NetBackup™ AdvancedDisk Storage Solutions Guide

UNIX, Windows, Linux

Release 11.2.0.1

COHESITY

NetBackup AdvancedDisk Storage Solutions 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 Introducing AdvancedDisk 7

About the AdvancedDisk storage option 7

Chapter 2 Licensing AdvancedDisk 9

About the AdvancedDisk license 9
License AdvancedDisk 9

Chapter 3 Configuring AdvancedDisk 11

Configuring the AdvancedDisk option 12
About AdvancedDisk file system requirements 13
Configure the NetBackup service credentials for CIFS storage and disk storage units 14
About AdvancedDisk storage servers 15
About AdvancedDisk data movers 15
About AdvancedDisk preferred or required read servers 16
About data encryption for AdvancedDisk storage 18
About key management for encryption of NetBackup AdvancedDisk storage 19
Configuring key management for NetBackup AdvancedDisk storage encryption 20
Set up the KMS database for NetBackup AdvancedDisk storage encryption 21
Create a KMS key group for NetBackup AdvancedDisk storage encryption 23
Create a KMS key for NetBackup AdvancedDisk storage encryption 24
Save a record of the KMS key names for NetBackup AdvancedDisk storage encryption 25
Configure an AdvancedDisk storage server 27
AdvancedDisk storage server configuration options 30
About AdvancedDisk disk pools 31
Configure a CIFS disk volume for AdvancedDisk encryption 32
Configure an AdvancedDisk disk pool 33

NetBackup nbdevconfig command options for AdvancedDisk disk pools 36
AdvancedDisk disk pool properties 38
Configure an AdvancedDisk storage unit 39
AdvancedDisk storage unit properties 40
About AdvancedDisk storage unit recommendations 42
About storage lifecycle policies 43
Creating a storage lifecycle policy 44
Storage lifecycle policy settings 44
Resilient network properties 47
Specify resilient connections for clients 49

Chapter 4 Managing AdvancedDisk 52

Manage AdvancedDisk storage servers 52
View AdvancedDisk storage servers 52
Determine the AdvancedDisk storage server state 53
View AdvancedDisk storage server attributes 53
Remove AdvancedDisk storage server attributes 54
Remove an AdvancedDisk storage server from disk pool access 55
Delete an AdvancedDisk storage server 55
Manage AdvancedDisk disk pools 56
View AdvancedDisk disk pools 56
About changing the AdvancedDisk disk pool size 56
Adding volumes to an AdvancedDisk disk pool 57
Change the AdvancedDisk disk pool properties 57
Enable active write-stream allocation in AdvancedDisk pool 58
Determine the AdvancedDisk disk pool state 59
Changing AdvancedDisk disk pool state 59
Determine the AdvancedDisk disk volume state 59
Change AdvancedDisk disk volume state 60
Merge AdvancedDisk disk pools 61
Remove a volume from an AdvancedDisk disk pool 62
Delete an AdvancedDisk disk pool 62
About monitoring AdvancedDisk storage capacity and usage 63
Monitor NetBackup disk activity 63
View AdvancedDisk disk reports 64
Display detailed AdvancedDisk storage usage information 65
NetBackup disk volume capacity and usage reference 66
Display KMS key information for AdvancedDisk encryption 68

Chapter 5 Troubleshooting AdvancedDisk 71

About unified logging 71
About using the `vxlogview` command to view unified logs 72
Examples of using vxlogview to view unified logs 74
About legacy logging 75
Creating NetBackup log file directories for AdvancedDisk 76
NetBackup AdvancedDisk log files 77
AdvancedDisk troubleshooting 79
Resolve an incorrect storage type problem 79

Chapter 1

Introducing AdvancedDisk

This chapter includes the following topics:

- About the AdvancedDisk storage option

About the AdvancedDisk storage option

The NetBackup AdvancedDisk storage option lets you use the disk storage that is exposed to NetBackup as a file system for backups. Storage can be direct attached storage (DAS), network attached storage (NAS), or storage area network (SAN) storage.

NetBackup requires exclusive access to the storage for capacity management and load balancing.

Table 1-1 describes some of the benefits of AdvancedDisk storage.

Table 1-1 AdvancedDisk features and benefits

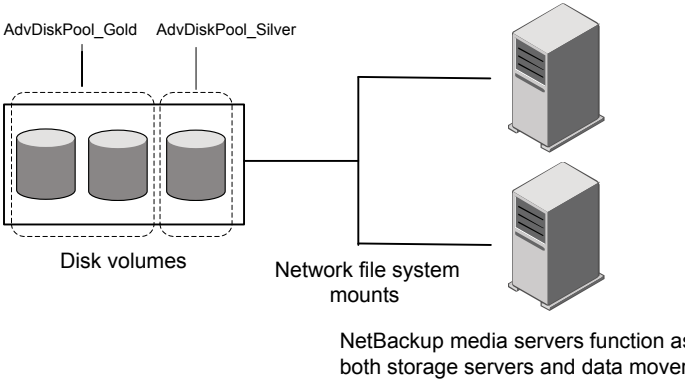
Feature	Benefit
Easy to deploy and use	NetBackup discovers the storage and uses NetBackup storage units and backup policies to use the storage.
Simplified growth	Lets you increase storage unit capacity by adding disks. Only add the capacity required, then update the NetBackup disk pools. Logical units of storage span physical boundaries, so you do not have to create new NetBackup storage units or change the backup policies.
Storage sharing	Multiple storage units can share a disk pool. Space is allocated dynamically as required. Automatic space allocation reduces the risk of backup failure.

Table 1-1 AdvancedDisk features and benefits *(continued)*

Feature	Benefit
Best fit selection	NetBackup predicts the size of the backup and selects the storage on which the backup fits best. The goal is to avoid out-of-space conditions and disk spanning.
Load balancing	Load balancing can occur at two levels, as follows: ■ Storage servers. If you have more than one storage server, NetBackup chooses the least busy media server for each backup. Load balancing increases the performance and the success of backup jobs. ■ Storage unit groups. If you have more than one storage unit, you can choose the storage unit group **Load Balance** option. If the destination of each storage unit is a separate disk pool, NetBackup chooses the least busy disk pool.
Intelligent capacity management	NetBackup expires backup images when the storage that is consumed reaches a threshold. The disk pool high water mark applies to both individual disk volumes and to disk pools.
Storage lifecycle	You can classify data based on its importance and manage it differently throughout each stage of its life. After it has been duplicated, data can be selectively expired based on the relative importance to the business. you can ensure that important backups are available for rapid restore for longer periods, ensuring your recovery time objectives.

Figure 1-1 shows a media server and attached disks.

Figure 1-1 AdvancedDisk storage example



Chapter 2

Licensing AdvancedDisk

This chapter includes the following topics:

- About the AdvancedDisk license
- License AdvancedDisk

About the AdvancedDisk license

AdvancedDisk is a feature that is licensed separately from base NetBackup.

See "License AdvancedDisk" on page 9.

If you remove the license key or if it expires, the following restrictions apply:

- You cannot create the disk pools or the storage units that reference AdvancedDisk disk pools.
- NetBackup jobs that attempt to use the disk pools or the storage units that are based on disk pools fail. The error message indicates that the feature is not licensed.

NetBackup does not delete the disk pools or the storage units that reference the disk pools. You can use them again if you enter a valid license.

License AdvancedDisk

No special installation is required for the NetBackup components of AdvancedDisk. However, you must enter a license. If you installed the license when you installed or upgraded NetBackup, you do not need to perform this procedure.

To license AdvancedDisk

1. Open the NetBackup web UI and sign into the NetBackup primary server.
2. Select **Settings > License management**.

3 Select **Add license**.

4 Selection the option **File system**.

5 Select **Browse** to select the file that you want to add.

6 Select **Add**.

Chapter 3

Configuring AdvancedDisk

This chapter includes the following topics:

- Configuring the AdvancedDisk option
- About AdvancedDisk file system requirements
- Configure the NetBackup service credentials for CIFS storage and disk storage units
- About AdvancedDisk storage servers
- About AdvancedDisk data movers
- About AdvancedDisk preferred or required read servers
- About data encryption for AdvancedDisk storage
- About key management for encryption of NetBackup AdvancedDisk storage
- Configuring key management for NetBackup AdvancedDisk storage encryption
- Configure an AdvancedDisk storage server
- About AdvancedDisk disk pools
- Configure a CIFS disk volume for AdvancedDisk encryption
- Configure an AdvancedDisk disk pool
- Configure an AdvancedDisk storage unit
- About storage lifecycle policies
- Creating a storage lifecycle policy
- Resilient network properties
- Specify resilient connections for clients

Configuring the AdvancedDisk option

This section provides an overview of how to configure the NetBackup AdvancedDisk option.

To configure a base NetBackup environment, see the *NetBackup Administrator's Guide, Volume I*:

https://support.cohesity.com/s/article/article-100040135

Table 3-1 AdvancedDisk configuration tasks

Step	Task	Section
Step 1	Learn about file system requirements	See "About AdvancedDisk file system requirements" on page 13.
Step 2	Learn about storage servers, data movers, and disk pools	See "About AdvancedDisk storage servers" on page 15. See "About AdvancedDisk data movers" on page 15. See "About AdvancedDisk disk pools" on page 31.
Step 3	Optionally, configure the Key Management Service	The Key Management Service is required if you use data encryption for the AdvancedDisk storage.
Step 4	Configure a storage server	See "Configure an AdvancedDisk storage server" on page 27.
Step 5	Optionally, configure CIFS disk volumes	For the **AdvancedDisk_crypt** disk type, you must configure CIFS volumes before you can add them to the disk pool. See "Configure a CIFS disk volume for AdvancedDisk encryption" on page 32.
Step 6	Configure a disk pool	See "Configure an AdvancedDisk disk pool" on page 33.
Step 7	Configure a storage unit	See "Configure an AdvancedDisk storage unit" on page 39.
Step 8	Create a storage lifecycle policy	See "About storage lifecycle policies" on page 43. See "Creating a storage lifecycle policy" on page 44.
Step 9	Create a backup policy	

Table 3-1 AdvancedDisk configuration tasks *(continued)*

Step	Task	Section
Step 10	Optionally, configure resilient network connections	See "Resilient network properties" on page 47.

About AdvancedDisk file system requirements

AdvancedDisk can read and write any nonshared file system that NetBackup supports. However, AdvancedDisk is subject to any operating system or file system requirements or limitations. Requirements and limitations may exist beyond those mentioned in this topic. For supported file systems, see the NetBackup operating system compatibility list.

Disk pool configuration may affect how you configure your file systems.

See "Configure an AdvancedDisk disk pool" on page 33.

Table 3-2 Additional requirements and limitations for file systems

File system	Requirements and limitations
CIFS	Windows Common Internet File System (CIFS) requirements: ■ Ensure that the Windows disk shares are configured to reconnect on login. ■ Networked mapped devices are not visible to Windows services; therefore, NetBackup cannot discover CIFS disk volumes. You must use the Windows Universal Naming Convention (UNC) to specify the CIFS volumes that you want to use for **AdvancedDisk** disk pools. ■ You must configure two Windows services to use the same credentials. See "Configure the NetBackup service credentials for CIFS storage and disk storage units" on page 14. ■ You cannot delete a disk pool that is created by specifying volumes (such as for CIFS volumes). The disk pool exists until you delete its storage server.

Table 3-2 Additional requirements and limitations for file systems *(continued)*

File system	Requirements and limitations
NFS	Network File System (NFS) requirements: ■ You must use manual mount points. Automatic mount and unmount can change mount points, which may cause disk resources to be unavailable. ■ The NFS server that exports the mount points must be configured to allow root access to the file systems. ■ NFS uses a file system paradigm to manage objects. Therefore, carefully choose the volumes to include in the disk pool. For example, NetBackup does not filter out common file system mount points, such as `/` and `/usr` on UNIX and Linux systems. You should not use those mount points for storage. ■ Cohesity recommends that you do not span backup images across NFS volumes in an AdvancedDisk disk pool. File system full conditions cannot be detected adequately. Therefore, a disk pool based on NFS volumes should be comprised of only one volume.
ZFS	Cohesity recommends that you do not span backup images across ZFS volumes in an AdvancedDisk disk pool. File system full conditions cannot be detected adequately. Therefore, a disk pool based on ZFS volumes should be comprised of only one volume.

