found, delete it from the NetBackup system. If the tape is missing yet is assigned and has valid duplicate images, use the command `bpexpdate` to expire the images before you delete the tape from Media Manager. This command is documented in the *NetBackup Administrator's Guide*.

About the tape drive or robot offline

If you have a problem with ACSLS drives going offline, try to configure the drives in an UP state or reset the drive. If drives persistently go offline, duplication may hang.

Also, if the tape drives are listed as AVR control, there may be a problem with the robotics control. List all drives as robotically controlled (that is, TLD, ACS, and so on). They are converted to AVR control if a problem occurs with the robot. To diagnose the problem, examine the system logs (for example, `/var/adm/messages` on UNIX systems) for error messages. You can also use the robotic test utilities (such as robtest) to further debug the problem.

About stopping bpvault

To stop a bpvault duplication process, you can use the `vltrun -haltdups` command from the command line interface.

See the *NetBackup Commands Reference Guide*.

This command sends a SIGUSR2 signal to the main duplication process, which is the primary vault job that is currently in the duplication process. This signal is automatically propagated to the other bpvault duplication instances without waiting for any current duplication job instance to finish. The current duplication completes and no more duplication instances run. However, the `bpvault.all` script continues to complete processing of the other bpvault commands.

To end a bpvault process immediately rather than wait a number of minutes for the current bpduplicate processes to complete, first run the `-haltdups` command. Then manually stop the bptm jobs on each server. However, do not stop the bpduplicate processes. The errors that are received by bpvault are logged and these images are not successfully duplicated. The failure of the bptm or bpduplicate means that

these images are duplicated on the next attempt if the number of duplicate_days is not exceeded.

About ejecting tapes that are in use

If Vault is configured to eject original media, it is possible that a piece of media is in use during the eject process (for example, for a restore or a media verify procedure). In this case, an error message is generated by Media Manager. A similar error may be generated by non-Media Manager controlled robots if a piece of media is currently in use.

If you receive one of these errors, use the Vault Operator Menu (`vltopmenu`) to re-eject the media after the media is no longer in use. You may receive additional error messages because the rest of the media for the scheduled job has already ejected.

About tapes not removed from the MAP

If media are not removed from the robot's media access port (MAP) and a timeout condition occurs, the job fails with status code 338 (vault eject timed out). If this failure occurs, the Vault reports do not accurately reflect the status of the media.

To recover, you should use the Vault Operator Menu (`vltopmenu`) or the `vlteject` command to eject the media that was not removed from the library and generate the reports.

Revaulting unexpired tapes

If Vault tapes that have not expired are injected back into a robot, you can revault them manually.

To revault unexpired tapes

1. Navigate to *Storage* > *Tape storage* and then select **Volumes**.
   - Select the Media ID you want to eject and then click **Eject from robot**.
2. Transfer the media to the off-site volume group by doing the following:
   - Select the media ID(s).
   - Select **Change volume group**.
   - Search and select the appropriate volume group from Select existing or you can specify a new volume group.

3. Return the media to your vault vendor so that all backups on that media are available for future disaster recovery.
4. Run the Recovery report to ensure that the media is available for future disaster recovery operations.

   Alternatively, you can use the `vmchange` command to eject the media and transfer it to the off-site volume group.

Debug logs

Vault writes debug logs in the standard NetBackup debug logging path as follows:

- Vault commands write messages in log files in a `vault` directory. You must first create the `vault` directories so that daily log files are generated. If the directories do not exist, the log files are not created.

  The log files are in the following vault directories:

  - UNIX

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

  - Windows

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

- The NetBackup Vault Manager (`nbvault`) writes messages in Veritas Unified Logging (VxUL) log files. (VxUL creates log file names and messages in a standardized format.)
- All unified logs are written to the following locations:

  - UNIX

    `/usr/openv/logs/nbvault`

  - Windows *`install_path`*`\NetBackup\logs\nbvault`

    The originator ID (OID) for NetBackup Vault is 166.

    See the "Using Logs and Reports" chapter of the *NetBackup Troubleshooting Guide* for more information on unified logging.

The NetBackup Vault Manager (`nbvault`) manages Vault activity and arbitrates access to the Vault robot, vault, and profile configuration information. The NetBackup Vault Manager must run at all times so Vault functions correctly. On Windows systems, use the `bpup.exe` and `bpdown.exe` commands to start and stop the NetBackup services, including the NetBackup Vault Manager. On UNIX systems,

use `netbackup start` and `netbackup stop` to start and stop NetBackup and Vault daemons.

See "Setting the duration and level for log files" on page 140.

See "Logs to accompany problem reports" on page 140.

Setting the duration and level for log files

The amount of information logged and how long it is retained is controlled by the following NetBackup configuration parameters:

- The length of time NetBackup retains debug logs. This setting affects all debug log files that NetBackup generates, not only the Vault debug logs.
- Vault logging level. Cohesity recommends that you use a debug level of 5 when you generate logs that you send to Cohesity for troubleshooting purposes. You can set the debug level to 5 for all Vault sessions or you can use the `-verbose` option on the `vltrun` command in the Vault policy that initiates the Vault job.

