Symantec NetBackup™ AdvancedDisk Storage Solutions Guide

UNIX, Windows, Linux

Release 7.6

✓ Symantec™

Symantec NetBackup™ AdvancedDisk Storage Solutions Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.6

Legal Notice

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

- Available memory, disk space, and NIC information

- Operating system

- Version and patch level

- Network topology

- Router, gateway, and IP address information

- Problem description:

  - Error messages and log files

  - Troubleshooting that was performed before contacting Symantec

  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

- Questions regarding product licensing or serialization

- Product registration updates, such as address or name changes

- General product information (features, language availability, local dealers)

- Latest information about product updates and upgrades

- Information about upgrade assurance and support contracts

- Information about the Symantec Buying Programs

- Advice about Symantec's technical support options

- Nontechnical presales questions

- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

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

Contents

Chapter 4	Managing AdvancedDisk 69

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
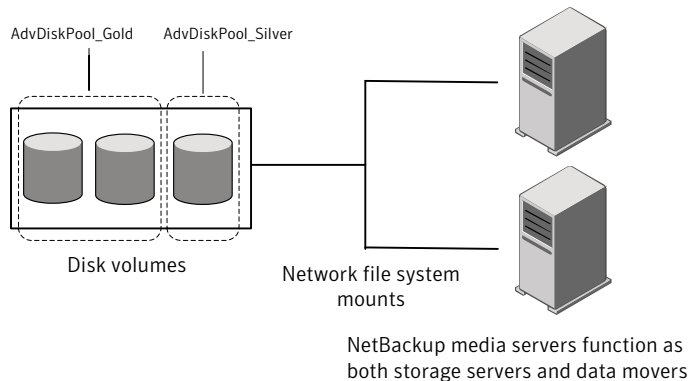
AdvDiskPool_Gold   AdvDiskPool_Silver

Disk volumes   Network file system mounts

NetBackup media servers function as both storage servers and data movers

Licensing AdvancedDisk

This chapter includes the following topics:

- About the AdvancedDisk license key

- Licensing AdvancedDisk

About the AdvancedDisk license key

AdvancedDisk is a feature that is licensed separately from base NetBackup. The Data Protection Optimization Option license key activates AdvancedDisk.

You may have a single license key that activates both NetBackup and the Data Protection Optimization Option. Alternatively, you may have one license key that activates NetBackup and another key that activates the Data Protection Optimization Option.

See "Licensing AdvancedDisk" on page 13.

If you remove the Data Protection Optimization Option 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 key.

Licensing AdvancedDisk

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

Enter the license key on the NetBackup master server. The following procedure describes how to use the **NetBackup Administration Console** to enter the license key.

To license AdvancedDisk

1   To add a license to a specific server, select **File** > **Change Server** and then select the server.

2   In the **NetBackup License Keys** dialog box, click **New**.

3   In the **Add a New License Key** dialog box, enter the license key and click **Add** or **OK**.

4   Click **Close**.

5   Restart all the NetBackup services and daemons.

Configuring AdvancedDisk

This chapter includes the following topics:

- Configuring the AdvancedDisk option

- About AdvancedDisk file system requirements

- Configuring 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

- Configuring an AdvancedDisk storage server

- About AdvancedDisk disk pools

- Configuring a CIFS disk volume for AdvancedDisk encryption

- Configuring an AdvancedDisk disk pool

- Configuring an AdvancedDisk storage unit

- About storage lifecycle policies

- Creating a storage lifecycle policy

- Creating a backup policy

- Resilient Network properties

■ Specifying resilient connections

Configuring the AdvancedDisk option

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

Table 3-1 describes the configuration tasks.

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

Table 3-1   AdvancedDisk configuration tasks

Step	Task	Section
Step 1	Learn about file system requirements	See "About AdvancedDisk file system requirements" on page 16.
Step 2	Learn about storage servers and data movers	See "About AdvancedDisk storage servers" on page 18. See "About AdvancedDisk data movers" on page 19.
Step 3	Optionally, configure the Key Management Service	The Key Management Service is required if you use data encryption for the AdvancedDisk storage. See "About data encryption for AdvancedDisk storage" on page 21.
Step 4	Configure a storage server	See "Configuring an AdvancedDisk storage server" on page 30.
Step 5	Learn about disk pools	See "About AdvancedDisk disk pools" on page 37.
Step 6	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 "Configuring a CIFS disk volume for AdvancedDisk encryption" on page 38.
Step 7	Configure a disk pool	See "Configuring an AdvancedDisk disk pool" on page 39.
Step 8	Configure a storage unit	See "Configuring an AdvancedDisk storage unit" on page 52.

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

Step	Task	Section
Step 9	Create a storage lifecycle policy	See "About storage lifecycle policies" on page 56. See "Creating a storage lifecycle policy" on page 57.
Step 10	Create a backup policy	See "Creating a backup policy" on page 62.
Step 11	Optionally, configure resilient network connections	See "Resilient Network properties" on page 63.

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 at the Symantec support Web site, as follows:

http://entsupport.symantec.com/

The following are additional requirements and limitations for file systems:

CIFS	Windows Common Internet File System (CIFS) requirements:

- Networked mapped devices are not visible to Windows services; therefore, NetBackup cannot discover CIFS disk volumes. You must use the UNC naming convention 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 "Configuring credentials for CIFS storage and disk storage units" on page 17.
- In the **Disk Pool Configuration Wizard**, you must use the Windows Universal Naming Convention to specify the CIFS volumes that you want to use for AdvancedDisk disk pools. (Networked mapped devices are not visible to Windows services; therefore, NetBackup cannot discover CIFS disk volumes.)
- 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.

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.
- Symantec 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   Symantec 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.

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

See "Configuring an AdvancedDisk disk pool" on page 39.

Configuring credentials for CIFS storage and disk storage units

For Common Internet File System (CIFS) storage with AdvancedDisk, two NetBackup services on Windows computers require matching credentials.

The following NetBackup services on Windows media servers to which the CIFS storage is attached must use the same credentials:

- NetBackup Client Service
  The NetBackup Client Service is either `bpcd.exe` or `bpinetd.exe`, depending on NetBackup release level. Regardless of the binary file name, the service requires the credentials.

- NetBackup Remote Manager and Monitor Service
  The NetBackup Remote Manager and Monitor Service binary file name is `nbrmms.exe`.

The credentials must be valid Windows credentials that allow read and write access to the storage. Configure the credentials on the media server or media servers that have a file system mount on the CIFS storage.

If credentials are not configured, NetBackup marks all CIFS AdvancedDisk storage units that use the UNC naming convention as DOWN.

To configure service credentials

1   In Windows, open the **Services** dialog box. How you open **Services** depends on the Windows version.

2   Double-click the service name to open the **Properties** dialog box for the service.

3   In the **General** tab, select the service that requires additional credentials. Click **Stop** to stop the service.

4   Select the **Log On** tab.

5   Select **This account** and then enter the credentials. Click **Apply**.

6   Select the **General** tab.

7   Click **Start** to start the service.

8   Repeat the steps 2 to 7 for each service that requires additional credentials.

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 19.

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 19.

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

See "About data encryption for AdvancedDisk storage" on page 21.

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

See "Configuring an AdvancedDisk storage server" on page 30.

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.

Table 3-2   Preferred or required read server descriptions

Server attribute	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 3-2   Preferred or required read server descriptions *(continued)*

Server attribute	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 Administrator's Guide, Volume I.

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 Administrator's Guide, Volume I.

About data encryption for AdvancedDisk storage

You can encrypt your data on the storage. To use encryption, you must use the **AdvancedDisk_crypt** type when you configure the storage servers and the disk pools. You also must use the `nbdevconfig` command to configure the storage servers and the disk pools.

See "Configuring an AdvancedDisk storage server" on page 30.

NetBackup uses the Key Management Service to manage encryption keys. You must configure KMS so that NetBackup can use AdvancedDisk encryption.

See "About key management for encryption of NetBackup AdvancedDisk storage" on page 22.

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

Information about data-at-rest encryption and security is available.

See the NetBackup Security and Encryption Guide available from the Symantec Knowledgebase.

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.

http://www.symantec.com/

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

See the NetBackup Security and Encryption Guide available from the Symantec Knowledgebase.

About key management for encryption of NetBackup AdvancedDisk storage

NetBackup supports encryption for AdvancedDisk storage.

See "About data encryption for AdvancedDisk storage" on page 21.