Configure the NetBackup service credentials for CIFS storage and disk storage units

For Common Internet File System (CIFS) storage with AdvancedDisk and BasicDisk storage units, the NetBackup Client Service and the NetBackup Remote Manager and Monitor Service services on Windows computers must using the same account credentials. If the account credentials are not configured properly, NetBackup marks all CIFS AdvancedDisk and BasicDisk storage units that use the UNC naming convention as DOWN.

To configure service credentials for CIFS storage and disk storage units

1. On the media servers that have a file system mount on the CIFS storage, configure the account and the credentials.

   The account must be the same account that the Windows operating system uses for read and write access to the CIFS share.

2. In Windows, configure both the NetBackup Client Service and the NetBackup Remote Manager and Monitor Service to run under the same Windows user account that you created in step 1.

   See your Windows documentation for details on how to configure the account for the services.

About AdvancedDisk storage servers

A storage server is a NetBackup media server that mounts the disk storage and writes data to and reads data from the disk storage.

For AdvancedDisk, NetBackup media servers function as both storage servers and data movers.

See "About AdvancedDisk data movers" on page 15.

Multiple storage servers can exist. The storage servers share the storage equally.

If you configure more than one storage server, be aware of the following:

- Each media server must mount the file systems of all the disk volumes within a disk pool.
- The mount points must be the same on each media server.
  NetBackup does not validate mount points, so you must ensure that the mount points are the same for each media server. You also must ensure that the mount points are valid.
- To obtain a consolidated list of disk volumes, NetBackup queries every media server. For large sets of servers, queries may affect performance.
- Disk volume status is monitored on a single media server. Which server monitors the status can change. Therefore, a change in disk volume availability on one media server may not be reflected in the disk volume status NetBackup reports.

An AdvancedDisk storage server can have the attributes that can help you manage your restore and your duplication traffic.

See "About AdvancedDisk preferred or required read servers" on page 16.

Storage servers are either **AdvancedDisk** type or **AdvancedDisk_crypt** type.

See "About data encryption for AdvancedDisk storage" on page 18.

Whether or not you want to specify storage server attributes or use encryption determines how you configure the storage servers.

See "Configure an AdvancedDisk storage server" on page 27.

About AdvancedDisk data movers

A data mover transfers data from primary storage (a NetBackup client) to secondary storage during backups. It also can move data back to primary storage during restores and from secondary storage to tertiary storage during duplication.

You do not configure data movers separately. For AdvancedDisk, NetBackup media servers function as both storage servers and data movers. Data movers are configured when you configure storage servers.

About AdvancedDisk preferred or required read servers

When you configure a storage server, you can specify that you want it to be preferred or required for restore jobs. You also can specify whether a server should be required for the read side of duplication jobs. These attributes can help manage the restore and the duplication traffic.

The following are the requirements to configure encryption:

- You must use the `nbdevconfig` command to configure the storage servers and the disk pools.
- You must use the `-setattribute` option when you configure the storage servers and the disk pools.
  Table 3-3 describes the possible arguments for the `-setattribute` option.

See "Configure an AdvancedDisk storage server" on page 27.

Table 3-3 Preferred or required read server descriptions

Argument	Description
`PrefRestore`	The server is preferred for the read side of restore operations. You can configure more than one server as preferred for restore. If you configure preferred for restore but not required for restore, NetBackup considers preferred storage servers for jobs first. If none are available, NetBackup considers any configured storage server. Normal NetBackup load balancing occurs among all storage servers marked `PrefRestore`.

Table 3-3 Preferred or required read server descriptions *(continued)*

Argument	Description
`ReqRestore`	The server is required for the read side of restore operations. You can configure more than one server as required for restore. If you configure required servers for restore but not preferred servers, jobs queue until a required server is available to execute the job. Other servers are never considered for restore jobs. Normal NetBackup rules for job retry apply. If you configure both preferred and required storage servers and a required server is not available, NetBackup considers preferred servers for jobs. If none are available, jobs queue until a required or preferred server is available. Other servers are never considered for restore jobs. Normal NetBackup load balancing occurs for all required servers. Load balancing does not occur between the required and preferred servers.
`ReqDuplicate`	The server is required for the read side of duplication operations. You can configure more than one server as required for duplication. If any server is configured as required for duplication, NetBackup considers only required for duplication servers for jobs. If a required server is unavailable, jobs queue until a required server is available to execute the job. Normal NetBackup rules for job retry apply. Required for duplication also applies to storage server allocation for synthetic backup operations.

Only the media servers that are configured in the storage unit are considered for jobs. Therefore, if you configure a subset of the disk pool media servers in a storage unit, NetBackup selects from those servers only.

If you use the preferred or required restore or duplication attributes for a storage server, the following may occur:

- A restore operation uses a storage server that does not have a `PrefRestore` or `ReqRestore` attribute. Reasons may be as follows:
  - The destination disk pool does not include a storage server with a restore or a duplication attribute.
  - A preferred or required storage server cannot be used because it is unavailable (NetBackup considers it DOWN).
- A restore or a duplication operation is queued.
  The reason may be that a preferred or required storage server cannot be used because it is unavailable (NetBackup considers it DOWN).

If you do not configure preferred or required restore servers, NetBackup uses normal criteria to select a media server for restore or duplication. (That is, if you configure more than one storage server.)

Information about how NetBackup balances storage unit and media server load is available.

See “Maximum concurrent jobs” in the NetBackup Web UI Administrator’s Guide.

You can use preferred or required restore servers rather than the **Media host override** host property.

Information about the **Media host override** property is available.

See “General Server properties” in the NetBackup Web UI Administrator’s Guide.

About data encryption for AdvancedDisk storage

You can encrypt your data on the storage that you use for AdvancedDisk. The following are the requirements to configure encryption:

- You must configure the NetBackup Key Management Service so that NetBackup can manage the encryption keys. NetBackup uses KMS to manage encryption keys. You must use NetBackup commands to configure both the Key Management Service and the AdvancedDisk storage server.
  See “About key management for encryption of NetBackup AdvancedDisk storage” on page 19.
- You must use the `nbdevconfig` command to configure the storage servers and the disk pools.
- You must use the `AdvancedDisk_crypt` type when you configure the storage servers and the disk pools.

After you configure KMS and **AdvancedDisk_crypt** storage servers and disk pools, NetBackup uses encryption for backup jobs to those disk pools.

Note: NetBackup does not span volumes for the **AdvancedDisk_crypt** type of disk pool.

See “About AdvancedDisk disk pools” on page 31.

AdvancedDisk encryption is supported on a subset of operating systems that NetBackup supports. For supported systems, see the NetBackup compatibility lists on the NetBackup support landing page.

https://support.cohesity.com/s/article/article-100040093

More information about data-at-rest encryption and security is available.

See the *NetBackup Security and Encryption Guide*:

https://support.cohesity.com/s/article/article-100040135

About key management for encryption of NetBackup AdvancedDisk storage

NetBackup uses the Key Management Service (KMS) to manage the keys for the data encryption for disk storage. KMS is a NetBackup primary server-based symmetric key management service. The service runs on the NetBackup primary server. An additional license is not required to use the KMS functionality.

NetBackup uses KMS to manage the encryption keys for AdvancedDisk storage.

See "About data encryption for AdvancedDisk storage" on page 18.

The following table describes the encryption keys that are required for the KMS database.

Table 3-4 Encryption keys required for the KMS database

Key	Description
Host Master Key	The Host Master Key protects the key database. The Host Master Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.
Key Protection Key	A Key Protection Key protects individual records in the key database. The Key Protection Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.

The following table describes the encryption keys that are required for each storage server and volume combination.

Table 3-5 Encryption keys required for each storage server and volume combination

Key	Description
A key group	A key group key protects the key group. Each storage server and volume combination requires a key group, and each key group key requires a pass phrase. The key group name must use the format for the storage type that is described as follows: For AdvancedDisk storage, the format depends on the operating system type that hosts the storage, as follows: ■ UNIX storage: *storage_server_name*:*volume_name* The following items describe the requirements for the key group name components for AdvancedDisk storage on UNIX: ■ *storage_server_name* : You must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server. ■ The colon (:) is required after the *storage_server_name*. ■ *volume_name* : Use the last directory name in the storage path for the *volume_name* . For example, use `backups` if the storage path is `/mnt/disk/backups`. ■ Windows storage: *storage_server_name*: The following items describe the requirements for the key group name components for AdvancedDisk storage on Windows: ■ *storage_server_name* : You must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server. ■ The colon (:) is required after the *storage_server_name*.
A key record	Each key group that you create requires a key record. A key record stores the actual key that protects the data for the storage server and volume.

See "Configuring key management for NetBackup AdvancedDisk storage encryption" on page 20.

More information about KMS is available in the *NetBackup Security and Encryption Guide*:

https://support.cohesity.com/s/article/article-100040135

Configuring key management for NetBackup AdvancedDisk storage encryption

For AdvancedDisk storage, encryption is optional. If you do not use encryption, you do not have to configure key management. To use encryption, you must first configure key management by using NetBackup commands. See Table 3-6.

Table 3-6 Configure key management by using NetBackup commands

Step	Task	Instructions
Step 1	Learn about NetBackup key management	See "About key management for encryption of NetBackup AdvancedDisk storage" on page 19.
Step 2	Set up the KMS database	See "Set up the KMS database for NetBackup AdvancedDisk storage encryption" on page 21.
Step 3	Create the key groups	Each storage server and volume combination requires a key group. See "Create a KMS key group for NetBackup AdvancedDisk storage encryption" on page 23.
Step 4	Create the key records	Each key group requires a key record. The key record contains the encryption key. See "Create a KMS key for NetBackup AdvancedDisk storage encryption" on page 24.
Step 5	Save a record of the key names	The record of the key names lets you recreate the keys if they are lost. See "Save a record of the KMS key names for NetBackup AdvancedDisk storage encryption" on page 25.

Set up the KMS database for NetBackup AdvancedDisk storage encryption

Setting up the KMS database is the first task in the process of configuring the NetBackup Key Management Service by using NetBackup commands.

See "Configuring key management for NetBackup AdvancedDisk storage encryption" on page 20.

To set up the KMS database

1. On the NetBackup primary server, create the KMS database by running the `nbkms` command with the `-createemptydb` option, as follows:

   UNIX: `/usr/openv/netbackup/bin/nbkms -createemptydb`

   Windows: *`install_path`*`\Veritas\NetBackup\bin\nbkms.exe -createemptydb`

   The following prompt appears:

   ```
   Enter the Host Master Key (HMK) passphrase (or hit ENTER to use a
   randomly generated HMK). The passphrase will not be displayed on
   the screen.
   Enter passphrase :
   ```

2. Enter a passphrase for the host master key (HMK) or press **Enter** to create a randomly generated key.

   After you enter the Host Master Key passphrase, the following prompt appears:

   ```
   An ID will be associated with the Host Master Key (HMK) just
   created. The ID will assist you in determining the HMK associated
   with any key store.
   Enter HMK ID :
   ```

3. Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.

   After you enter the Host Master Key ID, the following prompt appears:

   ```
   Enter the Key Protection Key (KPK) passphrase (or hit ENTER to use
   a randomly generated KPK). The passphrase will not be displayed on
   the screen.
   Enter passphrase :
   ```

4. Enter a pass phrase for the Key Protection Key or press **Enter** to create a randomly generated key.

   After you enter the Key Protection Key passphrase, the following prompt appears:

   ```
   An ID will be associated with the Key Protection Key (KPK) just
   created. The ID will assist you in determining the KPK associated
   with any key store.
   Enter KPK ID :
   ```

5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

6 In the Activity monitor, start the NetBackup Key Management Service on the primary server.

After you start the service, the initial database setup is complete.

7 After you set up the database, create key groups for the volumes in the disk pool.

See "Create a KMS key group for NetBackup AdvancedDisk storage encryption" on page 23.

Create a KMS key group for NetBackup AdvancedDisk storage encryption

Creating a KMS key group is the second task in the process of configuring the NetBackup Key Management Service manually.

See "Configuring key management for NetBackup AdvancedDisk storage encryption" on page 20.