For more information on logging properties for Vault management, see *NetBackup Web UI Administrator's Guide, Managing host properties* section.

Logs to accompany problem reports

To troubleshoot problems, Cohesity Customer Service requires a set of log files that NetBackup and Vault produces.

In most circumstances, you must provide log files from the following NetBackup processes:

- `admin` (on the master server); administrative commands process
- `bpcd` (on the primary server); NetBackup client daemon manager
- `bpsched` (on the primary server); NetBackup backup scheduler
- `bptm` (on the media server); NetBackup tape manager
- `nbvault` (on the primary server); Vault Manager service or daemon
- `vault` (on the primary server); Vault commands

Session log files also are useful for troubleshooting problems, and you should include the appropriate session log files with problem reports you send to Cohesity.

If you use the vlteject command or the Vault Operator Menu (vltopmenu) to perform consolidated ejects and reports, the following log file may also be useful:

- UNIX

  `/usr/openv/netbackup/vault/sessions/vlteject.mstr`

- Windows

  `install_path\NetBackup\vault\sessions\vlteject.mstr`

See the *NetBackup Troubleshooting Guide*.

Appendix A

Recovering from disasters

This appendix includes the following topics:

- About disaster recovery
- About disaster recovery in the NetBackup Vault context
- About preparing for recovery
- About recovering NetBackup
- Recovering data and restoring backup images
- Archiving and recovering from a specific point in time

About disaster recovery

This topic provides information about recovering data by using NetBackup and Vault, when you have to recall your media from your off-site storage location. It also provides general information about preparing for a disaster recovery situation.

See the "Disaster Recovery" section in the *NetBackup Troubleshooting Guide*.

Data backup is essential to any data protection strategy, especially a strategy that is expected to assist in disaster recovery. Regularly backing up data and then being able to restore that data within a specified time frame are important components of recovery. Regardless of any other recovery provisions, backup protects against data loss from complete system failure. And off-site storage of backup images protects against damage to your on-site media or against a disaster that damages or destroys your facility or site.

To perform recovery successfully, the data must be tracked to know at what point in time it was backed up. Knowing the time allows your organization to assess the information that cannot be recovered. Configure your data backup schedules to allow your organization to achieve its recovery point objective (RPO), which is the

point in time before which you cannot accept lost data. If your organization can accept one day's data loss, your backup schedule should be at least daily so you can achieve an RPO of one day before any disaster.

Your organization also may have a recovery time objective (RTO), which is the expected recovery time or how long it takes to recover. Recovery time is a function of the type of disaster and of the methods that are used for recovery. You may have multiple RTOs, depending on which services your organization must recover and when.

High availability technologies can make the recovery point very close or even identical to the point of failure or disaster, and they also can provide very short recovery times. However, the closer to the failure that you place your RTO and RPO, the more expensive it is to build and maintain the systems that are required to achieve recovery. Your analysis of the costs and benefits of various recovery strategies should be part of your organization's recovery planning. Understanding disaster recovery planning lets you place Vault and tape-based backups that are stored off-site in the proper context within your disaster recovery objectives.

About what defines a disaster

For an organization, a disaster is an unplanned event that interrupts its ability to function. Usually, the event affects the delivery of critical business functions and results in a loss of data.

The following are generally recognized as the types of disasters possible:

- Technological disasters result in shortcomings in performance, availability, capacity, and accessibility of your IT infrastructures. Technological disasters include computer or Internet crimes, computer viruses, power failures, network or telecommunication failures, hardware or software failures, and other similar failures.
- Human disasters are caused by people, including accidents, explosions, fires, riots, terrorist activities, and other events.
- Natural disasters are caused by nature, including hurricanes, tornadoes, earthquakes, floods, and other natural events.

The effect of a disaster often depends on the scale and timing of the event. Although a disaster is an event that is beyond your control, you can control the way in which your organization reacts to a disaster. By planning and preparing for a disastrous event, you can minimize the effect of the disaster.

About the disaster recovery process

Disaster recovery is the process of responding to an interruption in the services your organization uses to operate. Disaster recovery usually is focused on information, network, and telecommunication services, often at an alternative site and using one or more data-recovery methods.

Disaster recovery is part of a larger topic that is called business recovery, which includes restoring the actual capability for employees to perform their jobs. Business recovery includes logistic related items, such as telephones, office space, living arrangements for employees, and other logistical items. Business recovery itself is part of a larger topic that is called business continuity planning, which includes plans to manage the crisis to your organization, help resume normal business operations, and other inventions.

A resilient organization uses business continuity planning to help ensure that it can survive a disaster and resume operations at an acceptable level.

About disaster recovery plans

A disaster recovery plan is a plan to resume or recover a specific essential operation, function, or process of an organization. Although disaster recovery usually is used to describe information technology and telecommunication services recovery, other services an organization uses to conduct operations can and should be considered part of a plan. For example, an organization's people also are subject to the effects of a disaster and planning should include the effect on them and the resources necessary to help them recover so they can perform their duties.

By planning how your company responds in the event of a disaster, you ensure that your company can do the following:

- Protect critical data.
- Minimize the effect of a disaster.
- Use resources most effectively.
- Maintain business continuity.