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

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

Table 3-3   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 3-4   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. The key group key requires a pass phrase. The key group name must use the following format: ■ UNIX storage: *storage_server_name*:*volume_name* ■ Windows storage: *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*, you must specify the part of the mount point that is after the last slash. Therefore, the *volume_name* depends on how the operating system exposes the storage, as follows: 　■ On the storage that is exposed as a pathname (such as /mnt/disk/backups), use the last directory name for the *volume_name*. 　■ On the storage that is exposed as a drive letter (such as E:\), nothing appears after the last slash. Therefore, the *volume_name* is not required.
A key record	Each key group 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 23.

More information about KMS is available.

See the NetBackup Security and Encryption Guide.

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 manually by following the steps in this topic.

Table 3-5   Configure key management manually

Step	Task	Instructions
Step 1	Learn about NetBackup key management	See "About key management for encryption of NetBackup AdvancedDisk storage" on page 22.
Step 2	Set up the KMS database	See "Setting up the KMS database for NetBackup AdvancedDisk storage encryption" on page 24.
Step 3	Create the key groups	Each storage server and volume combination requires a key group. See "Creating a KMS key group for NetBackup AdvancedDisk storage encryption" on page 26.
Step 4	Create the key records	Each key group requires a key record. The key record contains the encryption key. See "Creating a KMS key for NetBackup AdvancedDisk storage encryption" on page 27.
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 "Saving a record of the KMS key names for NetBackup AdvancedDisk storage encryption" on page 28.

See "Displaying KMS key information for AdvancedDisk encryption" on page 86.

See "About data encryption for AdvancedDisk storage" on page 21.

Setting 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 manually.

See " Configuring key management for NetBackup AdvancedDisk storage encryption" on page 23.

To set up the KMS database

1   On the NetBackup master 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 pass phrase for the host master key (HMK) or press **Enter** to create a
    randomly generated key.

    After you enter the Host Master Key pass phrase, 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 pass phrase, 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   Start the NetBackup Key Management Service on the master server. You can do so in the **Activity Monitor** of the **NetBackup Administration Console**.

      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.

Creating 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.

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 master 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: nbkmsutil -createkg -kgname *storage_server_name*:*volume_name*

      Storage on Windows: 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*, you must specify the part of the mount point that is after the last slash. Therefore, the *volume_name* depends on how the operating system exposes the storage, as follows:

- On the storage that is exposed as a pathname, use the last directory name for the *volume_name*. If the pathname is `/mnt/disk/backups`, the *volume_name* must be `backups`, as follows:

  ```
  nbkmsutil -createkg -kgname UX_Host.symantecs.org:backups
  ```

- On the storage that is exposed as a drive letter (such as `E:\`), nothing appears after the last slash. Therefore, the *volume_name* is not required, as follows:

  ```
  nbkmsutil -createkg -kgname Win_Host.symantecs.org:
  ```

  The following is the path name to the `nbkmsutil` command:

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

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

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

See "Creating a KMS key for NetBackup AdvancedDisk storage encryption" on page 27.

Creating 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 23.

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 master 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`

The following examples show the usage for storage on different operating systems:

Storage on UNIX: `nbkmsutil -createkey -keyname AdvDisk_Key -kgname UX_Host.symantecs.org:backups -activate`

Storage on Windows: `nbkmsutil -createkey -keyname AdvDisk_Key -kgname Win_Host.symantecs.org: -activate`

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 "Saving a record of the KMS key names for NetBackup AdvancedDisk storage encryption" on page 28.

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

Symantec recommends that you save a record of the encryption key names. The key tag that is listed in the output is necessary if you need to recover or recreate the keys.

To save a record of the key names

1   To determine the key group names, use the following command on the master 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.symantecs.org: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          : -