A key group is a container for key records. Each storage server and volume combination requires a key group in the following format:

- UNIX storage: *storage_server_name*:*volume_name*
- Windows storage: *storage_server_name*:

To create a KMS key group

1 On the NetBackup primary server, create a key group by using the `nbkmsutil` command and the `-createkg` option. The format of the command depends on the operating system of the host or hosts to which the storage is attached, as follows:

Storage on UNIX:

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkg -kgname
storage_server_name:volume_name
```

Storage on Windows:

```
install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil -createkg
-kgname storage_server_name:
```

The following is the criteria for the key group name:

- For the *storage_server_name*, you must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server.

- The colon (:) is required after the *storage_server_name*.
- For the *volume_name* on UNIX host storage, specify the name of the last directory in the storage path. For example, use `backups` if the storage path is `/mnt/disk/backups`.
  Storage hosted on windows servers does not require a *volume_name*.

2 After you create the key groups, create a key record for each group.

See "Create a KMS key for NetBackup AdvancedDisk storage encryption" on page 24.

Create a KMS key for NetBackup AdvancedDisk storage encryption

Creating a KMS key is the third and the final task in the process of configuring the NetBackup Key Management Service manually.

See "Configuring key management for NetBackup AdvancedDisk storage encryption" on page 20.

Each key group requires at least one *key record*. The key record contains the encryption key itself and information about the key. The key is used to encrypt and decrypt data.

Note: If you create more than one key for a key group, only the last key remains active.

To create a KMS key

1. On the NetBackup primary server, create a key record by using the `nbkmsutil` command and the `-createkey` option.

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkey -keyname` *`keyname`* `-kgname` *`key_group_name`* `-activate`

   Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd\nbkmsutil -createkey -keyname` *`keyname`* `-kgname` *`key_group_name`* `-activate`

   Use the key group name that you configured when you created the key group.

   See "Create a KMS key group for NetBackup AdvancedDisk storage encryption" on page 23.

   You are prompted to enter a pass phrase:

   ```
   Enter a passphrase:
   ```

2. Enter and then re-enter a pass phrase; this pass phrase should differ from any pass phrases that you entered already.

3. Save a record of the pass phrase.

   See "Save a record of the KMS key names for NetBackup AdvancedDisk storage encryption" on page 25.

Save a record of the KMS key names for NetBackup AdvancedDisk storage encryption

Cohesity recommends that you save a record of the encryption key names and tags. The key tag is necessary if you need to recover or recreate the keys.

See "Configuring key management for NetBackup AdvancedDisk storage encryption" on page 20.

To save a record of the key names

1 To determine the key group names, use the following command on the primary server:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs`

Windows: *`install_path`*`\Program Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkgs`

The following is example output:

```
Key Group Name        : UX_Host.example.com:backups
Supported Cipher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Oct 01 01:00:00 2013
Last Modification Time: Tues Oct 01 01:00:00 2013
Description           : -
FIPS Approved Key     : Yes

Key Group Name        : Win_Host.example.com:
Supported Cipher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Oct 01 01:05:00 2013
Last Modification Time: Tues Oct 01 01:05:00 2013
Description           : -
FIPS Approved Key     : Yes
```

2 For each key group, write all of the keys that belong to the group to a file. Run the command on the primary server. The following is the command syntax:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname key_group_name > filename.txt`

Windows: `install_path\Program Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkeys -kgname key_group_name > filename.txt`

The following is example output:

```
nbkmsutil.exe -listkeys -kgname UX_Host.example.com:backups >
encrypt_keys_UX_Host.example.com_backups.txt

Key Group Name        : UX_Host.example.com:backups
Supported Cipher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Oct 01 01:00:00 2013
Last Modification Time: Tues Oct 01 01:00:00 2013
Description           : -
FIPS Approved Key     : Yes

  Key Tag               : 867d710aa7f4c64dcdd2cec6...cce
                          d0c831c1812c510acd05
  Key Name              : AdvDisk_Key
  Current State         : ACTIVE
  Creation Time         : Tues Oct 01 01:05:00 2013
  Last Modification Time: Tues Oct 01 01:05:00 2013
  Description           : -
  FIPS Approved Key    : Yes