About recovery priorities

Your organization must decide between recovery cost (the infrastructure and testing) and the level of functionality that must be recovered. You may choose to recover only the most critical business functions immediately and then recover other functions later. Although all functions of an organization should be valuable and necessary for the organization to operate, it may be acceptable to operate at a reduced level for a specific period of time. The longer your organization can operate without a

function, the easier and less expensive it becomes to recover that function. Therefore, given the higher cost of rapid recovery, only those functions that are required for immediate operation need to be recovered quickly. Delaying recovery of some functions can be a good business decision.

About developing disaster recovery plans

Developing a disaster recovery plan usually begins with an impact analysis that identifies the functions an organization requires to operate and determines how long each function can be unavailable until it affects the organization to an unacceptable extent.

Understanding the effect of disaster helps you identify the objectives for the recovery plan.

The following are examples of the objectives that may be in a disaster recovery plan:

- Ensure service to customers by making critical resources available.
- Minimize economic loss.
- Secure company assets.
- Minimize decision making during the recovery process.
- Reduce reliance on key individuals.
- Ensure a safe and orderly recovery within predetermined time period.
- Maintain a sense of security and organizational stability.

The priority you assign your objectives depends on the needs of your organization. By setting clear, prioritized objectives for your disaster recovery plan, you can reduce your organization's exposure to risks and ensure that your critical systems and networks are available during disruptions.

You can use the two following approaches to create disaster recovery plans:

- A general plan that is used any time a disaster occurs. A general plan should be flexible and is often impact-driven rather than disaster driven (that is, based on the effect to your organization rather than the type of disaster). A general plan usually is based on assumptions that define the scope of each impact in the plan. A general plan is easy to maintain and convenient. However, because it may require that some decisions are made at the time of disaster (such as assessing the type of impact and determining the response), the beginning of recovery can be delayed.
- Multiple smaller plans, each used for a specific disaster that your organization has determined is most likely to occur. For example, individual plans often are

created for power outages, network outages, fires, floods, and other similar occurrences. Individual disaster-specific plans are easier to create than a general plan. It is often clear which plan should be used, so fewer decisions are required at the beginning of recovery, which can result in quicker recovery. However, which plan to use may not always be clear (for example, if a fire causes a power outage). And if a disaster occurs for which a plan does not exist, recovery may be slow to begin and difficult to achieve.

A disaster recovery plan should be easy to follow and not require interpretation. Do not include unnecessary detail. If the plan is implemented, it will be in a time of high stress and pressure to perform; therefore, the plan should be simple, specific, and well tested.

You should publicize your disaster recovery plan within your organization so that everyone knows about it, understands how it works, and understands the reasoning behind the decisions in the plan.

About testing disaster recovery plans

Developing a disaster recovery plan is a waste of time and resources if it is not tested regularly, thoroughly, and frequently (frequently depends on any changes in your organization's functions and environment). The goal of disaster recovery testing is not to pass a test but to find out what does not work. Design your tests to find problems because it is better to find them during a test than during an actual recovery situation.

Testing can be as simple as calling all of the phone numbers in an emergency notification list to verify that everyone can be reached when needed. Or testing can be as complex as actually conducting operations at a recovery site to ensure that everything works correctly. Between those extremes, variations include walkthroughs, during which everyone that is involved in the recovery process discusses their roles in a moderated recovery scenario, and simulations that initiate the recovery plan but use simulated data. Using a combination of testing scenarios to test specific parts of the plan also can be effective.

About disaster recovery in the NetBackup Vault context

In the NetBackup Vault context, disaster recovery means restoring the NetBackup application (primary server, media servers, and clients) and then restoring the data that is stored at the off-site storage facility.

If you use NetBackup and Vault to backup your applications and store removable media at a secure off-site location, you also can perform application recovery so you do not have to reinstall your applications.

About preparing for recovery

Recovering data can be a difficult and time consuming process. The success of recovery often depends on how well you prepare for disaster. Your preparations for disaster and what you have to accomplish during a recovery depends on your recovery systems. For example, suppose your recovery site and systems are already operational and have NetBackup and Vault installed. You do not have to protect the NetBackup installation media and the license keys and install NetBackup during the recovery process. You only have to recover the NetBackup catalogs and data. Conversely, if your recovery systems do not have NetBackup and Vault installed and configured, you have to prepare for that and accomplish it during recovery.

You should do the following to prepare for recovery using NetBackup and Vault. (You may not have to do some of the items listed, and you may have to do more than what is listed.)

- Develop a disaster recovery plan.
- Test the disaster recovery plan.
- Back up and vault data regularly. In addition to backing up files on a regular basis, it is important to select the correct files to back up. You should back up all data that your organization's impact analysis determines is critical and store copies at a secure, off-site storage location.
- If you can recover to the same or identical hardware, back up and vault the applications that your organization's impact analysis determines are critical. You also should back up system files so you can quickly restore a system to normal operation.
  - Include all operating system files in your backups. For Microsoft Windows systems, the Windows system directories include the registry, without which it is impossible to restore a system to its original configuration. If you are using a NetBackup exclude list for a client, do not specify any Windows system files in that list.

