NetBackup™ NAS Administrator's Guide

Release 10.1

VERITAS™

NetBackup™ NAS Administrator's Guide

Last updated: 2022-08-30

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Section 1

About NAS backups

Chapter 1

Introduction

This chapter includes the following topics:

- About NAS backups
- Backups using NAS-Data-Protection policy
- Backups using NDMP policy

About NAS backups

NetBackup Snapshot Manager and NDMP V4 snapshot extension can make snapshots of client data on a NAS host. A NAS snapshot is a point-it-time disk image. You can retain the Snapshots on the disk for any duration. Using the Instant Recovery feature in NetBackup, you can efficiently restore the data from the disk. Broadly, in NetBackup, snapshot-based data protection for NAS can be performed using NAS-Data-Protection policy and NDMP policy.

Backups using NAS-Data-Protection policy

NAS-Data-Protection policy is a robust approach to backup the data residing on NAS storage. It is also known as dynamic NAS or D-NAS policy. NetBackup Snapshot Manager and the storage array plug-ins can make snapshots of NAS volumes and shares. The dynamic data streams can access the snapshots on the backup hosts and read them to create point-in-time backup copies. For more details about D-NAS policy, see *Section 2* of this guide.

Backups using NDMP policy

NetBackup can make snapshots of client data on a NAS (NDMP) host using NDMP V4 extension. The snapshot data is read over NDMP and backup copies are created

per configured target. For more details about NDMP policy, see *NetBackup™ for NDMP Administrator's Guide*.

Section 2

Using NAS-Data-Protection (D-NAS)

Chapter 2

D-NAS overview

This chapter includes the following topics:

- Dynamic data streaming for D-NAS Policy
- Understanding the features of D-NAS
- Dynamic streaming parameters
- Limitations and considerations

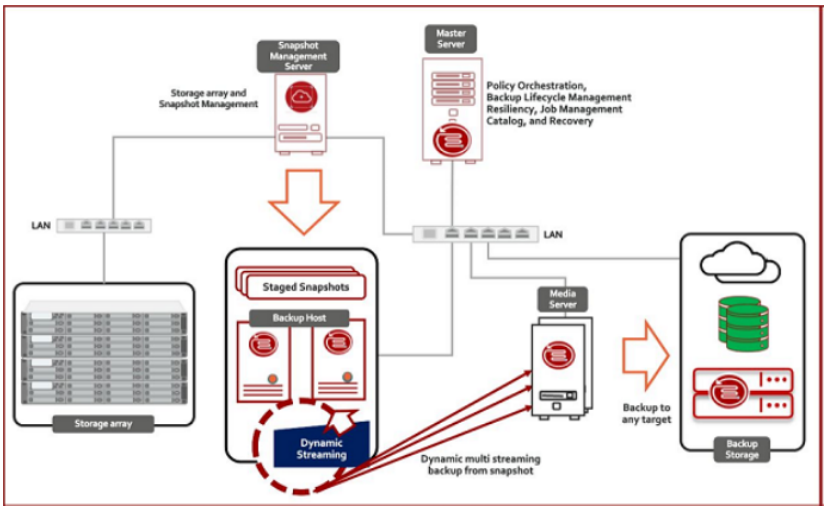
Dynamic data streaming for D-NAS Policy

Dynamic NAS (D-NAS): By means of Snapshot management server and the storage array plugins, NetBackup can make snapshots of NAS volumes and shares. The snapshots are accessed on backup hosts and read by dynamic streams to create point in time backup copies.

You can perform a snapshot enabled, off-host backup of NAS volumes, where a volume is backed up using dynamic backup streams.

Each NAS volume or share is read over NFS or SMB, and backed up using a configured number of backup streams. Files of these NAS volumes or shares are optimally distributed real time across streams to realize the full potential of backup streams. You cannot mix NAS volumes or shares of different storage array vendors in a single policy. In other words, using a single policy you can only protect assets for a single vendor and single NAS protocol.