Number of Keys: 1
```

3 Include in the file the pass phrase that you used to create the key record.

4 Store the file in a secure location.

Configure an AdvancedDisk storage server

Configure in this context means to configure as a storage server a NetBackup media server that can mount the storage.

See "About AdvancedDisk storage servers" on page 15.

How you configure an AdvancedDisk storage server depends on several factors, as follows:

Encrypted storage	If you want to encrypt the storage, you must use the NetBackup `nbdevconfig` command. For the **AdvancedDisk_crypt** type of storage server, you must specify the `-st` option with a value of **5**. See "About data encryption for AdvancedDisk storage" on page 18. See "To configure an AdvancedDisk storage server by using the command line" on page 29.
Storage server attributes	If you want to specify preferred or required attributes for the storage server, you must use the NetBackup `nbdevconfig` command. See "About AdvancedDisk preferred or required read servers" on page 16. See "To configure an AdvancedDisk storage server by using the command line" on page 29.
No encryption or attributes	Cohesity recommends that you use the storage server configuration wizard to configure the **AdvancedDisk** type of storage server. See "To configure an AdvancedDisk storage server by using the wizard" on page 29.

You can configure multiple storage servers for the same storage. Doing so provides load balancing and redundancy in case of a storage server failure. The following procedures explain how to configure multiple storage servers.

When you configure an AdvancedDisk storage server, it is also configured as a data mover.

See "About AdvancedDisk data movers" on page 15.

To configure an AdvancedDisk storage server by using the command line

1. Run the following command on the NetBackup primary server or the media server:

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server hostname -stype server_type -st 5 -media_server hostname [-setattribute attribute]`

   Windows: `install_path\NetBackup\bin\admincmd\nbdevconfig -creatests -storage_server hostname -stype server_type -st 5 -media_server hostname [-setattribute attribute]`

   The arguments for the command options are in a different topic. The arguments include those for encryption, for attributes, and so on.

   See "AdvancedDisk storage server configuration options" on page 30.

2. To verify that the storage server was configured correctly, run the following command:

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -u`

   Windows: `install_path\NetBackup\bin\admincmd\nbdevquery -liststs -u`

   The following is an excerpt of the command output that shows the proper storage type for AdvancedDisk (Formatted Disk, Direct Attached):

   ```
   Storage Server      : AdvDiskServer.example.com
   Storage Server Type : AdvancedDisk_crypt
   Storage Type        : Formatted Disk, Direct Attached
   State               : UP
   ```

3. After the storage server is created, you can do the following.

   - To configure another storage server, go to step 1 and then repeat the steps in this procedure.
   - If you have finished configuring storage servers, configure a disk pool.
     See "Configure an AdvancedDisk disk pool" on page 33.

To configure an AdvancedDisk storage server by using the wizard

1. On the left, select **Storage > Disk storage**. Select the **Storage servers** tab, then select **Add**.
2. In the **Storage type** list, select **Disk storage servers**.

   The types of storage servers that you can configure depend on the options for which you are licensed.

3. From the **Category** options, select **AdvancedDisk**.
4. Select **Start**.
5. Select a media server from the list and select **Select**.
6. Locate the success message at the top of the screen and select **Add disk pools**.

   Refer to the following topic for details on creating a disk pool and a storage unit:

   See "Configure an AdvancedDisk disk pool" on page 33.

   See "Configure an AdvancedDisk storage unit" on page 39.

AdvancedDisk storage server configuration options

The following are the `nbdevconfig` command options that are used to configure storage servers.

Table 3-7 Options to configure AdvancedDisk storage server

Option	Description
`-storage_server` *storage_server*	The name of the NetBackup media server that has a file system mount on the storage.
`-stype` *server_type*	For AdvancedDisk with encryption, use **AdvancedDisk_crypt**, otherwise use **AdvancedDisk**. **Note:** If you specify **AdvancedDisk_crypt** as the `-stype`, you must specify an **-st** value of **5** on the command line.
`-st` *storage_type*	A numeric value that specifies the storage server properties. For AdvancedDisk, the default value is 5 (direct attached, formatted disk). **Note:** For an **AdvancedDisk_crypt** `-stype`, you must specify **-st 5** on the command line.
`-media_server` *hostname*	Use the same name as the storage server name.

Table 3-7 Options to configure AdvancedDisk storage server *(continued)*

Option	Description
`-setattribute` *attribute*	An attribute to apply to the storage server for the read side of restore or duplication operations. The following are the attributes: ■ `PrefRestore`. The storage server is preferred for the read side of restore operations. More than one storage server can have the `PrefRestore` attribute. ■ `ReqRestore`. The storage server is required for the read side of restore operations. More than one storage server can have the ReqRestore attribute. ■ `ReqDuplicate`. The storage server is required for the read side of duplication operations. More than one storage server can have the `ReqDuplicate` attribute. See "About AdvancedDisk preferred or required read servers" on page 16.

About AdvancedDisk disk pools

A disk pool represents disk volumes on the underlying disk storage. NetBackup aggregates the disk volumes into pools of storage you can use for backups. A disk pool is the storage destination of a NetBackup storage unit.

Disk pools are either **AdvancedDisk** type or **AdvancedDisk_crypt** type.

See "About data encryption for AdvancedDisk storage" on page 18.

For the **AdvancedDisk_crypt** disk type on CIFS storage, you must configure the disk volumes before you configure the disk pool.

See "Configure a CIFS disk volume for AdvancedDisk encryption" on page 32.

See "Configure an AdvancedDisk disk pool" on page 33.

Cohesity recommends that disk pool and disk volume names be unique across your enterprise.

The following are disk pool and volume considerations for AdvancedDisk storage:

Capacity management	If an AdvancedDisk disk pool is a storage destination in a storage lifecycle policy, NetBackup capacity management applies. If you share the volumes in an AdvancedDisk disk pool with other users, NetBackup cannot manage disk pool capacity or storage lifecycle policies correctly.
Volume selection	NetBackup selects disk volumes based on available capacity and predicted size of the backup. NetBackup tries to write backup data to a single volume.

Disk spanning	If necessary, backup images span disk volumes in a disk pool. (Exception: NetBackup does not span volumes for the **AdvancedDisk_crypt** type of disk pool.) Backup images do not span across multiple disk pools. To reduce disk spanning, each volume in a disk pool should be larger than your largest backup. NetBackup then can store your largest backup on a single volume if that volume does not contain other backup images. **Note:** Some file systems limitations can affect whether or not NetBackup can detect file system capacity accurately. On those file systems, Cohesity recommends that you do not span backup images across volumes. See "About AdvancedDisk file system requirements" on page 13.
Disk size and performance	NetBackup assumes that all disk volumes within a disk pool are similar in size and performance characteristics. Although you can use dissimilar disk volumes in a disk pool, performance may be unpredictable. If you have the disk volumes that have significantly different characteristics, group them into multiple disk pools. Each of those disk pools should contain the volumes that have similar characteristics.
Disk contention	NetBackup queues backup and restore jobs if insufficient resources are available. To limit the possibility of write contention between backup jobs (and therefore job queuing), ensure that a disk pool contains a sufficient number of volumes. The number of volumes should be equal to or greater than: the total number of maximum concurrent jobs that are allowed in all of the storage units that use a disk pool.
Volume managers	The AdvancedDisk storage implementation presents mounted file systems as disk volumes to NetBackup. Therefore, you can use AdvancedDisk disk pools with the volume managers that work at a level closer to the hardware than the file system.

Configure a CIFS disk volume for AdvancedDisk encryption

AdvancedDisk_crypt and CIFS only.

For the **AdvancedDisk_crypt** disk type, you must use the NetBackup `nbdevconfig` command to specify each CIFS disk volume for the disk pool. You must also use the UNC notation to specify the volumes (NetBackup cannot discover Windows Common Internet File System (CIFS) disk volumes).

See "About AdvancedDisk file system requirements" on page 13.

Cohesity recommends that disk volume and disk pool names be unique across your enterprise.

You must first configure storage servers.

See "Configure an AdvancedDisk storage server" on page 27.

To configure an AdvancedDisk disk volume by using the command line

1. On the NetBackup primary server, configure the volume by using the following command:

   ```
   nbdevconfig -createdv -storage_server hostname -stype server_type
   -dv disk_volume_name -dp disk_pool_name
   ```

   The following is the path to the `nbdevconfig` command:

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

   The following describe the options:

`-storage_server` *hostname*	The name of the NetBackup media server that has a file system mount on the storage.
`-stype` *server_type*	For AdvancedDisk with encryption, use **AdvancedDisk_crypt**, otherwise use **AdvancedDisk**.
`-dv` *disk_volume_name*	The name of the disk volume; use UNC notation.
`-dp` *disk_pool_name*	The name of the disk pool for the volume.

2. Repeat step 1 for each disk volume that you want to add.

Configure an AdvancedDisk disk pool

How you configure an AdvancedDisk disk pool depends on the type, as follows:

AdvancedDisk_crypt type	You must use the `nbdevconfig` command if you configured an **AdvancedDisk_crypt** type of storage server. NetBackup encrypts the backup data on the **AdvancedDisk_crypt** type of disk pool. See "To configure an AdvancedDisk disk pool by using the `nbdevconfig` command" on page 35. NetBackup cannot discover Windows Common Internet File System (CIFS) disk volumes. For CIFS storage, you must use the UNC notation to specify the volumes. See "About AdvancedDisk file system requirements" on page 13. See "Configure a CIFS disk volume for AdvancedDisk encryption" on page 32.
AdvancedDisk type	Cohesity recommends that you use the disk pool configuration wizard to configure the **AdvancedDisk** type of disk pool. After you configure a storage server, the wizard prompts you to create a disk pool. Therefore, you may not need to invoke the disk pool wizard separately. See "To configure an AdvancedDisk disk pool by using the wizard" on page 34. NetBackup cannot discover Windows Common Internet File System (CIFS) disk volumes. For CIFS storage, you must use the UNC notation to specify the volumes. See "About AdvancedDisk file system requirements" on page 13.

Cohesity recommends that disk volume and disk pool names be unique across your enterprise.

You must first configure storage servers.

See "Configure an AdvancedDisk storage server" on page 27.

To configure an AdvancedDisk disk pool by using the wizard

1. On the left, select **Storage > Disk storage**.
2. Configure the following:
   - To select a storage server, select the **Change** button.
   - Enter the **Disk pool name** that you want to use.
   - Make any other configuration changes that you want for the disk pool. See "AdvancedDisk disk pool properties" on page 38.

   Click **Next**.

3 Select the volumes to use for the disk pool. NetBackup does not filter out common file system mount points, such as `/` and `/usr`. Therefore, carefully choose the volumes to include in a disk pool.

See "About AdvancedDisk file system requirements" on page 13.

4 On the **Review** page, verify the selections. To save the changes and add the disk pool, select **Finish**.

5 After the disk pool is created, configure an AdvancedDisk storage unit.

See "Configure an AdvancedDisk storage unit" on page 39.

To configure an AdvancedDisk disk pool by using the `nbdevconfig` command

1 On the host that has a file system mount on the storage, discover the volumes that are available and write them to a text file. If you intend to use multiple hosts to read to and write from the storage, use any of the hosts. The following is the NetBackup command to use, depending on your operating system:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_server` *`hostname`* `-stype` *`server_type`* `>` *`filename`*

Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevconfig -previewdv -storage_server` *`hostname`* `-stype` *`server_type`* `>` *`filename`*

The following describe the options:

`-storage_server` ***hostname***	The name of the NetBackup media server that has a file system mount on the storage.
`-stype` ***server_type***	For AdvancedDisk with encryption, use **AdvancedDisk_crypt**, otherwise use **AdvancedDisk**.
`>` *`filename`*	The name of the file into which to write the volume information. Cohesity recommends that you use a name that describes its purpose.

2 Copy the file that you created in step 1 to the primary server.

3 In a text editor, delete the line for each volume that you do not want to be in the disk pool. Do not delete the blank line at the end of the file.

Each volume that is listed in the file must be exposed to each AdvancedDisk storage server on the same mount point.

4 Configure the disk pool by using the following command, depending on your operating system:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp disk_pool_name -stype server_type -storage_servers hostname... -dvlist filename [-reason "string"] [-lwm low_watermark_percent] [-max_io_streams n] [-comment comment] [-M primary_server] [-reason "string"]`

Windows: `install_path\NetBackup\bin\admincmd\nbdevconfig -createdp -dp disk_pool_name -stype server_type -storage_servers hostname... -dvlist filename [-reason "string"] [-lwm low_watermark_percent] [-max_io_streams n] [-comment comment] [-M primary_server] [-reason "string"]`

The `nbdevconfig` command options are described in a different topic.

See "NetBackup nbdevconfig command options for AdvancedDisk disk pools" on page 36.

NetBackup nbdevconfig command options for AdvancedDisk disk pools

Table 3-8 shows the options that you can use when you use the `nbdevconfig` command to configure an AdvancedDisk disk pool

Table 3-8 nbdevconfig command options for AdvancedDisk disk pools

Option	Description
`-comment comment`	A comment that is associated with the disk pool.
`-dp disk_pool_name`	The name of the disk pool. Use the same name that you used when you configured the disk volumes.
`-dvlist filename`	The name of the file that contains the information about the volumes for the disk pool.

Table 3-8 nbdevconfig command options for AdvancedDisk disk pools *(continued)*

Option	Description
-hwm *high_watermark*	The *high_watermark* setting is a threshold that triggers the following actions: ■ When an individual volume in the disk pool reaches the *high_watermark*, NetBackup considers the volume full. NetBackup chooses a different volume in the disk pool to write backup images to. ■ When all volumes in the disk pool reach the *high_watermark*, the disk pool is considered full. NetBackup fails any backup jobs that are assigned to a storage unit in which the disk pool is full. NetBackup also does not assign new jobs to a storage unit in which the disk pool is full. ■ NetBackup begins image cleanup when a volume reaches the *high_watermark*; image cleanup expires the images that are no longer valid. For a disk pool that is full, NetBackup again assigns jobs to the storage unit when image cleanup reduces any disk volume's capacity to less than the *high_watermark*. If the storage unit for the disk pool is in a capacity-managed storage lifecycle policy, other factors affect image cleanup. The default is 98%.
-lwm *low_watermark*	The **Low water mark** is a threshold at which NetBackup stops image cleanup. The **Low water mark** setting cannot be greater than or equal to the **High water mark** setting. The default is 80%.
-M *primary_server*	The name of the primary server.
-max_io_streams *n*	Select this option to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit. When the limit is reached, NetBackup chooses another volume, if available. If not available, NetBackup queues jobs until a volume is available. Too many jobs that read and write data may degrade disk performance because of disk thrashing. (Disk thrashing is when the read and write heads move between the cylinders excessively as they seek the data for competing jobs.) Fewer streams may improve throughput, which may increase the number of jobs that complete in a specific time period. A starting point is to divide the **Maximum concurrent jobs** of all of the storage units by the number of volumes in the disk pool.
-reason "*string*"	The reason that you create the disk pool.

Table 3-8 nbdevconfig command options for AdvancedDisk disk pools *(continued)*

Option	Description
`-storage_servers` *hostname*	The name of each storage server that has a file system mount on the storage. Specify all NetBackup media servers that are storage servers for this disk pool.
`-stype` *server_type*	For AdvancedDisk with encryption, use **AdvancedDisk_crypt**, otherwise use **AdvancedDisk**.

AdvancedDisk disk pool properties

Table 3-9 describes the disk pool properties.

Table 3-9 AdvancedDisk disk pool properties

Property	Description
Storage server name	The storage server or storage servers. All NetBackup media servers that have a mount on the storage are listed. They share the storage for read and write purposes.
Disk pool name	The disk pool name.
Description	A description that is associated with the disk pool.
Limit I/O streams	Select this option to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit. When the limit is reached, NetBackup chooses another volume, if available. If not available, NetBackup queues jobs until a volume is available. Too many jobs that read and write data may degrade disk performance because of disk thrashing. (Disk thrashing is when the read and write heads move between the cylinders excessively as they seek the data for competing jobs.) Fewer streams may improve throughput, which may increase the number of jobs that complete in a specific time period. A starting point is to divide the **Maximum concurrent jobs** of all of the storage units by the number of volumes in the disk pool.

Table 3-9 AdvancedDisk disk pool properties *(continued)*

Property	Description
High water mark	The **High water mark** setting is a threshold that starts the following actions: ■ When an individual volume in the disk pool reaches the **High water mark**, NetBackup considers the volume full. NetBackup chooses a different volume in the disk pool to write backup images to. ■ When all volumes in the disk pool reach the **High water mark**, the disk pool is considered full. NetBackup fails any backup jobs that are assigned to a storage unit in which the disk pool is full. NetBackup also does not assign new jobs to a storage unit in which the disk pool is full. ■ NetBackup begins image cleanup when a volume reaches the **High water mark**; image cleanup expires the images that are no longer valid. For a disk pool that is full, NetBackup again assigns jobs to the storage unit when image cleanup reduces any disk volume's capacity to less than the **High water mark**. If the storage unit for the disk pool is in a capacity-managed storage lifecycle policy, other factors affect image cleanup. The default is 98%.
Low water mark	The **Low water mark** is a threshold at which NetBackup stops image cleanup. The **Low water mark** setting cannot be greater than or equal to the **High water mark** setting. The default is 80%.
Volumes	The disk volumes that comprise the disk pool.
Total size	The total amount of space available in the disk pool.
Total raw size	The total raw, unformatted size of the storage in the disk pool.
per volume	Select or enter the number of read and write streams to allow per volume. Many factors affect the optimal number of streams. Factors include but are not limited to disk speed, CPU speed, and the amount of memory.

Configure an AdvancedDisk storage unit

Create one or more storage units that reference the disk pool. To determine if storage units exist for the disk pool, go to **Storage > Storage units**.

See “About AdvancedDisk storage unit recommendations” on page 42.

More information about storage units is available. See the NetBackup Web UI Administrator's Guide.

To configure a storage unit for AdvancedDisk

1. On the left, select **Storage > Storage units**.
2. Select the **Storage units** tab, then select **Add**.
3. From the **Category** options, select **AdvancedDisk**.
4. Select **Start**.
5. Provide a name for the storage unit and configure any other settings. Then select **Next**.

   See "AdvancedDisk storage unit properties" on page 40.
6. Select the disk pool. Then select **Next**.
7. Select the media server. Then select **Next**.
8. On the **Review** page, verify the selections. To save the changes and add the storage unit, select **Save**.

AdvancedDisk storage unit properties

The following are the configuration options for a disk pool storage unit.

Table 3-10 AdvancedDisk storage unit properties

Property	Description
Storage unit name	Enter a unique name for the new storage unit. The name can describe the type of storage. The storage unit name is the name used to specify a storage unit for policies and schedules. The storage unit name cannot be changed after creation.
Storage unit type	Select **Disk** as the storage unit type.
Disk type	Select **AdvancedDisk** for the disk type.
Disk pool	Select the disk pool that contains the storage for this storage unit. All disk pools of the specified **Disk type** appear in the **Disk pool** list. If no disk pools are configured, no disk pools appear in the list.

Table 3-10 AdvancedDisk storage unit properties *(continued)*