    Restoring operating system files is not helpful if you are recovering data to a different system at your original site or disaster recovery site. You can back up those files, but then not restore them if you are recovering to a different system or site.
  - Back up executable and other files for applications you need to conduct critical operations. You may want to save money by using fewer tape

volumes, but backing up critical applications ensures that you can restore them to their exact configurations. For example, if you have applied software updates or patches, restoring from a backup eliminates the need to reapply them, reducing recovery time.

- Every time you vault media, store the Recovery Report securely. The same disaster that destroys your site can destroy your Recovery Report. You need the Recovery Report to identify the media you need to recall from off-site storage. Your vault vendor may let you vault your Recovery Report. If you have a recovery site equipped with computers, email the Recovery Report to that site.
- Record and protect the names of the policies that are used to backup the data you want to recover. The Recovery Report is organized by policy. You need to know which policies are used so you can identify the media you need to recover.
- Record and protect the names of the off-site volume groups for the data you want to recover. Those names are used during the recovery process. Alternatively, you can obtain the off-site volume group names after you restore the NetBackup catalog (because the catalog includes the Vault configuration).
- Document the commands and options that you need to recover data. For example, the `bpchangeprimary` command is used to promote the vaulted images to primary images so that you can restore from them. So you should have a record of the commands and options that you need during the recovery process.
- Protect the NetBackup and Vault installation media. You need the media so you can install NetBackup and Vault on the recovery system if it is not already installed.
- Record and protect the license keys for NetBackup and Vault. You need them for NetBackup and Vault on the recovery system if you have to install NetBackup. You can use temporary license keys if necessary.
- Protect the installation media and record the license keys for any other Cohesity products that must be installed on the recovery systems. For example, if you use the Veritas File System and Veritas Volume Manager on the recovery systems, you need their license keys when you install those products.
- Protect the installation media for the operating system and other applications that are required to run the systems you are using for recovery.
- Protect your DR plan. The same disaster that destroys your site can destroy your DR plan and recovery report. You should have copies stored so that they will be available when needed. Your vault vendor may let you vault a copy of the DR plan.

Note: Effective disaster recovery procedures are specific to an environment and provide detailed information about everything that should be accomplished to prepare for disaster and to recover after disaster occurs. Cohesity provides general disaster recovery information that is intended as a model only. You must evaluate the information and then develop your own disaster recovery plans and procedures.

About recovering NetBackup

See the "Disaster Recovery" section of the *NetBackup Troubleshooting Guide* for information about recovering NetBackup primary servers, media servers, and client systems after a disk failure. The procedures include reinstalling NetBackup and may include reinstalling the operating system if it is required.

You must first ensure that your computer and robotic hardware and any necessary network equipment is operational before you reinstall NetBackup. You can then use an appropriate procedure in the *NetBackup Troubleshooting Guide*.

After you reinstall NetBackup, you may have to configure robots and drives. (If you reinstall NetBackup on the original system, the device configuration is restored if you recover the NetBackup catalogs).

Recovering data and restoring backup images

Recovering data can be a difficult and time consuming process. The success of recovery often depends on how well you prepare for disaster and subsequent recovery.

Note: Effective disaster recovery procedures are specific to an environment and provide detailed information about everything that should be accomplished to prepare for disaster and to recover after disaster occurs. Cohesity provides general disaster recovery information that is intended as a model only. You must evaluate the information and then develop your own disaster recovery plans and procedures.

The steps you have to perform to recover can depend on the configuration of your original system and robotic devices, your original NetBackup configuration, the configuration of your recovery system and robots, and the configuration of NetBackup on the recovery systems. Therefore, providing specific disaster recovery procedures for all situations is not possible. Rather, these procedures are intended as general guidelines from which you can create your own procedures for recovering NetBackup and the data that was transferred off-site.

Although some detail is included about restoring the NetBackup catalogs to a recovery system, these procedures do not provide detail about every step of the recovery procedure.

Information in this section assumes the following:

- The primary backup images are unavailable.
- The NetBackup primary and media server software, Vault software, client software, and devices are installed and robots and drives are configured on systems to which you are recovering data.
- The NetBackup catalogs and data media have not been recalled from off-site storage.
- The Recovery Report is available.
- You know the name of the off-site volume group name to which the recovered images belong.
- You know the names of the original primary and media servers.

To recover data and restore backup images

1. Using the Recovery Report, identify the current catalog backup media and the media that is required to restore the data.

   The Recovery Report is organized by policy, so you should determine which policies were used to back up the data you want to recover.

2. Recall the appropriate catalog backup and data media from off site storage.

3. Recover the catalog.

   See "Recover the Catalog from an Online, Hot Backup" in the *NetBackup Troubleshooting Guide*.

4. If necessary, perform device discovery in NetBackup.

   By default, NetBackup catalog backups include the NetBackup device configuration information. If the recovery system has a different device configuration than the original system, the device configuration from the original system overwrites the device configuration when the catalog is recovered.

5 If the primary and media server names on the recovery system are different than the original system, change the server names in the NetBackup catalogs by using the `bpimage` command.