Dynamic streaming is built on the NetBackup client framework and uses NAS-Data-Protection policy type for snapshot and backup orchestration of NAS data. This policy supports SLP only for data lifecycle.



Understanding the features of D-NAS

This table explains the salient features of data protection using D-NAS.

Table 2-1

Feature	Description
Convenience of backup host pool	Backup host pool is a group of NetBackup backup hosts where the snapshot of the volume is staged for the backup process to read. These hosts can be NetBackup client, media, or primary server.

Table 2-1 *(continued)*

Feature	Description
Vendor change tracking	Vendor change tracking (VCT) is a mechanism to get the difference in the content of the volume or share between two points-in-time snapshots. It relies on storage array vendor's native technology to identify the difference, that is, add, modify, and delete files between two point-in-time snapshots of the same volume. You must ensure that the storage array you are using, provides such a capability in order to use this feature. VCT is not applicable in the following conditions: ■ Schedule type is other than INCR and CINR. It's only supported for INCR and CINR. ■ Base snapshot is not available. ■ Expired after copy retention options is selected for snapshot in SLP. ■ Accelerator is enabled for the policy.
Exclude volumes	You can exclude the volumes out of the backup selection list that you do not want to backup. For example, `/prodVol*` is the backup selection, and there may be a volume `/prodVol-Scratch` which you do not want to backup.
NetBackup accelerator	NetBackup's robust accelerator feature can be leveraged along with dynamic streaming for optimized and fast backups.
Checkpoint restart	You can leverage NetBackup's checkpoint restart feature along with dynamic streaming. By taking checkpoints periodically during the backup, NetBackup can retry a failed backup from the beginning of the last checkpoint without restarting the entire job.

Dynamic streaming parameters

Dynamic streaming is a group of backup streams running in parallel which dynamically distributes the files for backups amongst them. This optimizes and speedups the backup of dense NAS volumes or shares.

- **Maximum number of streams per volume**: The value determines the number of backup streams that are deployed for backing up each volume. For example, If a policy contains 10 volumes and the value of this parameter is set to 4, then you see group of 4 backup streams for each volume, thereby total of 40 child backup streams and 10 parent backup streams as part of backup execution of the policy.
- **Maximum number of files in a batch**: The value determines the maximum number of files that processed in a single burst by any stream. The files in a batch are processed sequentially within the stream. For example, Value of 300 for this parameter means that every stream is assigned maximum of 300 files in a single batch. So if a volume has one million files to be backed up and 4 streams assigned, then every stream is assigned 300 files each to begin with and then subsequently the streams are fed with 300 more files as and when they are ready for more backup processing.

Limitations and considerations

You can set up a NAS-Data-Protection policy for your workloads.

Note: If you use cloud as a storage unit, you must configure appropriate buffer size. Refer to the *NetBackup Cloud Administrator's Guide*.

Note the following important points about NAS-Data-Protection policy.

- The NAS-Data-Protection is not supported in the DNAT environment.
- This policy does not support copy-based retention for Snapshot images. Ensure that you carefully plan your policy scheduling and snapshot retention in SLP.
- Client side deduplication is not supported for NAS-Data-Protection policy.
- Vendor Change Tracking (VCT) and Accelerator options are mutually exclusive for NAS-Data-Protection policy. You cannot enable both. Veritas recommends that you do not toggle the policy with these options between different execution of this policy.
- Vendor Change Tracking (VCT) enabled backup with incremental schedule requires base snapshot copy to determine the difference between current snapshot copy and base snapshot copy. Differential incremental schedule refers to base snapshot copy from previous differential incremental or cumulative incremental or full schedule. Cumulative incremental schedule refers to base snapshot copy from previous cumulative incremental or full schedule. During VCT enabled backup with incremental schedule, if the base snapshot copy is

not available then the backup operation might fail with the error shown in Activity Monitor Detailed status.