Key Group Name       : Win_Host.symantecs.org:
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          : -
```

2   For each key group, write all of the keys that belong to the group to a file. Run
    the command on the master 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.symantecs.org:backups >
    encrypt_keys_UX_Host.symantecs.org_backups.txt

    Key Group Name       : UX_Host.symantecs.org: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          : -

      Key Tag    : 867d710aa7f4c64dcdd2cec6...cced0c831c1812c510acd05
      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          : -

    Number of Keys: 1
    ```

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

4   Store the file in a secure location.

Configuring 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 18.

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 21.
	See "To configure an AdvancedDisk storage server by using the command line" on page 32.
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 19.
	See "To configure an AdvancedDisk storage server by using the command line" on page 32.
No encryption or attributes	Symantec 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 32.

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 also is configured as a data mover.

See "About AdvancedDisk data movers" on page 19.

To configure an AdvancedDisk storage server by using the command line

1   Run the following command on the NetBackup master 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*`]`

    See "AdvancedDisk storage server options" on page 36.

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.symantecs.org
    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 "Configuring an AdvancedDisk disk pool" on page 39.

To configure an AdvancedDisk storage server by using the wizard

1   In the **NetBackup Administration Console**, select either **NetBackup
    Management** or **Media and Device Management**.

2   In the right pane, click **Configure Disk Storage Servers**.

3   Click **Next** on the welcome panel of the wizard.

    The **Add Storage Server** panel appears.

4 On the **Add Storage Server** panel, select **AdvancedDisk** from the drop-down menu. The following is an example of the wizard panel:
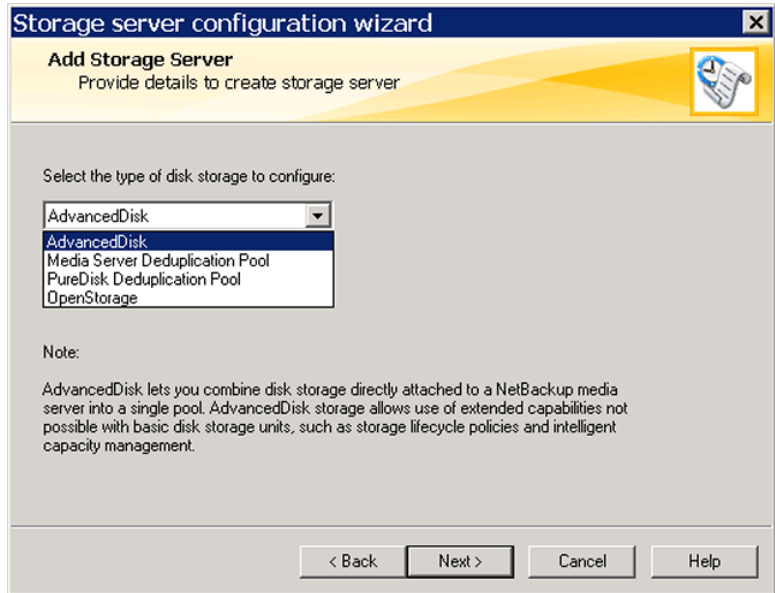
The types of storage servers that you can configure depend on the options for which you are licensed.

Click **Next.** A wizard panel about **Storage server details** appears.

5 For the **Storage server details**, select the media server that you want to configure as an AdvancedDisk storage server from the **Media server** drop-down menu. Then, click **Next**. The following is an example of the wizard panel:
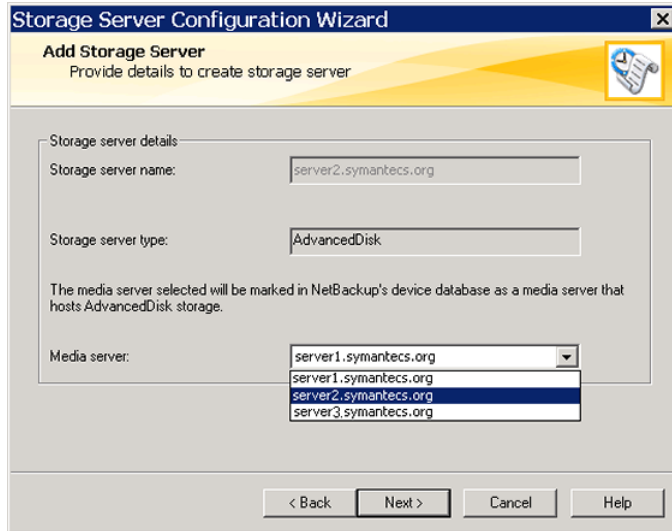
The **Storage Server Configuration Summary** panel appears.

6   On the **Storage Server Configuration Summary** panel, verify the selections. If OK, click **Next**. The following is an example of the wizard panel:
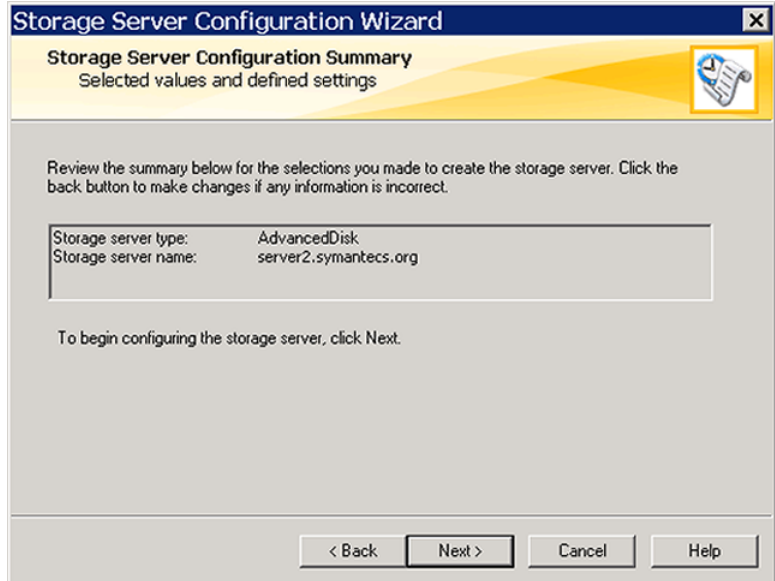
7   After NetBackup creates the storage server, a wizard panel describes the successful action. The following is an example of the wizard panel:
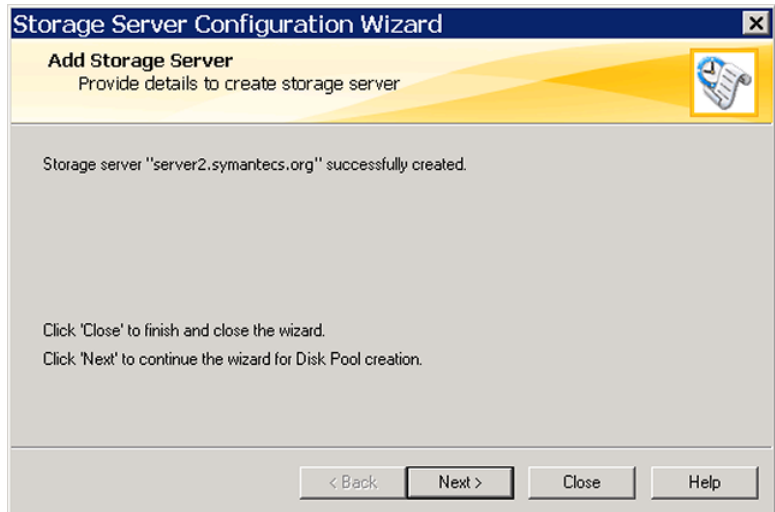
After the storage server is created, you can do the following.

- To configure another storage server, click **Close** and then repeat the steps in this procedure.

- To configure a disk pool for this storage server, click **Next**.
  Configure a disk pool if you have finished configuring the storage servers that can access the disk pool.

AdvancedDisk storage server options

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

Table 3-6   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.
`-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 19.

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.

When NetBackup sends backup data to a disk pool, NetBackup selects disk volumes based on available capacity and predicted size of the backup. NetBackup tries to write backup data to a single volume. If necessary, backup images span disk volumes in a disk pool. Backup images do not span across multiple disk pools.

For AdvancedDisk, NetBackup assumes exclusive ownership of the disk resources that comprise the disk pool. If you share those resources with other users, NetBackup cannot manage disk pool capacity or storage lifecycle policies correctly.

The following are disk volume considerations for AdvancedDisk storage:

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 spanning	If necessary, backup images span disk volumes in a disk pool. To reduce disk spanning, each volume in a disk pool should be larger than your largest backup.
	Note: Some file systems limitations can affect whether or not NetBackup can detect file system capacity accurately. On those file systems, Symantec recommends that you do not span backup images across volumes.
	See "About AdvancedDisk file system requirements" on page 16.
Disk contention	NetBackup queues backup and restore jobs if insufficient resources are available.
	To limit the possibility of disk 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.

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

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

See "About data encryption for AdvancedDisk storage" on page 21.

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

See "Configuring a CIFS disk volume for AdvancedDisk encryption" on page 38.

See "Configuring an AdvancedDisk disk pool" on page 39.

If an AdvancedDisk disk pool is a storage destination in a storage lifecycle policy, NetBackup capacity management applies.

Configuring 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.

(Alternatively, for the **AdvancedDisk** disk type, the **Disk Pool Configuration Wizard** lets you specify the CIFS volumes.)

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

You must first configure storage servers.

See "Configuring an AdvancedDisk storage server" on page 30.

To configure an AdvancedDisk disk volume by using the command line

1   On the NetBackup master 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.

Configuring an AdvancedDisk disk pool

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

AdvancedDisk type	Symantec recommends that you use the **Disk Pool Configuration Wizard** to configure the **AdvancedDisk** type of disk pool. However, you may use the `nbdevconfig` command.
	When you configure a storage server, that wizard continues to the **Disk Pool Configuration Wizard**. 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 40.
AdvancedDisk_crypt type	You must use the `nbdevconfig` command if you configured an **AdvancedDisk_crypt** type of storage server. The **AdvancedDisk_crypt** uses encryption for the storage.
	See "To configure an AdvancedDisk disk pool by using the `nbdevconfig` command" on page 48.
	If you use Common Internet File System (CIFS) volumes for your storage, you must configure the CIFS volumes before you configure the disk pool. (For the `nbdevconfig` command only; the wizard lets you add CIFS volumes to the disk pool.)
	See "Configuring a CIFS disk volume for AdvancedDisk encryption" on page 38.