The `bpimage` command and options required are as follows:

```
bpimage -newserver recovery_system -oldserver original_system
```

You can also use the `bpimage` command if the old system had separate media servers and the recovery system has a combined primary and media server. Use the name of the combined primary or media server for the argument to the `-newserver` option.

6 Specify the backup copy from which to restore by adding the copy number to the file `ALT_RESTORE_COPY_NUMBER`.

After you add the copy number to the file, all subsequent restore operations restore from that backup copy. The restore can be from the Backup, Archive, and Restore interface or from the bprestore command. Exception: the bprestore -copy x option and argument override the value in the ALT_RESTORE_COPY_NUMBER file.

The ALT_RESTORE_COPY_NUMBER file must be in the following directory on the NetBackup primary server:

- UNIX

  ```
  /usr/openv/netbackup
  ```

- Windows

  ```
  install_path\VERITAS\NetBackup
  ```

  See "Restoring from a specific backup copy" in the Backup, Archive, and Restore help.

7 If the media is not suspended or frozen, suspend the media.

Use the `bpmedia` command to suspend the media. Suspending the media prevents NetBackup from writing backup images to that media.

8 Inject the media into the robot.

Injecting the media moves it into the robot and also changes the off-site volume group attribute of the media to robotic volume group so NetBackup knows that the volumes are in the robot and ready for restore operations.

See “About injecting media” on page 82.

9 Using the Backup, Archive, and Restore interface, restore the data.

See the *NetBackup Backup, Archive, and Restore Getting Started Guide*.

10 After restoring all of the data, revault the media.

See "Revaulting unexpired media" on page 92.

Archiving and recovering from a specific point in time

If your data center or computing environment requires recovery to a specific point in time (not just to the most recent valid backups), you can set up a process that ensures that you can recover both the NetBackup catalog and the data for that specific time. You should retain the corresponding catalog backups for the same length of time as the corresponding data backups.

The following high-level information is intended as an overview of how to archive the catalog and data so you can recover to a specific point in time. Detailed instructions for accomplishing all the tasks necessary are not included.

Before you can recover to a specific point in time, you must archive the catalog and data.

To archive the catalog and data to a specific point in time

1 Use your normal procedures to vault the data and NetBackup catalogs for that data.

2 Use the `bpmedia` command to freeze the data volumes and catalog volumes that you want to retain.

Freezing the volumes prevents them from becoming unassigned and from appearing on the Picking List for Vault report. Do not recall the volumes from off-site storage when they expire.

3 Vault a printed copy of the Recovery Report for that specific point in time.

You need the Recovery Report from the specific point in time so you can recall and restore the appropriate catalog and data volumes.

4 Optionally, remove the media IDs from the volume database.

This reduces the size of the database and improves performance. Depending on the number of volumes, maintaining the media IDs in the volume database may not degrade performance much.

To recover the catalog and data to a specific point in time

1. Retrieve the appropriate printed Recovery Report from off-site storage.
2. Using the Recovery Report, recall the appropriate catalog backup and data volumes from off site storage.
3. Recover the catalog that you recalled from off-site storage.

   That version of the catalog contains information about the archived volumes and the images on them.
4. Use the `bpexpdate` command to reset the expiration date on the recalled volumes so they are not expired. Use the `-policy` option to change the expiration date for all media that is associated with a specific policy.
5. Change the images to be recovered to primary (NetBackup restores from the primary image).

   To change a large number of images to primary, use `bpchangeprimary -group` option to specify all images in a specific off-site volume group.

   For information about the `bpchangeprimary` command, see the *NetBackup Commands Reference Guide*.
6. Restore the data.

   The *NetBackup Administrator's Guide, Volume I* includes an alternative procedure for archiving the catalog. That alternative procedure uses the `catarc` catalog archive policy to archive old data in the NetBackup catalog. You can then vault the archived catalog data or a copy of the archived catalog data.

   See "Catalog Archiving" in the *NetBackup Administrator's Guide, Volume I*.

Appendix B

Vault file and directory structure

This appendix includes the following topics:

- UNIX files and directories
- Windows files and directories

UNIX files and directories

Vault is installed in `/usr/openv/netbackup` on UNIX systems. The following table describes the files in each of the directories Vault creates and uses on UNIX systems. Also included are Vault files that reside in NetBackup directories. The files are either copied into the directories during the installation process or created as Vault sessions run. The paths are specified in relation to the NetBackup directory.

Table B-1 lists the files and directories for Vault in UNIX.

Table B-1 Files and directories for Vault in UNIX

Directory, Program, or File	Purpose
`bin/nbvault`	Vault daemon that manages Vault activity.
`bin/vltadm`	Curses-based utility to configure NetBackup Vault and monitor its operations. `vltadm` requires root (administrator) privileges.
`bin/vltcontainers`	Command used to add media logically to containers.
`bin/vlteject`	Command used to eject media from Vault sessions and run the reports that are selected in the profile.