Property	Description
Media server	Specify the NetBackup media servers that can move data to and from the disk pool for this storage unit. Only the media servers that are configured as storage servers appear in the media servers list. Specify the media server or servers as follows: ■ To allow any server in the media server list to access the disk storage (default), select **Use any available media server**. ■ To restrict the media servers that can access the disk storage, select **Only use the following media servers**. Then, select the media servers to allow. The selection list includes only the media servers that are configured as storage servers for the disk pool. NetBackup selects the media server to use when the policy runs.
Maximum concurrent jobs	Specify the maximum number of write jobs that NetBackup can send to a disk storage unit at one time. (Default: one job. The job count can range from 0 to 256.) This setting corresponds to the **Maximum concurrent write drives** setting for a tape storage unit. NetBackup queues jobs until the storage unit is available. If three backup jobs are scheduled and **Maximum concurrent jobs** is set to two, NetBackup starts the first two jobs and queues the third job. If a job contains multiple copies, each copy applies toward the **Maximum concurrent jobs** count. **Maximum concurrent jobs** controls the traffic for backup and duplication jobs but not restore jobs. The count applies to all servers in the storage unit, not per server. If you select multiple media servers in the storage unit and 1 for **Maximum concurrent jobs**, only one job runs at a time. The number to enter depends on the available disk space and the server's ability to run multiple backup processes. **Warning:** A Maximum concurrent jobs setting of 0 disables the storage unit.
Maximum fragment size	Specify the largest fragment size that NetBackup can create to store backups. The default maximum fragment size for a disk storage unit is 524,288 megabytes. To specify a maximum fragment size other than the default, enter a value from 20 megabytes to 524,288 megabytes. Backups to disk are usually fragmented to ensure that the backup does not exceed the maximum size that the file system allows. If an error occurs in a backup, the entire backup is discarded. The backup restarts from the beginning, not from the fragment where the error occurred. (An exception is for backups for which checkpoint and restart are enabled. In that case, fragments before and including the last checkpoint are retained; the fragments after the last checkpoint are discarded.)

About AdvancedDisk storage unit recommendations

You can use storage unit properties to control how NetBackup moves backup and duplication data.

For example, you can configure a favorable client-to-server ratio for important clients by using the storage unit **Media server** setting.

See "About AdvancedDisk storage unit recommendations" on page 42.

You also can use the storage unit **Maximum concurrent jobs** setting to control the backup or the duplication traffic that is sent to the media servers.

See "About throttling traffic to the media servers" on page 43.

About configuring a favorable client-to-server ratio

For a favorable client-to-server ratio, you can use one disk pool and configure multiple storage units to separate your backup traffic. Because all storage units use the same disk pool, you do not have to partition the storage.

For example, assume that you have 100 important clients, 500 regular clients, and four media servers. You can use two media servers to back up your most important clients and two media servers to back up your regular clients.

The following example describes how to configure a favorable client-to-server ratio:

- Configure the media servers for AdvancedDisk and configure the storage.
- Configure a disk pool.
- Configure a storage unit for your most important clients (such as STU-GOLD). Select the disk pool. Select **Only use the following media servers**. Select two media servers to use for your important backups.
- Create a backup policy for the 100 important clients and select the STU-GOLD storage unit. The media servers that are specified in the storage unit move the client data to the storage server.
- Configure another storage unit (such as STU-SILVER). Select the same disk pool. Select **Only use the following media servers**. Select the other two media servers.
- Configure a backup policy for the 500 regular clients and select the STU-SILVER storage unit. The media servers that are specified in the storage unit move the client data to the storage server.

Backup traffic is routed to the wanted data movers by the storage unit settings.

Note: NetBackup uses storage units for media server selection for write activity (backups and duplications) only. For restores, NetBackup chooses among all media servers that can access the disk pool.

About throttling traffic to the media servers

You can use the **Maximum concurrent jobs** settings on disk pool storage units to throttle the traffic to the media servers. Effectively, this setting also directs higher loads to specific media servers when you use multiple storage units for the same disk pool. A higher number of concurrent jobs means that the disk can be busier than if the number is lower.

For example, two storage units use the same set of media servers. One of the storage units (STU-GOLD) has a higher **Maximum concurrent jobs** setting than the other (STU-SILVER). More client backups occur for the storage unit with the higher **Maximum concurrent jobs** setting.

About storage lifecycle policies

A storage lifecycle policy (SLP) is a storage plan for a set of backups. An SLP is configured within the **Storage lifecycle policies** utility. It contains instructions in the form of storage operations, to be applied to the data that is backed up by a backup policy. Operations are added to the SLP that determine how the data is stored, copied, replicated, and retained. NetBackup retries the copies as necessary to ensure that all copies are created.

SLPs offer the opportunity for users to assign a classification to the data at the policy level. A data classification represents a set of backup requirements, which makes it easier to configure backups for data with different requirements. For example, email data and financial data.

SLPs can be set up to provide staged backup behavior. They simplify data management by applying a prescribed behavior to all the backup images that are included in the SLP. This process allows the NetBackup administrator to leverage the advantages of disk-based backups in the near term. It also preserves the advantages of tape-based backups for long-term storage.

The **SLP settings** host properties allow administrators to customize how SLPs are maintained and how SLP jobs run.

Best practice information about SLPs appears in the following document:

https://support.cohesity.com/s/article/article-100009913

Creating a storage lifecycle policy

A storage lifecycle policy (SLP) is a storage plan for a set of backups. The operations in an SLP are the backup instructions for the data. Use the following procedure to create an SLP that contains multiple storage operations.

To add a storage operation to a storage lifecycle policy

1. On the left, select **Storage > Storage lifecycle policies**.
2. Click **Add**.
3. Enter the Storage lifecycle policy name.

   See "Storage lifecycle policy settings" on page 44.
4. Add one or more operations to the SLP. The operations are the instructions for the SLP to follow and apply to the data that is specified in the backup policy.

   If this is the first operation added to the SLP, click **Add**.

   To add a child operation, select an operation and then click **Add child**.
5. Select an **Operation** type. If you're creating a child operation, the SLP displays only those operations that are valid based on the parent operation that you selected.
6. Configure the properties for the operation.
7. The **Window** tab displays for the following operation types: **Backup From Snapshot**, **Duplication**, **Import**, **Index From Snapshot**, and **Replication**. If you'd like to control when the secondary operation runs, create a window for the operation.
8. On the **Properties** tab, go to and expand **Advanced**. Choose if NetBackup should process active images after the window closes.
9. Select **Create** to create the operation.
10. Add additional operations to the SLP as needed. (See step 4.)
11. Change the hierarchy of the operations in the SLP if necessary.
12. Select **Create** to create the SLP. NetBackup validates the SLP when it is first created and whenever it is changed.
13. Configure a backup policy and select a storage lifecycle policy as the **Policy storage**.

Storage lifecycle policy settings

The following table describes the settings for storage lifecycle policies.

Figure 3-1 Storage lifecycle policy tab

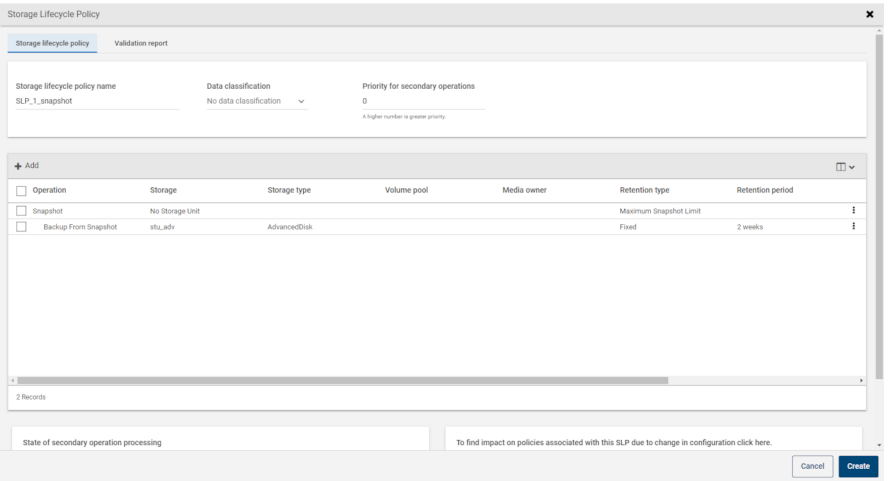


Table 3-11 Storage lifecycle policy tab

Setting	Description
Storage lifecycle policy name	The **Storage lifecycle policy name** describes the SLP. The name cannot be modified after the SLP is created.

Table 3-11 Storage lifecycle policy tab *(continued)*

Setting	Description
Data classification	The **Data classification** defines the level or classification of data that the SLP is allowed to process. The dropdown menu contains all of the defined classifications as well as the **Any** classification, which is unique to SLPs. The **Any** selection indicates to the SLP that it should preserve all images that are submitted, regardless of their data classification. This setting is available for SLP configuration only and is not available to configure a backup policy. The **Data classification** is an optional setting. One data classification can be assigned to each SLP and applies to all operations in the SLP. If a data classification is selected (other than **Any**), the SLP stores only those images from the policies that are set up for that data classification. If no data classification is indicated, the SLP accepts images of any classification or no classification. The **Data classification** setting allows the NetBackup administrator to classify data based on relative importance. A classification represents a set of backup requirements. When data must meet different backup requirements, consider assigning different classifications. For example, email backup data can be assigned to the silver data classification and financial data backup may be assigned to the platinum classification. A backup policy associates backup data with a data classification. Policy data can be stored only in an SLP with the same data classification. Once data is backed up in an SLP, the data is managed according to the SLP configuration. The SLP defines what happens to the data from the initial backup until the last copy of the image has expired.
Priority for secondary operations	The **Priority for secondary operations** option is the priority that jobs from secondary operations have in relationship to all other jobs. The priority applies to the jobs that result from all operations except for **Backup** and **Snapshot** operations. Range: 0 (default) to 99999 (highest priority). For example, you may want to set the **Priority for secondary operations** for a policy with a gold data classification higher than for a policy with a silver data classification. The priority of the backup job is set in the backup policy on the **Attributes** tab.
Operations	Use the **Add child**, **Edit**, and **Delete** options to create a list of operations in the SLP. An SLP must contain one or more operations. Multiple operations imply that multiple copies are created. The list also contains the columns that display information about each operation. Not all columns are displayed by default.
Move	Use the move option to change the hierarchy of the source for each copy. One copy can be the source for many other copies.

Table 3-11 Storage lifecycle policy tab *(continued)*

Setting	Description
State of Secondary Operation Processing	The **Active** and **Postponed** options refer to the processing of all duplication operations in the SLP. **Note:** These options apply to any duplication operations that create tar-formatted images. For example, those created with `bpduplicate`. These options do not affect the images that are duplicated as a result of OpenStorage optimized duplication or NDMP. Nor do they affect if one or more destination storage units are specified as part of a storage unit group. ■ Enable **Active** to let secondary operations continue as soon as possible. When an operation is changed from **Postponed** to **Active**, NetBackup continues to process the images, picking up where it left off when secondary operations were made inactive. ■ Enable **Postponed** to postpone the secondary operations for the entire SLP. **Postponed** does not postpone the creation of duplication jobs, it postpones the creation of images instead. The duplication jobs continue to be created, but they are not run until secondary operations are active again. All secondary operations in the SLP are inactive indefinitely unless the administrator selects **Active** or until the **Until** option is selected and an activation date is indicated.
Check for conflicts with backup policies option	Select this option to see how changes to this SLP can affect the policies that are associated with this SLP. The option generates a report that displays on the **Validation report** tab. This option performs the same validation as the `-conflict` option performs when used with the `nbstl` command.

Resilient network properties

To access this setting, in the web UI select **Hosts > Host properties**. Select the server or client. If necessary click **Connect**, then click **Edit primary server**, **Edit media server**, or **Edit client**. Click **Resilient network**.

For media servers and clients, the **Resilient network** properties are read only. When a job runs, the primary server updates the media server and the client with the current properties.

The **Resilient network** properties let you configure NetBackup to use resilient network connections for backups and restores. A resilient connection allows backup and restore traffic between a client and a NetBackup media server to function effectively in high-latency, low-bandwidth networks such as WANs. The data travels across a wide area network (WAN) to media servers in a central datacenter.

NetBackup monitors the socket connections between the remote client and the NetBackup media server. If possible, NetBackup re-establishes dropped connections and resynchronizes the data stream. NetBackup also overcomes latency issues to maintain an unbroken data stream. A resilient connection can survive network

interruptions of up to 80 seconds. A resilient connection may survive interruptions longer than 80 seconds.

The NetBackup Remote Network Transport Service manages the connection between the computers. The Remote Network Transport Service runs on the primary server, the client, and the media server that processes the backup or restore job. If the connection is interrupted or fails, the services attempt to re-establish a connection and synchronize the data.

NetBackup protects only the network socket connections that the NetBackup Remote Network Transport Service (`nbrntd`) creates. Examples of the connections that are not supported are:

- Clients that back up their own data (deduplication clients and SAN clients)
- Granular Recovery Technology (GRT) for Exchange Server or SharePoint Server
- NetBackup `nbfsd` process.

NetBackup protects connections only after they are established. If NetBackup cannot create a connection because of network problems, there is nothing to protect.

Resilient connections apply between clients and NetBackup media servers, which includes primary servers when they function as media servers. Resilient connections do not apply to primary servers or media servers if they function as clients and back up data to a media server.

Resilient connections can apply to all of the clients or to a subset of clients.

Note: If a client is in a subdomain that is different from the server subdomain, add the fully qualified domain name of the server to the client's hosts file. For example, `india.domain.org` is a different subdomain than `china.domain.org`.

When a backup or restore job for a client starts, NetBackup searches the **Resilient network** list from top to bottom looking for the client. If NetBackup finds the client, NetBackup updates the resilient network setting of the client and the media server that runs the job. NetBackup then uses a resilient connection.

Table 3-12 Resilient network properties

Property	Description
FQDN or IP address	The full qualified domain name or IP address of the host. The address can also be a range of IP addresses so you can configure more than one client at once. You can mix IPv4 addresses and ranges with IPv6 addresses and subnets. If you specify the host by name, it is recommended that you use the fully qualified domain name. Use the arrow buttons on the right side of the pane to move up or move down an item in the list of resilient networks.
Resiliency	**Resiliency** is either **On** or **Off**.

Note: The order is significant for the items in the list of resilient networks. If a client is in the list more than once, the first match determines its resilient connection status. For example, suppose you add a client and specify the client IP address and specify **On** for **Resiliency**. Suppose also that you add a range of IP addresses as **Off**, and the client IP address is within that range. If the client IP address appears before the address range, the client connection is resilient. Conversely, if the IP range appears first, the client connection is not resilient.

Other NetBackup properties control the order in which NetBackup uses network addresses.

The NetBackup resilient connections use the SOCKS protocol version 5.

Resilient connection traffic is not encrypted. It is recommended that you encrypt your backups. For deduplication backups, use the deduplication-based encryption. For other backups, use policy-based encryption.

Resilient connections apply to backup connections. Therefore, no additional network ports or firewall ports must be opened.

Note: If multiple backup streams run concurrently, the Remote Network Transport Service writes a large amount of information to the log files. In such a scenario, it is recommended that you set the logging level for the Remote Network Transport Service to 2 or less. Instructions to configure unified logs are in a different guide.

Specify resilient connections for clients

Use the following procedure to specify resilient connections for NetBackup clients.

See "Resilient network properties" on page 47.

Alternatively, you can use the `resilient_clients` script to specify resilient connections for clients:

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

To specify resilient connections for clients

1. Open the **NetBackup web UI**.
2. On the left, click **Hosts > Host properties**.
3. Select the primary server. If necessary, click **Connect**. Then click **Edit primary server**.
4. Click **Resilient network**.
5. You can perform the following actions:

Add a setting

To add a host or IP address setting

1. Click **Add**.
2. Enter a client host name or an IP address.

   If you specify the client host by name, it is recommended that you use the fully qualified domain name.
3. Ensure that the **On** option is selected.
4. Click **Add and add another**.
5. Repeat until you have added each setting.
6. When you finish adding network settings, click **Add**.

Edit a setting

To edit a host or IP address setting

1. Locate the client host name or the IP address.
2. Click **Actions > Edit**.
3. Select the desired **Resiliency** setting.
4. Click **Save**.

Delete a setting

Delete a host or IP address setting

1. Locate the client host name or the IP address.
2. Click **Actions > Delete**.

Up arrow, Down arrow	Change the order of items **1** Select the client host name or the IP address. **2** Click the **Up** or **Down** button. The order of the items in the list is significant. See "Resilient network properties" on page 47.

The settings are propagated to the affected hosts through normal NetBackup inter-host communication, which can take up to 15 minutes.

6 If you want to begin a backup immediately, restart the NetBackup services on the primary server.

Chapter 4

Managing AdvancedDisk

This chapter includes the following topics:

- Manage AdvancedDisk storage servers
- Manage AdvancedDisk disk pools
- About monitoring AdvancedDisk storage capacity and usage
- Monitor NetBackup disk activity
- View AdvancedDisk disk reports
- Display detailed AdvancedDisk storage usage information
- Display KMS key information for AdvancedDisk encryption

Manage AdvancedDisk storage servers

After you configure AdvancedDisk, you can perform various tasks to manage storage servers.

See "View AdvancedDisk storage servers" on page 52.

See "Determine the AdvancedDisk storage server state" on page 53.

See "View AdvancedDisk storage server attributes" on page 53.

See "Remove AdvancedDisk storage server attributes" on page 54.

See "Remove an AdvancedDisk storage server from disk pool access" on page 55.

See "Delete an AdvancedDisk storage server" on page 55.

View AdvancedDisk storage servers

You can view a list of storage servers that are already configured.

To view AdvancedDisk storage servers

- On the left, select **Storage > Disk storage**. Then select the **Storage servers** tab.

  This tab shows all configured storage servers. Use the sort feature to sort by Category or use the filter to select the AdvancedDisk type.

Determine the AdvancedDisk storage server state

Use the NetBackup `nbdevquery` command to determine the state of an AdvancedDisk storage server.

To determine AdvancedDisk storage server status

- Run the following command:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -stype AdvancedDisk -storage_server` *`server_name`* `-U`

  Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevquery -liststs -stype AdvancedDisk -storage_server` *`server_name`* `-U`

  The `State` field of the command output shows either UP or DOWN.

View AdvancedDisk storage server attributes

Use the NetBackup `nbdevquery` command to view the storage server attributes.

The following is the path to the `nbdevconfig` command:

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

To view AdvancedDisk storage server attributes

- Run the following command on the NetBackup primary server or a storage server:

  ```
  nbdevquery -liststs -storage_server storage_server -stype
  AdvancedDisk –U
  ```

  The following is example output:

  ```
  Storage Server      : advdsk_server.example.com
  Storage Server Type : AdvancedDisk
  Storage Type        : Formatted Disk, Direct Attached
  State               : UP
  Flag                : PrefRestore
  ```

  This example output is shortened; more flags may appear in actual output.

Remove AdvancedDisk storage server attributes

Use the `nbdevconfig` command to remove the following storage server attributes:

- Preferred restore server (`PrefRestore`)
- Required restore server (`ReqRestore`)
- Required duplication server (`ReqDuplicate`)

See "About AdvancedDisk preferred or required read servers" on page 16.

Attributes are added when you use the `nbdevconfig` command to configure a storage server.

See "Configure an AdvancedDisk storage server" on page 27.

The following is the path to the `nbdevconfig` command:

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

To remove AdvancedDisk storage server attributes

- Run the following command on the NetBackup primary server or on a storage server:

  ```
  nbdevconfig -changests -storage_server storage_server -stype
  AdvancedDisk -clearattribute attribute
  ```

Remove an AdvancedDisk storage server from disk pool access

Use the `nbdevconfig` command to remove a storage server so that it no longer can access a disk pool. If NetBackup jobs exist that use that storage server, you cannot remove the storage server.

Warning: If you remove the only storage server, data may be lost. NetBackup cannot access the disk pool and the backup images on the disk pool.

The following is the path to the `nbdevconfig` command:

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

To remove an AdvancedDisk storage server from disk pool access

1. For every storage unit that specifies the storage server (media server) in **Use one of the following media servers,** clear the check box that specifies the media server.

   This step is not required if the storage unit is configured to use any available media server.

2. If only one storage server exists, change the state of all disk pools on the array to DOWN. To do so, use the following command:

   ```
   nbdevconfig -changestate -stype AdvancedDisk -dp disk_pool_name
   -state DOWN
   ```

3. Remove the storage server. The following is the command syntax:

   ```
   nbdevconfig -changedp -stype AdvancedDisk -dp disk_pool_name
   -del_storage_servers storage_server
   ```

Delete an AdvancedDisk storage server

If you delete a storage server, NetBackup removes the storage server only from your configuration.

The media server is not deleted from your configuration. To delete the media server, use the NetBackup `nbemmcmd` command.

If a disk pool is configured from the disk volumes that the storage server manages, you cannot delete the storage server.

Warning: Do not delete a storage server if its storage contains unexpired NetBackup images. If you do, data loss may occur.

To delete an AdvancedDisk storage server

1. On the left, select **Storage > Disk storage**.
2. Select the **Storage servers** tab.
3. Locate and select the storage server. Then select **Actions > Delete**.

Manage AdvancedDisk disk pools

After you configure AdvancedDisk, you can perform various tasks to manage your AdvancedDisk disk pools.

See "View AdvancedDisk disk pools" on page 56.

See "About changing the AdvancedDisk disk pool size" on page 56.

See "Adding volumes to an AdvancedDisk disk pool" on page 57.

See "Change the AdvancedDisk disk pool properties" on page 57.

See "Enable active write-stream allocation in AdvancedDisk pool" on page 58.

See "Determine the AdvancedDisk disk pool state" on page 59.

See "Changing AdvancedDisk disk pool state" on page 59.

See "Determine the AdvancedDisk disk volume state" on page 59.

See "Change AdvancedDisk disk volume state" on page 60.

See "Merge AdvancedDisk disk pools" on page 61.

See "Remove a volume from an AdvancedDisk disk pool" on page 62.

See "Delete an AdvancedDisk disk pool" on page 62.

View AdvancedDisk disk pools

You can view the disk pools that are configured in NetBackup.

To view disk pools

1. On the left, select **Storage > Disk storage**.
2. Select the **Disk pools** tab.
3. Use the sort feature to sort by disk pool category or use the filter to select the AdvancedDisk type.

About changing the AdvancedDisk disk pool size

Two methods exist to change the size of a disk pool, as follows:

- If you use a logical volume manager, you can use it to change the size of a disk volume by adding LUNs to it.
- If you do not use a logical volume manager, you can change the size by adding or removing volumes from the disk pool.
  See "Adding volumes to an AdvancedDisk disk pool" on page 57.
  See "Remove a volume from an AdvancedDisk disk pool" on page 62.

Adding volumes to an AdvancedDisk disk pool

You can expand a disk pool's capacity by adding disk volumes to the disk pool. The names of the new volumes must differ from the names of the volumes in the current disk pool.

The NetBackup storage units that use the disk pool use the additional storage capacity automatically. You do not have to change the storage units.

(By default, NetBackup automatically increases disk pool capacity if the capacity of the underlying disk volumes increases. Similarly, NetBackup decreases the capacity of a disk pool if the underlying disk volume capacity decreases.)

Table 4-1 Add volumes process for an AdvancedDisk disk pool

Task	Procedure
Create a disk pool from the new disk volumes on the storage server.	See "Configure an AdvancedDisk disk pool" on page 33.
Merge the disk pools.	When you merge the disk pools, specify the original disk pool as the primary one. NetBackup deletes the secondary disk pool after the merge. See "Merge AdvancedDisk disk pools" on page 61.

Change the AdvancedDisk disk pool properties

You can change the storage server for a disk pool and change the properties of a disk pool.

To add volumes to a disk pool, you must use a different procedure.

See "Adding volumes to an AdvancedDisk disk pool" on page 57.

To change the disk pool properties

1. On the left, select **Storage > Disk storage**.
2. Select the **Disk pools** tab.

3. Select the link for the disk pool that you want to change.
4. Go to **Disk pools options** and select **Edit**.
5. Change the wanted properties.

   See "AdvancedDisk disk pool properties" on page 38.
6. Click **Save**.

Enable active write-stream allocation in AdvancedDisk pool

The active write-stream allocation feature in AdvancedDisk, intelligently manages the write streams for faster data writes.

By default, backup jobs allocate disks based on the largest available free space. As a result, NetBackup writes to the same disks, causing heavy I/O operations on those disks, while other volumes remain idle until they have the largest free space for the next job.

This feature improves the efficiency of AdvancedDisk pools that use multiple disk volumes in the following ways:

- When all volumes in the AdvancedDisk pool have the same number of active write streams, additional streams are allocated to the volumes with higher available storage-space.
- If the stream counts differ per volume, additional streams are allocated to the volumes with fewer active write-streams.

Here are some of the advantages of the Active write-stream allocation feature:

- Distributes backup jobs across multiple disks instead of concentrating I/O on a few disks.
- Reduces performance bottlenecks caused by writing to the same disks repeatedly.
- Utilizes all available disk volumes more effectively, preventing idle resources.

The active write-stream allocation feature is not enabled by default. You need to enable the feature for each AdvancedDisk pool using NetBackup CLI.

To enable the active write-stream feature:

1. Log on to the computer hosting the primary or media server with NetBackup admin privilege.
2. Run the following command in the NetBackup CLI:

```
nbdevconfig -changedp -stype AdvancedDisk -dp my_disk_pool
-setattribute ActiveWriteStream
```

To disable the active write-stream feature:

1. Log on to the computer hosting the primary or media server with NetBackup admin privilege.
2. Run the following command in the NetBackup CLI:

   ```
   nbdevconfig -changedp -stype AdvancedDisk -dp my_disk_pool
   -clearattribute ActiveWriteStream
   ```

Determine the AdvancedDisk disk pool state

The disk pool state is UP or DOWN.

To determine the AdvancedDisk disk pool state

1. On the left, select **Storage > Disk storage**.
2. Select the **Disk Pools** tab.
3. Locate the disk pool.

   The state is displayed in the **Status** column.

Changing AdvancedDisk disk pool state

You can change the state of a NetBackup disk pool. Pool states are UP or DOWN.

To change the state to DOWN, the disk pool must not be busy. If backup jobs are assigned to the disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

To change AdvancedDisk disk pool state

1. Open the NetBackup web UI.
2. On the left, select **Storage > Disk storage**. Then select the **Disk pools** tab.
3. Select the disk pool.
4. Select **Up disk pool** or **Down disk pool**.

Determine the AdvancedDisk disk volume state

Use the NetBackup `nbdevquery` command to determine the state of the volumes in AdvancedDisk disk pools.

To determine the AdvancedDisk disk volume state

- Display the state of the volumes in a disk pool by using the following command:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -U -stype` *`server_type`* `-dp` *`disk_pool_name`*

Windows: *install_path*\NetBackup\bin\admincmd\nbdevquery -listdv -U -stype *server_type* -dp *disk_pool_name*

The following items describe the arguments for the options:

-stype *server_type*	For the server type, use one of the following types: ■ **AdvancedDisk** for nonencrypted storage. ■ **AdvancedDisk_crypt** for encrypted storage.
dp *disk_pool_name*	The name of the disk pool. To display the disk volumes in all disk pools of the specified type, omit the -dp option.

The command displays all of the volumes in the disk pool. The *state* is either **UP** or **DOWN**.

Change AdvancedDisk disk volume state

Use the NetBackup nbdevconfig command to change disk volume state. The state is **UP** or **DOWN**.

To change the state to **DOWN**, the disk pool in which the volume resides must not be busy. If backup jobs are assigned to the disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

NetBackup jobs still read from and write to a disk pool that has a downed volume, but the downed volume is unavailable.

To change the AdvancedDisk disk volume state

1. Determine the name of the disk volume.

   See "Determine the AdvancedDisk disk volume state" on page 59.

2. Change the disk volume state. The following is the command syntax:

   UNIX: /usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate -stype *server_type* -dp *disk_pool_name* -dv *vol_name* -state *state*

   Windows: *install_path*\NetBackup\bin\admincmd\nbdevconfig -changestate -stype *server_type* -dp *disk_pool_name* -dv *vol_name* -state *state*

   The following items describe the arguments for the options:

`-stype` *server_type*	For the server type, use one of the following types: ■ **AdvancedDisk** for nonencrypted storage. ■ **AdvancedDisk_crypt** for encrypted storage.
`-dp` *disk_pool_name*	The name of the disk pool.
`-dv` *vol_name*	The name of the disk volume.
`-state` *state*	Specify **UP** or **DOWN**. **RESET** sets the internal state to **UP**, sets committed_space to zero, and sets the precommitted space to zero.

Merge AdvancedDisk disk pools

Use the NetBackup `nbdevconfig` command to merge existing disk pools.

NetBackup updates the catalog records to show the correct location of the backup images in those disk pools.

If the secondary disk pool is referenced by storage units, you must first delete those storage units.

The following is the path to the nbdevconfig command:

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

To merge AdvancedDisk disk pools

1. Change the state of each disk pool to DOWN.

   See "Changing AdvancedDisk disk pool state" on page 59.

   If backup jobs are assigned to a disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

2. Merge the disk pools. The following is the command syntax. The primary disk pool is the one you want to retain; `nbdevconfig` deletes the secondary disk pool after the merge.

   ```
   nbdevconfig -mergedps -stype AdvancedDisk -primarydp
   disk_pool_name -secondarydp disk_pool_name
   ```

3. Change the state of the primary disk pool to UP.

   See "Changing AdvancedDisk disk pool state" on page 59.

Remove a volume from an AdvancedDisk disk pool

Use the `nbdevconfig` command to remove a volume from a disk pool. The following are the prerequisites:

- NetBackup image fragments cannot exist on the disk volume.
- NetBackup jobs cannot be active on the disk volume.

By default, NetBackup automatically decreases disk pool capacity if you remove a disk volume.

The following is the path to the `nbdevconfig` command:

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

To remove a volume from an AdvancedDisk disk pool

1. Change the disk volume state to DOWN.

   See "Change AdvancedDisk disk volume state" on page 60.

2. Change the disk pool state to DOWN.

   See "Changing AdvancedDisk disk pool state" on page 59.

3. Remove the volume by using the `nbdevconfig` command. The following is the command syntax:

   ```
   nbdevconfig -deletedv -stype AdvancedDisk -dp disk_pool_name -dv
   vol_name
   ```

4. Change the disk pool state to UP.

   See "Changing AdvancedDisk disk pool state" on page 59.

Delete an AdvancedDisk disk pool

If you delete a disk pool, NetBackup removes it from your configuration.

If a disk pool is the storage destination of a storage unit, you must first delete the storage unit.

Warning: Do not delete a disk pool that contains unexpired NetBackup images; if you do, data loss may occur.

To delete an AdvancedDisk disk pool

1. On the left, select **Storage > Disk storage**.
2. Select the **Disk pools** tab.

3 Select a disk pool.

4 Select **Delete > Delete**.

About monitoring AdvancedDisk storage capacity and usage

Table 4-2 describes the ways that you can monitor storage capacity and usage.

Table 4-2 Monitor storage capacity and usage

What	Description
Disk pools tab	The details for a disk pool on the **Disk pools** tab display the information that was stored when NetBackup polled the disk pools. NetBackup polls every 5 minutes; therefore, the value may not be as current as the value that is displayed on the **Storage servers** tab. To display the tab, select **Storage > Disk storage**.
Storage servers tab	The storage server view displays real-time values. To display the tab, select **Storage > Disk storage**.
The `nbdevquery` command	See "Display detailed AdvancedDisk storage usage information" on page 65.

Monitor NetBackup disk activity

You can monitor NetBackup disk-related activity and status by viewing the NetBackup log files.

Some NetBackup commands or processes write messages to their own log files. Other processes use Veritas Unified Logging (VxUL) log files. VxUL uses a standardized name and file format for log files. An originator ID (OID) identifies the process that writes the log messages.

Table 4-3 shows the NetBackup logs for disk-related activity.

The messages that begin with a `sts_` prefix relate to the interaction with the storage vendor software plug-in. Most interaction occurs on the NetBackup media servers.

Table 4-3 NetBackup logs

Activity	VxUL OID	Processes that use the ID
Backups and restores	N/A	Messages appear in the log files for the following processes: ■ The `bpbrm` backup and restore manager ■ The `bpdbm` database manager ■ The `bpdm` disk manager ■ The `bptm` tape manager for I/O operations
Backups and restores	117	The `nbjm` job manager.
Device configuration	111	The `nbemm` process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration	202	The Storage Server Interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

To view and manage VxUL log files, you must use NetBackup log commands. Information about how to use and manage logs on NetBackup servers is available.

See the *NetBackup Logging Reference Guide*:

https://support.cohesity.com/s/article/article-100040135

View AdvancedDisk disk reports

The NetBackup disk reports include information about the disk pools, disk storage units, disk logs, images that are stored on disk media, and storage capacity.

In the NetBackup web UI, navigate to **Detection and reporting > Reporting** to generate reports. From the **Report type** drop-down list, select the type of report you want to generate.

Table 4-4 describes the disk reports available.

Table 4-4 Disk reports

Report	Description
Images on Disk	From the **Report type** drop-down list, select **Images on media**, and then set **Media type** to **Disk**. The Images on Disk report generates the image list present on the disk storage units that are connected to the media server. The report is a subset of the Images on Media report; it shows only disk-specific columns. The report provides a summary of the storage unit contents. If a disk becomes bad or if a media server crashes, this report can let you know what data is lost.
Disk logs	From the **Report type** drop-down list, select **Media logs**, and then set **Media type** to **Disk logs**. The Disk logs report displays the media errors or the informational messages that are recorded in the NetBackup error catalog. The report is a subset of the Media Logs report; it shows only disk-specific columns.
Disk Pool Status	Navigate to **Storage > Disk Storage > Disk Pools**. All disk pools are displayed. The Status column shows the current status of each disk pool. For disk pool capacity, see the **Disk pools** tab in **Storage > Disk storage**.

Display detailed AdvancedDisk storage usage information

The NetBackup `nbdevquery` command lets you display detailed information about the storage use of disk pools and disk volumes.

To determine the disk volume storage usage

1. Determine the names of all AdvancedDisk disk pools in your NetBackup domain:

   ```
   nbdevquery -listdp -stype AdvancedDisk

   V7.5 DiskPool-AdvDisk 1 201.00 201.00 3 98 80 -1 adv_server.example.com
   ```

   The version is the I/O format not the NetBackup release level. The version may differ on your system.

2. Determine disk volume names in the AdvancedDisk disk pool:

   ```
   nbdevquery -listdv -stype AdvancedDisk -dp disk_pool_name
   ```

   Replace *disk_pool_name* with the name of the disk pool for which you want to determine the volume names.

   The following is example output:

   ```
   V7.5 DiskPool-AdvDisk AdvancedDisk /advdisk_disc1 @aaaak 0.00 0.00 100 1
   V7.5 DiskPool-AdvDisk AdvancedDisk /advdisk_disc2 @aaaal 200.00 79.75 60
   V7.5 DiskPool-AdvDisk AdvancedDisk /advdisk_disc3 @aaaam 1.00 1.00 0 1 0
   ```

3. Display the usage information for a specific AdvancedDisk disk volume:

   ```
   nbdevquery -listdv -stype AdvancedDisk -dp disk_pool_name -dv
   disk_volume_name -D
   ```

   Replace *disk_pool_name* with the name of the disk pool for which you want to determine the volume names. Replace *disk_volume_name* with the name of the disk volume for which you want to display usage information.

   The output from the command includes the following fields:

   ```
   total_capacity      : 214748364800
   total_phys_capacity : 214748364800
   free_space          : 85625798656
   free_phys_space     : 85625798656
   potential_free_space: 0
   committed_space     : 0
   precommitted_space  : 0
   ```

   See “NetBackup disk volume capacity and usage reference” on page 66.

NetBackup disk volume capacity and usage reference

NetBackup determines the space available for backups on a volume by using the following formula:

Available space equals `free_space` plus `potential_free_space` minus `committed_space`.

The `potential_free_space` value is used only for a disk volume that is capacity managed. A disk volume is capacity managed when its disk pool is capacity managed. A disk pool is capacity managed when it is a destination in a storage lifecycle policy and the **Retention Type** is **Capacity managed**.

Table 4-5 describes the capacity values that NetBackup uses for space calculations.

Table 4-5 Disk capacity values

Field	Description
`total_capacity`	The total size of the disk. This value is derived from the file system and is updated at 1-minute intervals.
`total_phys_capacity`	For the purposes of AdvancedDisk, `total_capacity` and `total_phys_capacity` should have the same values.
`free_space`	The amount of free space on the disk. This value is derived from the file system and is updated at 1-minute intervals.
`free_phys_space`	For the purposes of AdvancedDisk, `free_space` and `free_phys_space` should have the same values.
`potential_free_space`	The sum of all of the fragments on the disk that NetBackup duplicated as part of a storage lifecycle policy and that are eligible for expiration. A fragment becomes eligible for expiration when it has been duplicated successfully. NetBackup calculates `potential_free_space` a the end of duplication sessions and expiration sessions. The `potential_free_space` value may become stale between computations. However, the next computation provides an accurate value.

Table 4-5 Disk capacity values *(continued)*

Field	Description
`committed_space`	The estimated size of all of the jobs-in-progress that write to the volume, based on the following: ■ For an existing backup, NetBackup uses the size of the most recent backup plus 20%. ■ For a new backup (including user backups), NetBackup uses the capacity of the disk volume over the high-water mark. For example, on a 2-TB volume that has a 98% high-water mark, NetBackup uses 40 GBs. ■ For duplication jobs, NetBackup uses the size of the source image.
`precommitted_space`	The `precommitted_space` is a helper value for `committed_space`. NetBackup decrements the value while a backup job runs. Each time NetBackup updates the capacity and free space information, NetBackup updates the value of `committed_space` to the current value of `precommitted_space`. This process ensures that all capacity-related values are updated at the same time to provide the most accurate usage description for the disk volume.

Display KMS key information for AdvancedDisk encryption

You can use the `nbkmsutil` command to list the following information about the key groups and the key records:

Key groups — See To display KMS key group information.

Keys — See To display KMS key information.

Note: Cohesity recommends that you keep a record key information. The key tag that is listed in the output is necessary if you need to recover keys.

To display KMS key group information

- To list all of the key groups, use the `nbkmsutil` with the `-listkgs` option. The following is the command format:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs`

  Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd\nbkmsutil -listkgs`

  The following is example output on UNIX hosted storage. On Windows, the volume name is not used.

```
Key Group Name        : AdvDiskServer1.example.com:AdvDisk_Volume
Supported Cipher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description           : -
```

To display KMS key information

- To list all of the keys that belong to a key group name, use the `nbkmsutil` with the `-listkgs` and `-kgname` options. The following is the command format:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:AdvDisk_Volume`

  Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd\nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:`

  The following is example output on UNIX hosted storage. On Windows, the volume name is not used.