When you create an AdvancedDisk disk pool, you specify or select the following:

- The NetBackup media servers that share the storage.
  The media servers must be configured as storage servers. They also function as data movers.

When you specify the storage servers, you associate them with the disk pool. Only those storage servers can access the disk pool.

See "About AdvancedDisk storage servers" on page 18.

- The disk volumes to include in the pool. If you use multiple storage servers for the same disk pool, you must use the same mount point on all storage servers for each volume.

  Normally, NetBackup discovers the volumes on the host you specify in the **Disk Pool Configuration Wizard** or the nbdevconfig command line. However, NetBackup cannot discover Common Internet File System (CIFS) disk volumes. (Networked mapped devices are not visible to Windows services.) Therefore, you must use the Windows Universal Naming Convention to specify the CIFS volumes that you want to use for AdvancedDisk disk pools.

  For **AdvancedDisk**, the **Disk Pool Configuration Wizard** lets you specify the CIFS volumes.

  For **AdvancedDisk_crypt**, you must use the nbdevconfig command to specify the CIFS volumes *before* you configure the disk pool.

  See "Configuring a CIFS disk volume for AdvancedDisk encryption" on page 38.

- The disk pool properties.

  See "AdvancedDisk disk pool properties" on page 51.

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

You must first configure storage servers.

See "Configuring an AdvancedDisk storage server" on page 30.

To configure an AdvancedDisk disk pool by using the wizard

1   If the **Disk Pool Configuration Wizard** was launched from the **Storage Server Configuration Wizard**, go to step 3.

    Otherwise, in the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.

2   From the list of wizards in the right pane, click **Configure Disk Pool**.

3   Click **Next** on the welcome panel of the wizard.

    The **Disk Pool** panel appears.

4   On the **Disk Pool** panel, select **AdvancedDisk** in the **Type** windows.

The following is an example of the wizard panel:
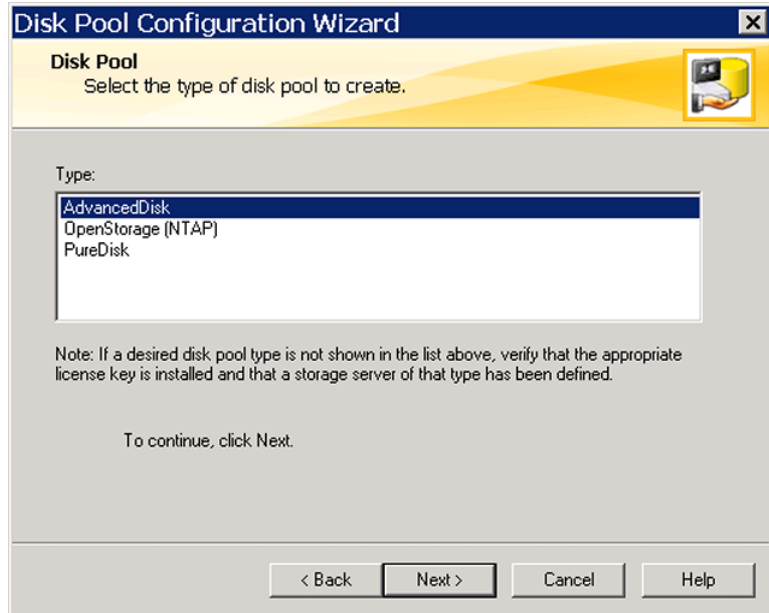
The types of disk pools that you can configure depend on the options for which you are licensed.

Click **Next**. The **Select Storage Server** wizard panel appears.

5 On the **Select Storage Server** panel, select the NetBackup media servers that you want to function as storage servers for this disk pool.

The following is an example of the wizard panel:
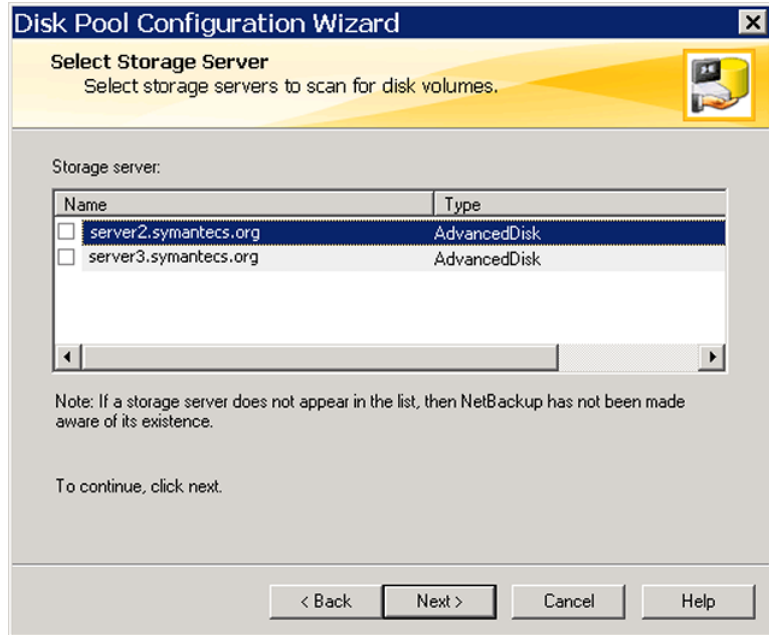
All NetBackup media servers that you configured as AdvancedDisk storage servers appear.

Click **Next**. The **Select Volumes** wizard panel appears.

6   On the **Select Volumes** panel, select the volumes for this disk pool.

The following is an example of the wizard panel:
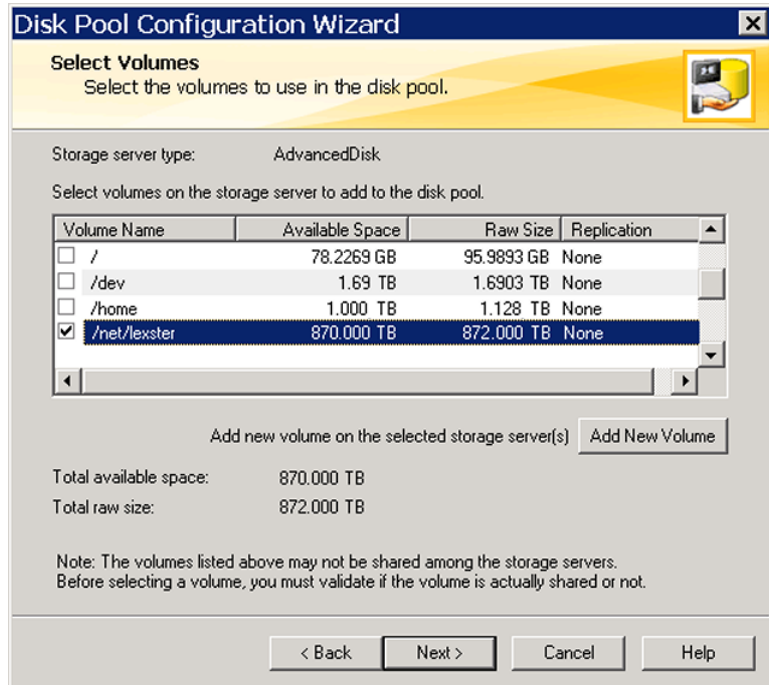
The wizard panel displays the volumes available on the storage server. If you selected more than one storage server, volumes that are common to all of them appear.

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.

To specify a Common Internet File System (CIFS) disk volume, click **Add New Volume**. In the **Add New Volume** dialog box, enter the Windows Universal Naming Convention (UNC) pathname of the CIFS volume and then click **Validate and Add**.

See "About AdvancedDisk file system requirements" on page 16.

Click **Next**. The **Additional Disk Pool Information** wizard panel appears.

7 On the **Additional Disk Pool Information** panel, enter the values for this disk pool.

The following is an example of the wizard panel:
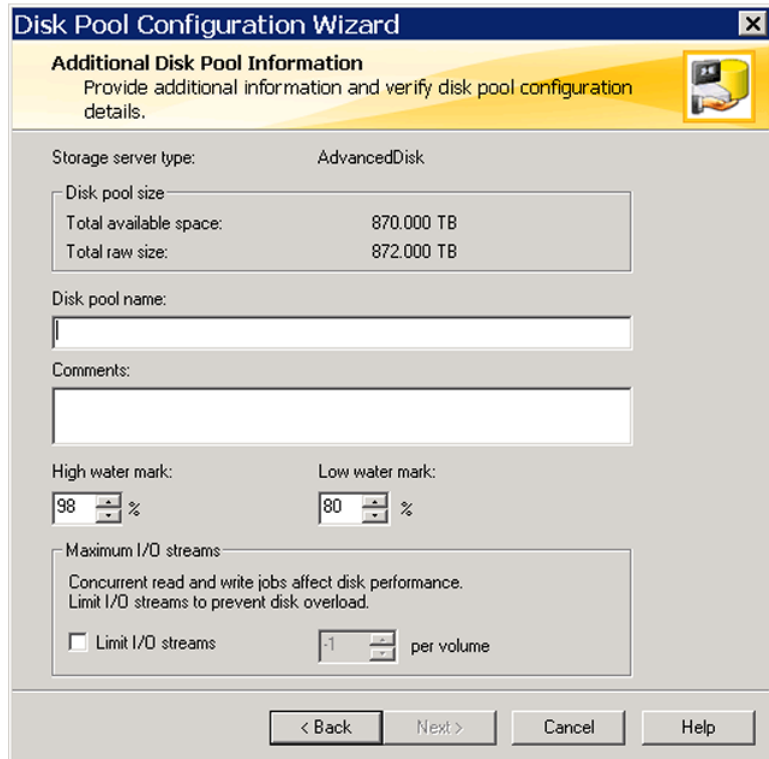
See "AdvancedDisk disk pool properties" on page 51.

Click **Next**. The **Summary** wizard panel appears.

8 On the **Summary** panel, verify the selections. If OK, click **Next**.

The following is an example of the wizard panel:
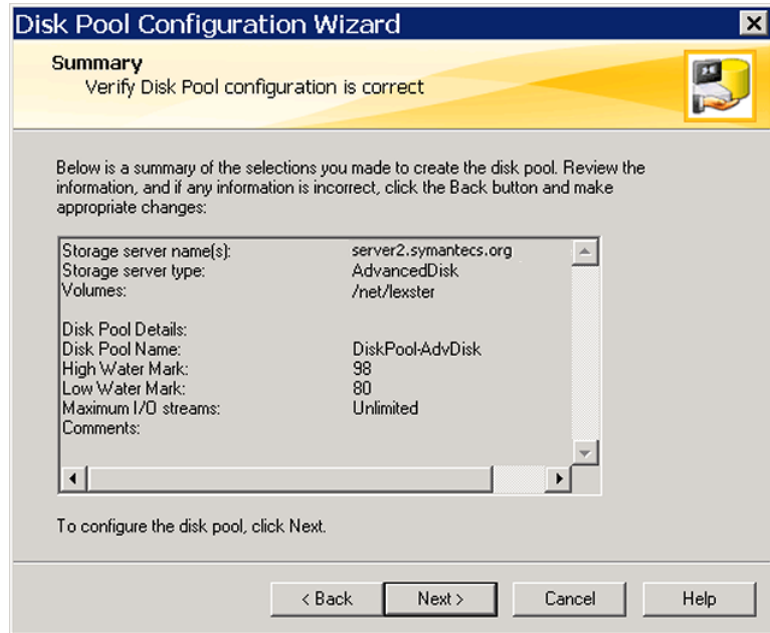
9 After NetBackup creates the disk pool, a wizard panel describes the successful action.

To continue, click **Next**.

The **Storage Unit creation** wizard panel appears.

10 To configure a storage unit for the disk pool, ensure that **Create a Storage Unit that uses *disk_pool_name*** is selected, then click **Next**. Otherwise, click **Close** to exit from the wizard.

The following is an example of the wizard panel:
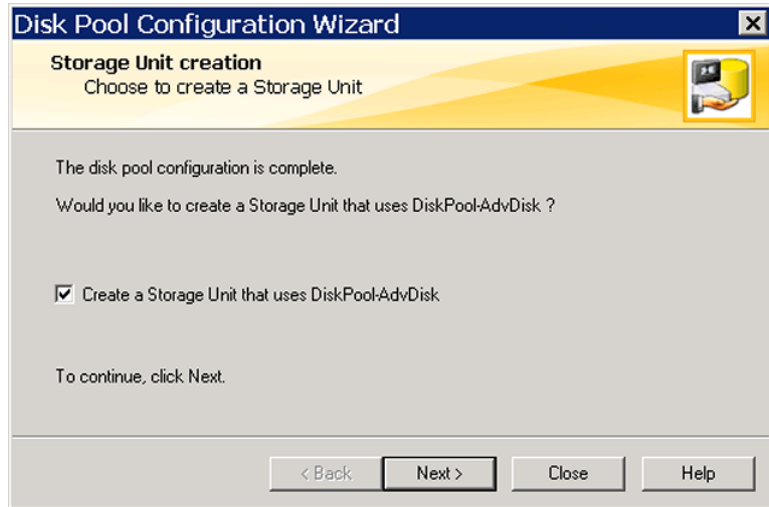
If you click **Next**, a wizard screen appears in which you enter the details about the storage unit.

11 Enter the appropriate information for the storage unit.

The following is an example of the wizard panel:
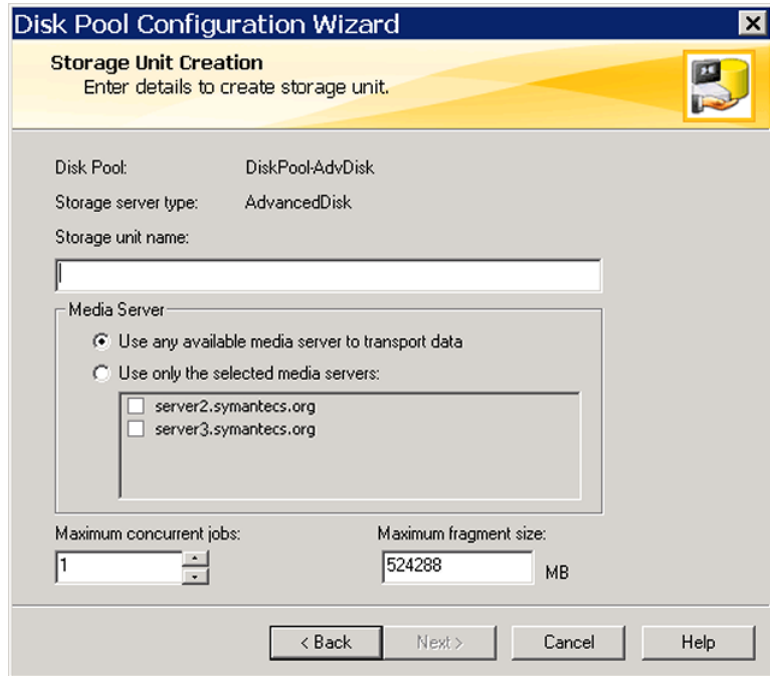
See "AdvancedDisk storage unit properties" on page 53.

Click **Next** to create the storage unit.

12 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

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. Symantec recommends that you use a name that describes its purpose.

2   Copy the file that you created in step 1 to the master 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` *`master_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` *`master_server`*`] [-reason` `"`*`string`*`"]`

`-dp` *`disk_pool_name`*	The name of the disk pool. Use the same name that you used when you configured the disk volumes.
`-stype` *`server_type`*	For AdvancedDisk with encryption, use **AdvancedDisk_crypt**, otherwise use **AdvancedDisk**.
`-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.
`-dvlist` *`filename`*	The name of the file that contains the information about the volumes for the disk pool.
`-hwm` *`high_watermark`*	See "AdvancedDisk disk pool properties" on page 51.
`-lwm` *`low_watermark`*	See "AdvancedDisk disk pool properties" on page 51.
`-max_io_streams` *`n`*	See "AdvancedDisk disk pool properties" on page 51.
`-comment` *`comment`*	See "AdvancedDisk disk pool properties" on page 51.
`-M` *`master_server`*	The name of the master server.
`-reason "`*`string`*`"`	The reason that you create the disk pool.

AdvancedDisk disk pool properties

Table 3-7 describes the disk pool properties.

Table 3-7 AdvancedDisk disk pool properties

Property	Description
Name	The disk pool name.
Storage server	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 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.
Comment	A comment that is associated with the disk pool.
High water mark	The **High water mark** setting is a threshold that triggers 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%.

	Table 3-7	AdvancedDisk disk pool properties *(continued)*

Property	Description
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.
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.

Configuring an AdvancedDisk storage unit

Create one or more storage units that reference the disk pool.

The **Disk Pool Configuration Wizard** lets you create a storage unit; therefore, you may have created a storage unit when you created a disk pool. To determine if storage units exist for the disk pool, see the **NetBackup Management > Storage > Storage Units** window of the **NetBackup Administration Console**.

See "About AdvancedDisk storage unit recommendations" on page 55.