Table B-1 Files and directories for Vault in UNIX *(continued)*

Directory, Program, or File	Purpose
`bin/vltinject`	Command used to inject media into a robot and update the database.
`bin/vltoffsitemedia`	Command that lets the user change the off-site parameters of a given piece of media.
`bin/vltopmenu`	Utility that lets the user initiate a menu screen containing the various options that an operator of the NetBackup Vault feature can use. It allows the user to eject or inject media, print various reports individually or collectively, and consolidate reports and ejects across sessions.
`bin/vltrun`	Process that runs all the NetBackup commands that are used during a Vault session.
`bin/goodies/vlt_ejectlist_notify`	Script called by the vault session just before vault tapes are ejected.
`bin/goodies/vlt_end_notify`	Script called by the vault session just before it exits.
`bin/goodies/vlt_endeject_notify`	Script called by the vault session at the end of eject processing.
`bin/goodies/vlt_start_notify`	Script called by the vault session after it starts.
`bin/goodies/vlt_starteject_notify`	Script called by the vault session when the eject process starts.
`db/vault/vault.xml`	Vault configuration file.
`help/vltadm`	Contains help files for the Vault Administration (vltadm) interface.
`/logs/vault`	Directory where the Vault commands log messages.
`vault`	Main directory for Vault. Contains session directories.
`vault/sessions`	A subdirectory that contains working session directories and log files. In a cluster environment, the sessions directory must reside on the shared disk.
`vault/sessions/cntrDB`	The database of information for media that is vaulted in containers.
`vault/sessions/sid`*`xxx`*	Subdirectory that contains working session subdirectories. Can be manually removed to reduce disk usage if necessary.
`vault/sessions/`*`vault_name`*`/session.last`	Counter to show current duplication session

Table B-1 Files and directories for Vault in UNIX *(continued)*

Directory, Program, or File	Purpose
`allmedia_inventory.rpt`	All Media Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`container_inv.rpt`	Container Inventory report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report in that folder includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/logs/detail.log`	Shows the output of every command that was run during the session.
`detailed_distlist_vault.rpt`	Detailed Distribution List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`distlist_robot.rpt`	Distribution List for Robot Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`distlist_vault.rpt`	Distribution List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/logs/duped.images`	List of images successfully duplicated during the session.
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/logs/duplicate.log.nn`	Contains the output from bpduplicate.

Table B-1 Files and directories for Vault in UNIX *(continued)*

Directory, Program, or File	Purpose
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/eject.list`	List of media to be ejected for the session.
`lostmedia.rpt`	Lost Media Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report will include the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`non_vaulted.rpt`	Non-vaulted Images Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`offsite_inventory.rpt`	Off-site Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`picklist_robot.rpt`	Picking List for Robot report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`picklist_vault.rpt`	Picking List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/preview.list`	A list of all images that to be considered for duplication or ejection by the current vault session.

Table B-1 Files and directories for Vault in UNIX *(continued)*

Directory, Program, or File	Purpose
`recovery.rpt`	Recovery Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault/sessions/`*`vault_name`* `/sid`*`xxx`*`/logs/summary.log`	This file provides a concise view of the critical session details that occurred during a session. For example, the file can contain the following pieces of information: ■ The duration of a session ■ The robot, vault, profile, session ID, and Job ID ■ A summary report that shows the primary server, start and stopped times, and the exist status. The exit status can show if an error occurred and which session step if occurred at. This log is appended for email notification.
`summary_distlist_vault.rpt`	Summary Distribution List report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault_inventory.rpt`	Vault Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.

Windows files and directories

Vault is installed in the directory that is specified by *`install_path`*`\NetBackup` on Windows systems. The following table describes the files in each of the directories Vault creates and uses on Windows. Also included are Vault files that reside in NetBackup directories. The files are either copied into the directories during the installation process or created as Vault sessions run. The paths are specified in relation to the NetBackup directory.

Table B-2 lists the files and directories for Vault in Windows.

Table B-2 Files and Directories for Vault in Windows

Directory, Program, or File	Purpose
`bin\nbvault.exe`	NetBackup Vault Manager service.
`bin\vltcontainers.exe`	Command used to add media logically to containers.
`bin\vlteject.exe`	Command used to eject media from Vault sessions and run the reports that are selected in the profile.
`bin\vltinject.exe`	Command used to inject media into a robot and update the Media Manager database.
`bin\vltoffsitemedia.exe`	Command that lets the user to change the off-site parameters of a given piece of media.
`bin\vltopmenu.exe`	Utility that lets the user initiate a menu screen containing the various options that an operator of the NetBackup Vault feature can use. It lets the user eject or inject media, print various reports individually or collectively, and consolidate reports and ejects across sessions.
`bin\vltrun.exe`	Process that runs all the NetBackup commands that are used during a Vault session.
`bin\goodies\vlt_ejectlist_notify`	Script called by the vault session just before vault tapes are ejected.
`bin\goodies\vlt_end_notify`	Script called by the vault session just before it exits.
`bin\goodies\vlt_endeject_notify`	Script called by the vault session at the end of eject processing.
`bin\goodies\vlt_start_notify`	Script called by the vault session after it starts.
`bin\goodies\vlt_starteject_notify`	Script called by the vault session when the eject process starts.
`db\vault\vault.xml`	Vault configuration file.
`logs\nbvault`	Directory where the Vault service, `nbvault.exe`, logs messages.
`logs\vault`	Directory where the Vault commands log messages.
`vault`	Main Vault directory. Contains the session directories.
`vault\sessions`	A subdirectory containing working session directories and log files. In a cluster environment, the sessions directory must reside on the shared disk.
`vault\sessions\cntrDB`	Database of information for media that is vaulted in containers.