```
Key Group Name        : AdvDiskServer1.example.com:AdvDisk_Volume
Supported Cipher      : AES_256
Number of Keys        : 1
Has Active Key        : Yes
Creation Time         : Wed Nov 30 16:53:48 2011
Last Modification Time: Wed Nov 30 16:53:48 2011
Description           : -

  Key Tag    : 867d710aa7f4c64dcdd2cec6...cced0c831c1812c510acd05
  Key Name              : dp-key
  Current State         : ACTIVE
  Creation Time         : Tues Jan 01 01:00:00 2013
  Last Modification Time: Tues Jan 01 01:00:00 2013
  Description           : -

Number of Keys: 1
```

Chapter 5

Troubleshooting AdvancedDisk

This chapter includes the following topics:

- About unified logging
- About legacy logging
- NetBackup AdvancedDisk log files
- AdvancedDisk troubleshooting
- Resolve an incorrect storage type problem

About unified logging

Unified logging creates log file names and messages in a format that is standardized across Cohesity products. Only the `vxlogview` command can assemble and display the log information correctly. Server processes and client processes use unified logging.

Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

Windows	*install_path*\NetBackup\logs
UNIX	/usr/openv/logs

Note: Only the following types of users can access the logs: root and service users in Linux systems, and users present in the administrators group of Windows systems.

You can access logging controls in **Logging** host properties. You can also manage unified logging with the following commands:

`vxlogcfg`	Modifies the unified logging configuration settings.
`vxlogmgr`	Manages the log files that the products that support unified logging generate.
`vxlogview`	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 74.

About using the `vxlogview` command to view unified logs

Only the `vxlogview` command can assemble and display the unified logging information correctly. The unified logging files are in binary format and some of the information is contained in an associated resource file. These logs are stored in the following directory. You can display `vxlogview` results faster by restricting the search to the files of a specific process.

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\NetBackup\logs`

Table 5-1 Fields in `vxlogview` query strings

Field name	Type	Description	Example
`PRODID`	Integer or string	Provide the product ID or the abbreviated name of product.	`PRODID = 51216` `PRODID = 'NBU'`
`ORGID`	Integer or string	Provide the originator ID or the abbreviated name of the component.	`ORGID = 116` `ORGID = 'nbpem'`
`PID`	Long Integer	Provide the process ID	`PID = 1234567`
`TID`	Long Integer	Provide the thread ID	`TID = 2874950`
`STDATE`	Long Integer or string	Provide the start date in seconds or in the locale-specific short date and time format. For example, a locale can have the format 'mm/dd/yy hh:mm:ss AM/PM'	`STDATE = 98736352` `STDATE = '4/26/11 11:01:00 AM'`

Table 5-1 Fields in `vxlogview` query strings *(continued)*

Field name	Type	Description	Example
`ENDATE`	Long Integer or string	Provide the end date in seconds or in the locale-specific short date and time format. For example, a locale can have the format 'mm/dd/yy hh:mm:ss AM/PM'	`ENDATE = 99736352` `ENDATE = '04/27/11 10:01:00 AM'`
`PREVTIME`	String	Provide the hours in 'hh:mm:ss' format. This field should be used only with operators `=`, `<`, `>`, `>=`, and `<=`	`PREVTIME = '2:34:00'`
`SEV`	Integer	Provide one of the following possible severity types: 0 = `INFO` 1 = `WARNING` 2 = `ERR` 3 = `CRIT` 4 = `EMERG`	`SEV = 0` `SEV = INFO`
`MSGTYPE`	Integer	Provide one of the following possible message types: 0 = `DEBUG` (debug messages) 1 = `DIAG` (diagnostic messages) 2 = `APP` (application messages) 3 = `CTX` (context messages) 4 = `AUDIT` (audit messages)	`MSGTYPE = 1` `MSGTYPE = DIAG`
`CTX`	Integer or string	Provide the context token as string identifier or `'ALL'` to get all the context instances to be displayed. This field should be used only with the operators `=` and `!=`.	`CTX = 78` `CTX = 'ALL'`

Table 5-2 Examples of query strings with dates

Example	Description
`(PRODID == 51216) && ((PID == 178964)|| ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM'))`	Retrieves the log file message for the NetBackup product ID 51216 between 9AM and 12PM on 2015-05-02.
`((prodid = 'NBU') && ((stdate >= '11/18/14 00:00:00 AM') && (endate <= '12/13/14 12:00:00 PM'))) || ((prodid = 'BENT') && ((stdate >= '12/12/14 00:00:00 AM') && (endate <= '12/25/14 12:00:00 PM')))`	Retrieves the log messages for the NetBackup product NBU between 2014-18-11 and 2014-13-12 and the log messages for the NetBackup product BENT between 2014-12-12 and 2014-25-12.
`(STDATE <= '04/05/15 0:0:0 AM')`	Retrieves the log messages that were logged on or before 2015-05-04 for all of the installed Cohesity products.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Note: Only the following types of users can access the logs: root and service users in Linux systems, and users present in the administrators group of Windows systems.

Table 5-3 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`

Table 5-3 Example uses of the vxlogview command *(continued)*

Item	Example
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"`
Display results faster	You can use the `-i` option to specify an originator for a process: `# vxlogview -i nbpem` The `vxlogview -i` option searches only the log files that the specified process (`nbpem`) creates. By limiting the log files that it has to search, `vxlogview` returns a result faster. By comparison, the `vxlogview -o` option searches all unified log files for the messages that the specified process has logged. **Note:** If you use the `-i` option with a process that is not a service, `vxlogview` returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the `-o` option instead of the `-i` option. The -i option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).
Search for a job ID	You can search the logs for a particular job ID: `# vxlogview -i nbpem | grep "jobid=`*`job_ID`*`"` The `jobid=` search key should contain no spaces and must be lowercase. When searching for a job ID, you can use any `vxlogview` command option. This example uses the `-i` option with the name of the process (`nbpem`). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the jobid=*job_ID*.

About legacy logging

In NetBackup legacy debug logging, a process creates log files of debug activity in its own logging directory. By default, NetBackup creates only a subset of logging directories, in the following locations:

Windows
install_path\NetBackup\logs
install_path\Volmgr\debug

UNIX
/usr/openv/netbackup/logs
/usr/openv/volmgr/debug

To use legacy logging, a log file directory must exist for a process. If the directory is not created by default, you can use the `mklogdir` utility to create the directories. Or, you can manually create the directories. When logging is enabled for a process, a log file is created when the process begins. Each log file grows to a certain size before the NetBackup process closes it and creates a new log file.

Note: To apply the appropriate permissions on the legacy log directories, always use the `mklogdir` utility present in Windows and Linux to create the legacy log directories for each platform.

You can use the following utility to create all of the log directories:

- Windows: *install_path*`\NetBackup\Logs\mklogdir.bat`
- UNIX: `/usr/openv/netbackup/logs/mklogdir`

Follow these recommendations when you create and use legacy log folders:

- Do not use symbolic links or hard links inside legacy log folders.
- Sometimes if a process runs for a non-root or non-admin user, no logging that occurs in the legacy log folders. In that case use the `mklogdir` command to create a folder for the required user.
- To run a command line for a non-root or non-admin user (troubleshooting when the NetBackup services are not running), create user folders for the specific command line. Create the folders either with the `mklogdir` command or manually with the non-root or non-admin user privileges.

Creating NetBackup log file directories for AdvancedDisk

Before you configure your NetBackup feature, create the directories into which the NetBackup commands write log files. Create the directories on the primary server and on each media server that you use for your feature. The log files reside in the following directories:

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

More information about NetBackup logging is available in the *NetBackup Logging Reference Guide*, available through the following URL:

https://support.cohesity.com/s/article/article-100040135

To create log directories for NetBackup commands

- Depending on the operating system, run one of the following scripts:

  UNIX: `/usr/openv/netbackup/logs/mklogdir`

  Windows: *`install_path`*`\NetBackup\logs\mklogdir.bat`

To create the `tpconfig` command log directory

- Depending on the operating system, create the `debug` directory and the `tpcommand` directory (by default, the `debug` directory and the `tpcommand` directory do not exist). The pathnames of the directories are as follows:

  UNIX: `/usr/openv/volmgr/debug/tpcommand`

  Windows: *`install_path`*`\Veritas\Volmgr\debug\tpcommand`

NetBackup AdvancedDisk log files

You can monitor NetBackup AdvancedDisk activity and status by viewing the NetBackup log files.

Some NetBackup commands or processes write messages to their own log files. For those commands and processes, the log directories must exist so that the utility can write log messages.

See "Creating NetBackup log file directories for AdvancedDisk" on page 76.

Other processes use Veritas Unified Logging (VxUL) files. Each process has a corresponding VxUL originator ID. VxUL uses a standardized name and file format for log files. To view VxUL log files, you must use the NetBackup `vxlogview` command.

More information about how to view and manage VxUL log files is available. See the *NetBackup Logging Reference Guide*:

https://support.cohesity.com/s/article/article-100040135

The following are the component identifiers for log messages:

- An `sts_` prefix relates to the interaction with the plug-in that writes to and reads from the storage.
- An `encrypt` prefix relates to interaction with the encryption plug-in.
- A `KMSCLIB` prefix relates to interaction with the NetBackup Key Management Service.

Most interaction occurs on the NetBackup media servers. Therefore, the log files on the media servers that you use for disk operations are of most interest.

Warning: The higher the log level, the greater the affect on NetBackup performance. Use a log level of 5 (the highest) only when directed to do so by a Cohesity representative. A log level of 5 is for troubleshooting only.

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup primary server. The log levels for some processes specific to certain options are set in configuration files as described in Table 5-4.

Table 5-4 describes the logs.

Table 5-4 NetBackup logs

Activity	OID	Processes
Backups and restores	N/A	Messages appear in the log files for the following processes: ■ The `bpbrm` backup and restore manager. ■ The `bpdbm` database manager. ■ The `bpdm` disk manager. ■ The `bptm` tape manager for I/O operations. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/` ■ Windows: *`install_path`*`\NetBackup\logs\`
Backups and restores	117	The `nbjm` Job Manager.
Image cleanup, verification, import, and duplication	N/A	The `bpdbm` database manager log files. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/bpdbm` ■ Windows: *`install_path`*`\NetBackup\logs\bpdbm`
Device configuration	111	The `nbemm` process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration	202	The Storage Server Interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

AdvancedDisk troubleshooting

The following may help you troubleshoot AdvancedDisk:

Table 5-5 AdvancedDisk troubleshooting

Problem	Solution
Unable to access storage	If NetBackup cannot access the storage, one possible cause is that the storage server was created with the incorrect `nbdevconfig` storage type (`-st`) value. An AdvancedDisk storage server `-st` value is 5 (formatted disk, directly attached); values other than 5 are incorrect. More procedural information is available about resolving this problem. See "Resolve an incorrect storage type problem" on page 79.
Multiple storage servers on Windows	AdvancedDisk does not support Common Internet File System (CIFS). If you try to configure multiple storage servers, NetBackup returns the following message: `DSM does not support to use multiple Windows Storage Servers for server type: AdvancedDisk.`
Volume state changes to DOWN when volume is unmounted	If a volume becomes unmounted, NetBackup changes the volume state to DOWN. NetBackup jobs that require that volume fail. To change the volume state to UP, mount the file system
Disk failure - AdvancedDisk	If recovery mechanisms do not protect a disk that fails, the backup images on that disk are lost. Operating system read and write errors may occur for the volume that represents the disk. NetBackup cannot use that volume because of the errors, and NetBackup jobs may fail. To prevent NetBackup from trying to read from or write to the disk, you must change the volume state to DOWN in NetBackup. If the volume represents other disks that still function, those disks are not available because the volume state is DOWN. You may be able to read from the volume by mounting it manually. If so, you may be able to recover image fragments from any disks that did not fail. If you replace a failed disk, you can use the same mount point for the replacement disk. Change the volume state to UP, and NetBackup uses that volume again. Any valid backup images on that volume are available for restores.

Resolve an incorrect storage type problem

First determine the storage server value to verify that the storage server was created with the incorrect `nbdevconfig` storage type value. Then proceed to resolving the problem if necessary.

To determine the storage server value

- Invoke the following command on the primary server or a media server that functions as a storage server:

  The following output shows an incorrect value for AdvancedDisk:

```
Storage Server      : halo
Storage Server Type : AdvancedDisk
Storage Type        : Formatted Disk, Network Attached
```

To resolve an incorrect storage type problem

1. Delete all disk pools that use the storage server.
2. Delete the storage server.
3. Reconfigure the storage server.
4. Recreate the disk pools.
5. If necessary, specify the new disk pools in the storage units.

   If you recreated the disk pools with the same names as the ones you deleted, this step is not necessary.

See "AdvancedDisk troubleshooting" on page 79.