More information about storage units is available.

See the NetBackup Administrator's Guide, Volume I.

To configure a storage unit from the Actions menu

1   In the **NetBackup Administration Console**, in the left pane, select **NetBackup Management > Storage > Storage Units**.

2   Click **Actions** > **New > Storage Unit**.
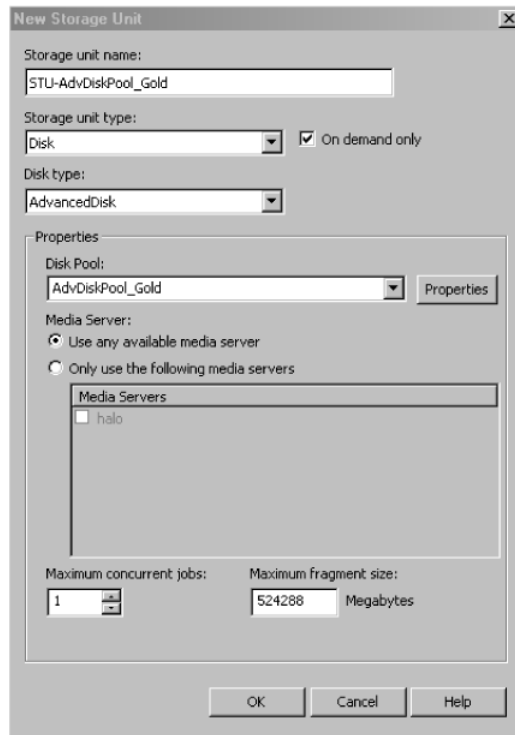
3   Complete the fields and set the options in the **New Storage Unit** dialog box.

See "AdvancedDisk storage unit properties" on page 53.

4   Click **OK**.

AdvancedDisk storage unit properties

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

Table 3-8   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.
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 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.)

Table 3-8	AdvancedDisk storage unit properties *(continued)*

Property	Description
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.

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 configuring a favorable client-to-server ratio" on page 55.

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 56.

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.

An SLP 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 Parameters** properties in the **NetBackup Administration Console** allow administrators to customize how SLPs are maintained and how SLP jobs run.

Best-practice information about SLPs appears in the following document:

http://www.symantec.com/docs/TECH208536

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   In the **NetBackup Administration Console**, select **NetBackup Management > Storage > Storage Lifecycle Policies**.

2   Click **Actions > New > New Storage Lifecycle Policy** (Windows) or **Actions > New > Storage Lifecycle Policy** (UNIX).
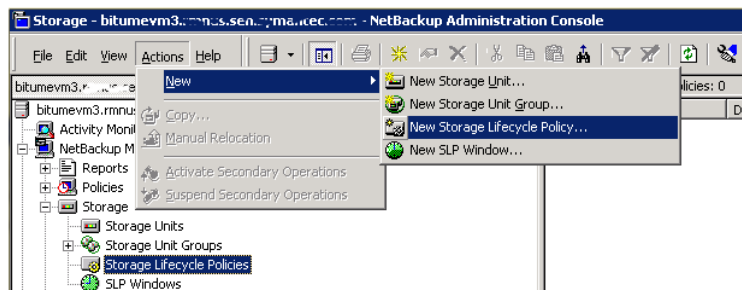
3   In the **New Storage Lifecycle Policy** dialog box, enter a **Storage lifecycle policy name**.

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**.

If this is not the first operation in the SLP, add an operation that is either hierarchical or non-hierarchical:

To create a hierarchical operation, select an operation to become the source of the next operation. Click **Add**. The new operation is a child of the selected operation. The child is indented under the parent operation.
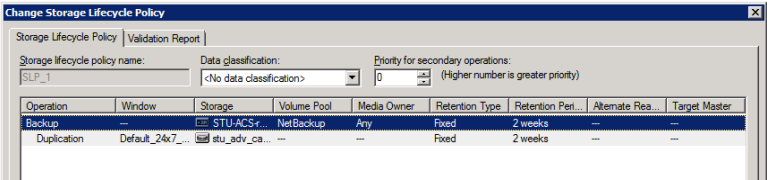
To create a non-hierarchical operation, do not select an operation. A non-hierarchical operation means that the operation does not have a parent and child relationship with another operation. The new operation is not indented.
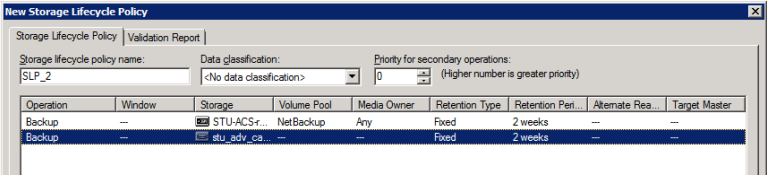
5   In the **Properties** tab of the **New Storage Operation** dialog box, select an **Operation** type. If you're creating a child operation, the SLP displays only those operations that are valid based on the parent operation that you've selected.

The name of the operation reflects its purpose in the SLP:

- **Backup**

- **Duplication**

- **Import**

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 Click the **Advanced** button in the **Properties** tab to display options about how the window should behave if the window closes and a secondary operation is not yet complete.

9 Click **OK** 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 Click **OK** 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**.

See "Creating a backup policy" on page 62.

Storage Lifecycle Policy dialog box settings

The **New Storage Lifecycle Policy** dialog box and the **Change Storage Lifecycle Policy** dialog box contain the following settings.

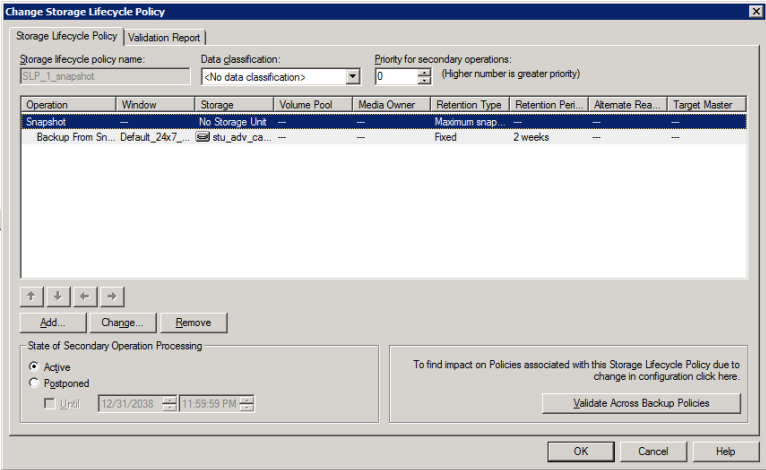**Figure 3-1** Storage Lifecycle Policy tab

Table 3-9   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.
Data classification	The **Data classification** defines the level or classification of data that the SLP is allowed to process. The drop-down 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. It is available for SLP configuration only and is not available to configure a backup policy.
	In an Auto Image Replication configuration where the master server domains run different versions of NetBackup, see the following topic for special considerations:
	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.

Table 3-9   Storage Lifecycle Policy tab *(continued)*

Setting	Description
Operations	Use the **Add**, **Change**, and **Remove** buttons 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 display by default.
	For column descriptions, see the following topic:
Arrows	Use the arrows to indicate the indentation (or hierarchy) of the source for each copy. One copy can be the source for many other copies.
Active and **Postponed**	The **Active** and **Postponed** options appear under **State of Secondary Operation Processing** and refer to the processing of all duplication operations in the SLP.
	Note: The **Active** and **Postponed** options apply to duplication operations that create tar-formatted images. For example, those created with `bpduplicate`. The **Active** and **Postponed** options do not affect the images that are duplicated as a result of OpenStorage optimized duplication, NDMP, or if one or more destination storage units are specified as part of a storage unit group.
	These options do not apply if either the source media server or the destination media server is not at NetBackup 7.6.
	■ Enable **Active** to let secondary operations continue as soon as possible. When 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.
Validate Across Backup Policies button	Click this button to see how changes to this SLP can affect the policies that are associated with this SLP. The button generates a report that displays on the **Validation Report** tab.
	This button performs the same validation as the `-conflict` option performs when used with the `nbstl` command.

Creating a backup policy

The easiest method to set up a backup policy is to use the **Policy Configuration Wizard**. This wizard guides you through the setup process by automatically choosing the best values for most configurations.

Not all policy configuration options are presented through the wizard. For example, calendar-based scheduling and the **Data Classification** setting. After the policy is created, modify the policy in the **Policies** utility to configure the options that are not part of the wizard.

Note: Do not use the Policy Configuration Wizard to configure policies for Replication Director.

Using the Policy Configuration Wizard to create a backup policy

Use the following procedure to create a backup policy with the Policy Configuration Wizard.

To create a backup policy with the Policy Configuration Wizard

1   In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.

2   In the right pane, click **Create a Policy** to begin the **Policy Configuration Wizard**.

3   Click **Next** to start the wizard and follow the prompts.

Click **Help** on any wizard panel for assistance while running the wizard.

Creating a backup policy without using the Policy Configuration Wizard

Use the following procedure to create a backup policy in the **NetBackup Administration Console** without using the Policy Configuration Wizard.