Table B-2 Files and Directories for Vault in Windows *(continued)*

Directory, Program, or File	Purpose
`vault\sessions\sid`*`xxx`*	Subdirectory containing working session subdirectories. Can be manually removed to reduce disk usage if necessary.
`vault\sessions\`*`vault_name`*`\session.last`	Counter to show current duplication session
`allmedia_inventory.rpt`	All Media Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`container_inv.rpt`	Container Inventory report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report in that folder includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\logs\detail.log`	Shows the output of every command that was run during the session.
`detailed_distlist_vault.rpt`	Detailed Distribution List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report in that folder includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`distlist_robot.rpt`	Distribution List for Robot report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`distlist_vault.rpt`	Distribution List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\logs\duped.images`	List of images successfully duplicated during the session.

Table B-2 Files and Directories for Vault in Windows *(continued)*

Directory, Program, or File	Purpose
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\logs\duplicate.log.nn`	Contains the output from bpduplicate.
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\eject.list`	List of media to be ejected for the session.
`lostmedia.rpt`	Lost Media Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`non_vaulted.rpt`	Non-vaulted Images Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`offsite_inventory.rpt`	Off-site Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`picklist_robot.rpt`	Picking List for Robot report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`picklist_vault.rpt`	Picking List for Vault report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\preview.list`	A list of all images to be considered for duplication or ejection by the current vault session.

Table B-2 Files and Directories for Vault in Windows *(continued)*

Directory, Program, or File	Purpose
`recovery.rpt`	Recovery Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile Reports tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault\sessions\`*`vault_name`* `\sid`*`xxx`*`\logs\summary.log`	This file provides a concise view of the critical session details that occurred during a session. For example, the file can contain the following pieces of information: ■ The duration of a session ■ The robot, vault, profile, session ID, and Job ID ■ A summary report that shows the primary server, start and stopped times, and the exist status. The exit status can show if an error occurred and which session step if occurred at. This log is appended for email notification.
`summary_distlist_vault.rpt`	Summary Distribution List report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.
`vault_inventory.rpt`	Vault Inventory Report. If a report name includes a timestamp, it is part of a consolidated report operation. If you configure the profile **Reports** tab to write reports to a folder, the file name of the report includes the session ID. Report file names that include `_ff` are for debug purposes only. They are created when the reports are generated.

Index

A

ACS number 39
ACSLS server 39
adding alternate media server names 23, 41
All Media Inventory report 119
alternate media server names
    adding 23, 41
Alternate Media Server Names tab 41
At Time of Eject setting (Suspend This Session's Media) 63

B

Backup Policies setting 52
Backups Started setting 53
bpdbjobs
    changes for Vault 134

C

CAP.. *See* media access port
catalog backup
    Catalog Backup Schedule setting 59
    Skip the Catalog Backup Step setting 59
changing off-site volume group name 127
changing off-site volume pool name 127
changing volume group name 127
changing volume pool name 127
choose backups
    Backup Policies setting 52
    Backups Started setting 53
    Clients setting 53
    disk pools 53
    Media Servers setting 54
    Schedules setting 54
    Source Volume Group setting 54
    Type Of Backups setting 55
    Volume pools 55
clearing the media description field 99
clearing the vault fields 83
Clients setting 53
clusters 16
    shared disk 159
Complete Inventory List for Vault. *See* All Media Inventory report
Complete Inventory List for Vault.. *See* All Media Inventory report
concurrent copies
    continue or fail 101
    during original backup 102
    overview 100
configuration
    Eject tab 59
    methods 39
    profile 51
    Reports tab 65
    volume pools 34
Container Inventory Report 120
Containers of Many Media setting 48
continue
    for concurrent copies 101
copying a profile 126
creating
    a profile 49
    a vault 45
    a vault policy 70
critical policies 58

D

debug logs 139
deferred reports 68
Deferred setting (Eject Mode) 63
Detailed Distribution List for Vault 112
disaster recovery
    definition 144
    definition of disaster recovery plan 144
    developing a disaster recovery plan 145
    preparing for disaster 142
    priorities 145
    testing a disaster recovery plan 146
Distribution List for Vault 111, 116
duplicate images 11

E

e-mail
    notifying a tape operator when eject begins 95
eject
    consolidating ejects 81
    Eject Mode setting 63
    Suspend Media On Which Backups Were Written setting 64
Eject Mode settings 63
Eject tab 59
eject.list file 75
ejected tapes returned to robot 138
ejecting partial images
    use suspend to avoid 24
error codes 136
EXIT status 136

F

fail
    for concurrent copies 101
First Off-Site Slot ID setting 48
Full Inventory List for Vault.. *See* Off-site Inventory report

G

General tab 41

I

images
    duplicate 11
    original 11
Immediate Eject setting 63
immediate reports 68
Immediate setting (Eject Mode) 63
Immediately setting (Suspend This Session's Media) 63
Inventory List for Vault.. *See* Vault Inventory report
Iron Mountain Electronic Format report 124