To create a policy without the Policy Configuration Wizard

1   In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.

2   On the **Actions** menu, click **New > Policy**.

3   Type a unique name for the new policy in the **Add a New Policy** dialog box.

4   If necessary, clear the **Use Policy Configuration Wizard** checkbox.

5   Click **OK**.

6   Configure the attributes, the schedules, the clients, and the backup selections
    for the new policy.

Resilient Network properties

The **Resilient Network** properties appear for the master server, for media servers,
and for clients. For media servers and clients, the **Resilient Network** properties
are read only. When a job runs, the master 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. 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 master
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 for Exchange or SharePoint

- 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 master servers when they function as media servers. Resilient connections
do not apply to master 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 different subdomain than the server, add the fully qualified domain name of the server to the client's hosts file. For example, **india.symantecs.org** is a different subdomain than **china.symantecs.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.

Figure 3-2   Master server Resilient Network host properties
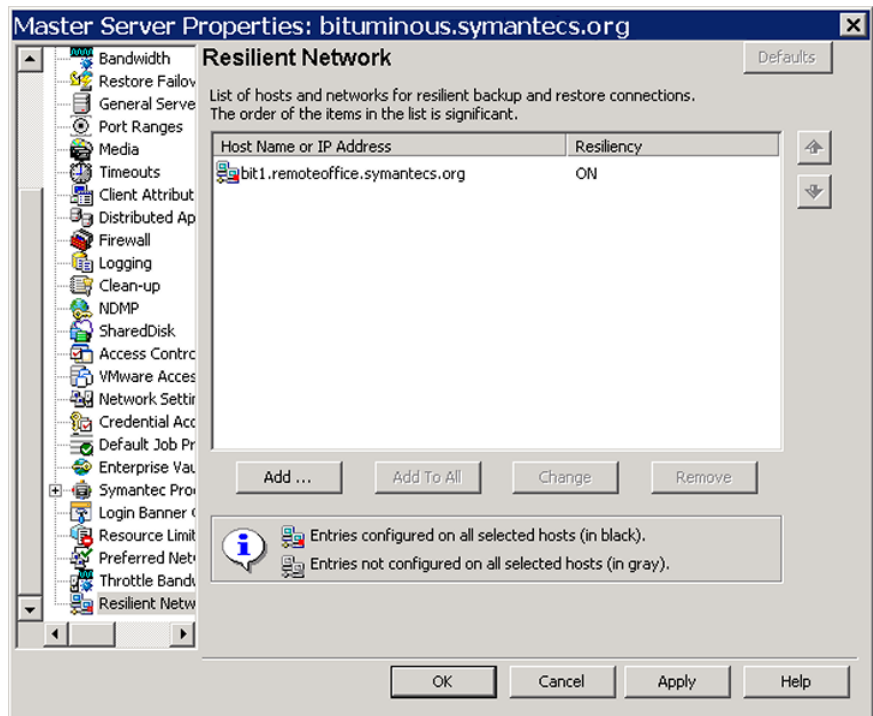

Table 3-10 describes the **Resilient Network** properties.

Table 3-10   Resilient Network dialog box properties

Property	Description
Host Name or IP Address	The **Host 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, Symantec recommends 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.

The resilient status of each client also appears as follows:

■ In the **NetBackup Administration Console**, select **NetBackup Management > Policies** in the left pane and then select a policy. In the right pane, a **Resiliency** column shows the status for each client in the policy.

■ In the **NetBackup Administration Console**, select **NetBackup Management > Host Properties > Clients** in the left pane. In the right pane, a **Resiliency** column shows the status for each client.

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. Symantec recommends 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, Symantec recommends 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.

See the NetBackup Troubleshooting Guide.

Specifying resilient connections

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

See "Resilient Network properties" on page 63.

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

- Windows:
  install_path\Veritas\NetBackup\bin\admincmd\resilient_clients

- UNIX: /usr/openv/netbackup/bin/admincmd/resilient_clients

To specify resilient connections

1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.

2 In the right pane, select the master server on which to specify properties.

3 On the **Actions** menu, click **Properties**.

4 In the properties dialog box left pane, select **Resilient Network**.

5 In the **Resilient Network** dialog box, use the following buttons to manage resiliency for clients:

Add	To add resilient settings

       1   Click **Add**.

            The **Add Resilient Network Settings** dialog box appears

       2   Enter a client host name, an IP address, or an address range.

            If you specify the client host by name, Symantec recommends that you use the fully qualified domain name.

            For address ranges, use Classless Inter-Domain Routing (CIDR) notation (for example, **192.168.100.0/24** or **fd00::/8**).

       3   Ensure that the **Resiliency On** option is selected.

       4   Click **Add**.

       5   Repeat until you have finished entering clients or address ranges.

       6   When finished adding network settings, click **Close**.

Add To All   If you select multiple hosts in the **NetBackup Administration Console**, the entries in the **Resilient Network** list may appear in different colors, as follows:

- The entries that appear in black type are configured on all of the hosts.
- The entries that appear in gray type are configured on some of the hosts only.

For the entries that are configured on some of the hosts only, you can add them to all of the hosts. To do so, select them and click **Add To All**.

Change   To change resilient settings

       1   Select the client host name, the IP address, or the address range.

       2   Click **Change**.

            The **Change Resilient Network Settings** dialog box appears

       3   Select the desired **Resiliency** setting.

       4   Click **OK**.

Remove   Remove the select host or address range as follows

       1   Select the client host name, the IP address, or the address range.

       2   Click **Remove**.

            The client is removed immediately; a confirmation dialog box does not appear.

Move an item in the list of items

1   Select the client host name, the IP address, or the address range.

2   Click the appropriate button to move the item up or down.

The order of the items in the list is significant.

See "Resilient Network properties" on page 63.

Managing AdvancedDisk

This chapter includes the following topics:

- Managing AdvancedDisk storage servers
- Managing AdvancedDisk disk pools
- About monitoring AdvancedDisk storage capacity and usage
- Monitoring NetBackup disk activity
- Viewing AdvancedDisk disk reports
- Displaying detailed AdvancedDisk storage usage information
- Displaying KMS key information for AdvancedDisk encryption

Managing AdvancedDisk storage servers

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

See "Viewing AdvancedDisk storage servers" on page 70.

See "Determining AdvancedDisk storage server state" on page 70.

See "Viewing AdvancedDisk storage server attributes" on page 70.

See "Removing AdvancedDisk storage server attributes" on page 71.

See "Removing an AdvancedDisk storage server from disk pool access" on page 72.

See "Deleting an AdvancedDisk storage server" on page 72.

Viewing AdvancedDisk storage servers

Use the **NetBackup Administration Console** to view a list of storage servers already configured.

To view AdvancedDisk storage servers

◆ In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Credentials > Storage Server**.

The right pane, labeled **All Storage Servers** , shows all configured storage servers. AdvancedDisk storage servers show AdvancedDisk in the **Server Type** column.

Determining AdvancedDisk storage server state

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

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

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

- Windows: *install_path*`\NetBackup\bin\admincmd`

To determine AdvancedDisk storage server status

◆ Run the following command:

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

The `State` field shows either UP or DOWN.

Viewing 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 master server or a storage server:

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

The following is example output:

```
Storage Server      : advdsk_server.symantecs.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.

Removing 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 19.

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

See "Configuring an AdvancedDisk storage server" on page 30.

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 master server or on a storage server:

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

Removing 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`

Deleting 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   In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**.

2   On the **Edit** menu, select **Delete**.

3   Click **Yes** in the confirmation dialog box.

Managing AdvancedDisk disk pools

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

See "Viewing AdvancedDisk disk pools" on page 73.

See "About changing the AdvancedDisk disk pool size" on page 73.

See "Adding volumes to an AdvancedDisk disk pool" on page 74.

See "Changing AdvancedDisk disk pool properties" on page 74.

See "Determining AdvancedDisk disk pool state" on page 76.

See "Changing AdvancedDisk disk pool state" on page 76.

See "Determining AdvancedDisk disk volume state" on page 76.

See "Changing AdvancedDisk disk volume state" on page 77.

See "Merging AdvancedDisk disk pools" on page 78.

See "Removing a volume from an AdvancedDisk disk pool" on page 78.

See "Inventorying a NetBackup disk pool" on page 79.

See "Deleting an AdvancedDisk disk pool" on page 80.

Viewing AdvancedDisk disk pools

Use the **NetBackup Administration Console** to view configured disk pools.

To view disk pools

◆   In the **NetBackup Administration Console** tree, in the left pane, select **Media and Device Management > Devices > Disk Pools**.

The list appears in the right pane.

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, you must inventory the disk pool so that NetBackup reads the new size of the pool.

  See "Inventorying a NetBackup disk pool" on page 79.

- 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 74.

  See "Removing a volume from an AdvancedDisk disk pool" on page 78.

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 "Configuring an AdvancedDisk disk pool" on page 39.
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 "Merging AdvancedDisk disk pools" on page 78. |
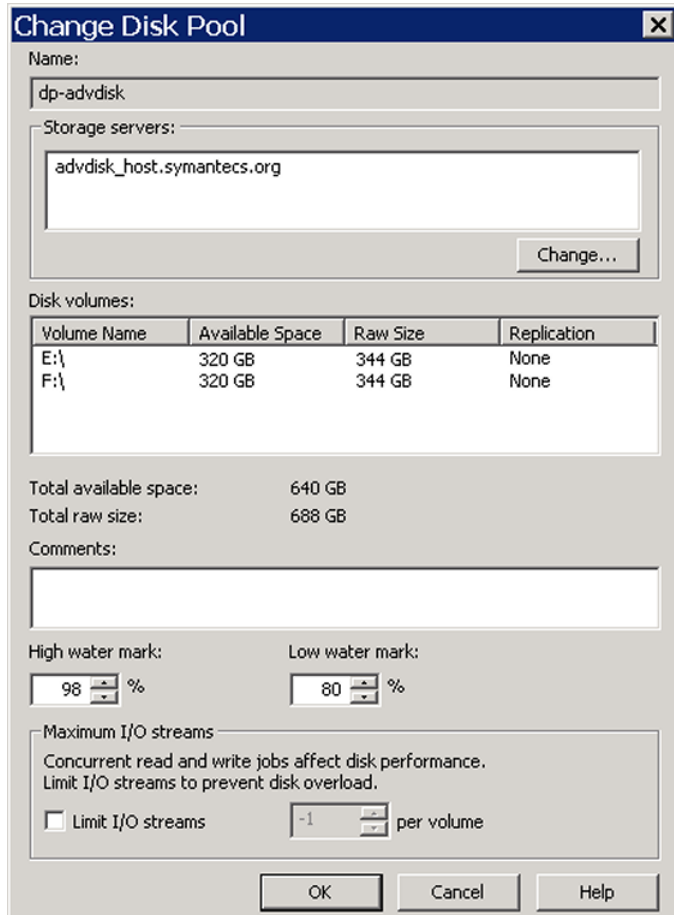
Changing AdvancedDisk disk pool properties

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 74.

To change disk pool properties

1   In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices > Disk Pools**.

2   In the right pane, select the disk pool that you want to change.

3   Click **Edit** > **Change**.

4   In the **Change Disk Pool** dialog box, change storage servers or the properties.

     See "AdvancedDisk disk pool properties" on page 51.

5   Click **OK**.

Determining AdvancedDisk disk pool state

Disk pool state is UP or DOWN.

To determine AdvancedDisk disk pool state

1 In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Device Monitor**.

2 Select the **Disk Pools** tab.

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

Changing AdvancedDisk disk pool state

Disk pool state is 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 In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Device Monitor**.

2 Select the **Disk Pools** tab.

3 Select the disk pool.

4 Select either **Actions > Up** or **Actions > Down**.

Determining AdvancedDisk disk volume state

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

To determine 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**.

.

Changing 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

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.

Merging 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 76.

    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 76.

Removing 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 "Changing AdvancedDisk disk volume state" on page 77.

2   Change the disk pool state to DOWN.

    See "Changing AdvancedDisk disk pool state" on page 76.

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 76.

Inventorying a NetBackup disk pool

An inventory of a NetBackup disk pool reads the capacity of the disk volumes in the pool. An inventory operation lets you update NetBackup with the new capacity values if you do the following:

■ Increase or decrease the size of the disk volumes in a disk pool.

■ Add volumes to or remove volumes from a disk pool.

How you increase or decrease the underlying storage capacity depends on your storage implementation. You must complete that process before you inventory the disk pool.

To inventory a NetBackup disk pool

1   in the **NetBackup Administration Console**, select **Media and Device Management** > **Devices** > **Disk Pools**.

2   On the **Actions** menu, select **Inventory Disk Pools**.

3   In the **Inventory Disk Pool** dialog box, select the disk pool to inventory and then click **Start Inventory.**

4   To update the NetBackup catalog with the capacity values returned by the inventory, click **Update Configuration**.

5   To inventory another disk pool, go to step 3.

6   To exit, click **Close**.

Deleting 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   In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Devices > Disk Pools**.

2   Select a disk pool

3   Click **Edit** > **Delete**.

4   In the **Delete Disk Pool** dialog box, verify that the disk pool is the one you want to delete and then click **OK**.

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
The NetBackup Administration Console **Disk Pools** window	The **Disk Pools** window displays a value 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 in the **Storage Server** window.

To display the window, select **Media and Device Management > Devices > Disk Pools**. |

Table 4-2   Monitor storage capacity and usage *(continued)*

What	Description
The NetBackup Disk Pool status report	See "Viewing AdvancedDisk disk reports" on page 82.
NetBackup Administration Console **Storage Server** window	The storage server view displays real-time values. To display the window, select **Media and Device Management > Credentials > Storage Servers**.
The **NetBackup License Keys** dialog box	The summary of active capacity-based license features in the **NetBackup License Keys** dialog box. The summary displays the storage capacity for which you are licensed and the capacity used. It does not display the amount of physical storage space. To open the dialog box, select **Help** > **License Keys** in the NetBackup Administration Console.
The `nbdevquery` command	See "Displaying detailed AdvancedDisk storage usage information" on page 83.

The NetBackup OpsCenter also provides information about storage capacity and usage.

See the NetBackup OpsCenter Administrator's Guide.

Monitoring 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 log (VxUL) 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 Troubleshooting Guide.

Viewing 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.

Table 4-4 describes the disk reports available.

Table 4-4   Disk reports

Report	Description
Images on 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	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 Storage Unit Status	The Disk Storage Unit Status report displays the state of disk storage units in the current NetBackup configuration. For disk pool capacity, see the disk pools window in **Media and Device Management > Devices > Disk Pools**. Multiple storage units can point to the same disk pool. When the report query is by storage unit, the report counts the capacity of disk pool storage multiple times.
Disk Pool Status	The Disk Pool Status report displays the state of disk pool storage units. This report displays only when a Data Protection Optimization Option license is installed.

To view disk reports

1   In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Reports > Disk Reports**.

2   Select the name of a disk report.

3   In the right pane, select the report settings.

4   Click **Run Report**.

Displaying 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.symantecs.org
    ```

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
    ```

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.
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.

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

Field	Description
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.

Displaying 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: Symantec 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.

The following are the directories in which the `nbkmsutil` command resides:

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

To display KMS key group information

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

```
nbkmsutil -listkgs

Key Group Name       : AdvDiskServer1.symantecs.org: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 an example:

```
nbkmsutil -listkeys -kgname AdvDiskServer1.symantecs.org:AdvDisk_Volume

Key Group Name       : AdvDiskServer1.symantecs.org: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
```

Toubleshooting AdvancedDisk

This chapter includes the following topics:

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

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. Unified logging creates log file names and messages in a standardized format. All NetBackup processes use either unified logging or legacy logging.

Unlike the files that are written in legacy logging, unified logging files cannot be viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file.

See "About legacy logging" on page 91.

Server processes and client processes use unified logging.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. 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:

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

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using 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 90.

See the NetBackup Commands Reference Guide for a complete description about these commands.

These commands are located in the following directory:

UNIX	/usr/openv/netbackup/bin
Windows	*install_path*\NetBackup\bin

About using the vxlogview command to view unified logs

Use the vxlogview command to view the logs that unified logging creates. These logs are stored in the following directory.

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

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the vxlogview command can assemble and display the log information correctly.

You can use vxlogview to view NetBackup log files as well as PBX log files.

To view PBX logs using the vxlogview command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.

- To specify the PBX product ID. enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

Examples of using vxlogview to view unified logs

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

Table 5-1   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`

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 "05/03/05 06:51:48 AM"`
	`    -e "05/03/05 06:52:48 AM"`

Table 5-1   Example uses of the vxlogview command *(continued)*

Item	Example
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*.

A complete description of `vxlogview` is in the NetBackup Commands Reference Guide.

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. In legacy debug logging, each process creates logs of debug activity in its own logging directory. All NetBackup processes use either unified logging or legacy logging.

See "About unified logging" on page 88.

To enable legacy debug logging on NetBackup servers, you must first create the appropriate directories for each process.

UNIX	`/usr/openv/netbackup/logs` `/usr/openv/volmgr/debug`
Windows	*install_path*`\NetBackup\logs` *install_path*`\Volmgr\debug`

After the directories are created, NetBackup creates log files in the directory that is associated with each process. A debug log file is created when the process begins.

To enable debug logging for the NetBackup Status Collection Daemon (`vmscd`), create the following directory before you start `nbemm`.

As an alternative, you can stop and restart `nbemm` after creating the following directory:

UNIX	`/usr/openv/volmgr/debug/reqlib`
Windows	*install_path*`\Volmgr\debug\reqlib\`

Tables are available that list the log directories that you must create.

Note: On a Windows server, you can create the debug log directories at once, under *install_path*`\NetBackup\Logs`, by running the following batch file: *install_path*`\NetBackup\Logs\mklogdir.bat`.

Media servers have only the `bpbrm`, `bpcd`, `bpdm`, and `bptm` debug logs.

Creating NetBackup log file directories

Before you configure a feature that uses the OpenStorage framework, create the directories into which NetBackup commands write log files. Create the directories on the master server and on each media server that you use for OpenStorage. 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.

See the *NetBackup Troubleshooting Guide*.

See "About NetBackup AdvancedDisk log files" on page 93.

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`

About NetBackup AdvancedDisk 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" on page 92.

Other processes use Veritas unified log (VxUL) files. Each process has a corresponding VxUL originator IDs. 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 Troubleshooting Guide.

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 Symantec representative. A log level of 5 is for troubleshooting only.

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup master server. The log levels for some processes specific to certain options are set in configuration files as described in Table 5-2.

Table 5-2 describes the logs.

	Table 5-2	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 5-3 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 "Resolving an incorrect storage type problem" on page 95.
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.

Resolving 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 master 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 95.

Index