L

log files
    debug logs 139
    set duration 140
    vault session 130
LSM number 39

M

MAP.. *See* media access port
media access port
    capacity 39
    number 39
    to use for eject 48
media description field
    clearing 99
media missing in robot 137
media server names
    adding alternate 23, 41
Media Servers setting 54
menu user interface
    bpdbjobs 134
    overview 131
    Vault Administration Interface 131
    Vault Oerator Menu Interface 132
    vltadm 131
    vltopmenu 132
Monitoring a vault session 74
moving a vault to different robot 127
multiple copies 100
    overview 100

N

notify scripts
    for a specific profile 98
    for a specific robot 97
    for a specific vault 98
    order of execution 98
    using 96
    vlt_ejectlist_notify 96
    vlt_end_notify 97
    vlt_endeject_notify 97
    vlt_start_notify 96
    vlt_starteject_notify 97
notifying a tape operator when eject begins 95

O

Off-site Inventory report 118
off-site volume group 49
    renaming 127
Off-Site Volume Group setting 49
off-site volume pool 34
    renaming 127
Off-Site Volume Pools setting 64
Off-site Volume Pools windows (Eject tab) 64
organizing reports by profile 31

organizing reports by robot 30
organizing reports by vault 31
original images 11

P

partial backups
    use suspend to avoid vaulting 24
Picking List for Robot 110
Picking List for Vault 115
policy 70
    NetBackup policy for Vault 70
preferred vaulting strategies 21
preview vault session 73
preview.list file 73
printing
    troubleshooting problems 135
profile
    configuring 51
    copying a 126
    creating 49
    notify script for a specific 98
    organizing reports by 31
    overlap time window 22
Profile dialog 50

R

recovery
    keep primary copy on site 28
    match volume pools to usage 27
    preparing for efficient 26
    revault unexpired media 29
    use precise naming conventions 27
    vault NetBackup catalogs 26
Recovery Report for Vault 121
renaming off-site volume group 127
renaming off-site volume pool 127
renaming volume group 127
renaming volume pool 127
reports
    All Media Inventory 119
    Complete Inventory List for Vault.. *See* All Media Inventory report
    consolidating reports 108
    Container Inventory Report 120
    deferred 68
    Detailed Distribution List for Vault 112
    Distribution List for Robot 116
    Distribution List for Vault 111
reports *(continued)*
    Full Inventory List for Vault.. *See* Off-site Inventory report
    immediate 68
    inventory 117
    Inventory List for Vault.. *See* Vault Inventory report
    Iron Mountain Electronic Format 124
    Lost Media Report 31, 122
    Off-site Inventory 118
    organizing by profile 31
    organizing by robot 30
    organizing by vault 31
    Picking List for Robot 110
    Picking List for Vault 115
    printing 104
    Recovery Report for Vault 121
    Summary Distribution List for Vault 114
    types of 110
    Vault Inventory report 117
Reports tab 43, 65
resource contention
    vault original backups to avoid 22
resuming a vault session 74
Retention level setting 54
revault media 92
robot
    control host 45
    notify script for a specific 97
    organizing reports by 30
Robot Name setting 45
robotic volume group 24
Robotic Volume Group setting 49
running multiple sessions simultaneously 72

S

Schedules setting 54
scratch volume pools 29
server name group 42
Skip the Catalog Backup Step setting 59
Skip the Eject Step setting 64
Slot ID 48
Slots for Individual Media setting 49
Source Volume Group setting 54
status codes 136
Summary Distribution List for Vault 114
supported clusters 16
supported robots 16
supported systems 16

suspend
Suspend Media On Which Backups Were Written setting 24
Suspend Option setting 24
use suspend to avoid partial backups 24
Suspend Media for the Next Session setting 64
Suspend Media on Which Backups Were Written setting 64
Suspend Option setting 64
Suspend This Session's Media setting 64

T

time window
overlapping 23
troubleshooting
drive or robot offline 137
ejected tapes returned to robot 138
ejecting tapes while in use 138
error codes 136
logs 140
media missing in robot 137
printing problems 135
Types Of Backups setting 55

V

Vault
accessing 11
vault
clearing the Vault fields 83
creating a 45
moving to a different robot 127
name 49
notify script for a specific 98
only the intended backups 24
organizing reports by 31
original backups 22
paradigm 12, 21
policy 70
vendor 49
Vault Administration Interface 131
Vault dialog 46
Vault Inventory report 117
Vault Management Properties dialog
Alternate Media Server Names tab 41
General tab 41
Reports tab 43
Vault Name setting 49
Vault Operator Menu Interface 132
vault original backups 22
vault session
previewing 73
resuming 74
running 70
running multiple sessions simultaneously 72
stopping 74
Vault Vendor setting 49
vaulting
containers 48
defined 12
original backups in a 24x7 environment 26
paradigm 12, 21
preferred strategies 21
vltoffsitemedia command
changing Vault attributes 94
volume group
configuration 49
renaming 127
robotic 49
source 54
volume pool
configuration 34
for backup media that remains on site 34
for catalog media 34
match to data usage 27
naming conventions 27
off-site 34
overview 34
renaming 127
use scratch volume pools 29

W

Windows files and directories 158