- NAS-Data-Protection policy is a snapshot enabled data protection policy. You can configure only storage lifecycle policy (SLP) against policy's storage destination. Additionally, the SLP should always have Snapshot as the primary job and Backup from Snapshot as secondary job.
- If the NAS-Data-Protection policy is used in a backup host that is running anti-virus software, the parent backup from snapshot job might hang.
  The anti-virus software may block NetBackup process interactions causing the processes to hang. In this particular scenario, the nbcs process on the backup host might hang resulting in the backup-from-snapshot job to hang. Create an antivirus exclusion for nbcs on the backup host.
  To cancel the hung job:
  - Note down the process ID of the nbcs process which is running on the backup host. This can be obtained from the job details section.
  - Login to the backup host and manually kill the nbcs process.
  - Refer to the Technote for more details regarding how to exclude the NetBackup processes from virus scanning: https://www.veritas.com/support/en_US/article.100004864
  - If the above steps cannot resolve the issue (and the nbcs hang persists), uninstall the network component from antivirus. On Symantec Endpoint Protection, this is called the "Network and Host Exploit Mitigation" component.
- For NAS-Data-Protection policy, multiple images are created for a single volume that is backed up. The number of images is equal to the value configured for the **Maximum number of streams per volume** in the policy. Since a single image cannot be referred from a single volume, NetBackup groups the images associated with a volume. When an operation is performed on one of the images in a volume, the same operation is also performed on the other grouped images in the volume. For example, if **Maximum number of streams per volume** is set as four and you select one image for a volume to expire, the other three images also expire. The image grouping is applicable for the following operations:
  - Browse and Restore
  - Image expiration
  - Image import
  - Image duplication
  - Image verification
  - Set primary copy

Note: Image grouping is not applicable for importing images as part of Image Sharing operation.

- To enable checkpoint restart for NAS-Data-Protection policies created before upgrading to version 9.0, you must select the **Take checkpoints every** check box and enter a value in minutes.

Note: The NAS-Data-Protection policy cannot be configured using the NetBackup web UI.

Chapter 3

Pre-requisites for D-NAS configuration

This chapter includes the following topics:

- Prerequisites for D-NAS configuration
- Domain user requirement for SMB share backups
- Minimum supported backup host versions for different features
- Configuring a backup host pool
- Configuring storage lifecycle policies

Prerequisites for D-NAS configuration

You need to meet the following pre-requisites.

- Ensure that you have installed the NetBackup Snapshot Manager component. For more details, see *Veritas NetBackup™ Snapshot Manager Install and Upgrade Guide*.
- Prepare the plug-in that you want to use for the NetBackup DNAS configuration. For more details, refer the *Veritas NetBackup™ Snapshot Manager Install and Upgrade Guide*.
- Identify the backup host that you want to use for the configuration.
- If NAS Data Protection policy uses TAPE storage unit in SLP for protecting NAS volumes, then the number of tape drives must be greater than or equal to the maximum number of streams per volume, otherwise backups fail. The other parameters of TAPE, like Media multiplexing and maximum concurrent write drives, does not have any affect on NetBackup DNAS backups.

- For SMB backups using NAS-Data-Protection policy the primary, media and backup host version should be 9.1 onwards.

Domain user requirement for SMB share backups

This step is required for Windows backup hosts for SMB share backups only. You must log on to the NetBackup client service and the NetBackup legacy network service as a domain user to perform the tasks described in the following sections.

Note: The Windows domain user must be a part of the local administrative group.

To log on to the NetBackup services as a domain user:

1. Make sure that the NetBackup client service and the NetBackup legacy network service are running.
2. In Windows Services, double-click the NetBackup service.
3. Check the **Log on** tab: if any of these services is not logged on as the domain user, change the logon to the domain account and restart the service. If both the services are not logged on as the domain user, you must do it in the following sequence:
   - Log on to the first service as domain user and restart the service.
   - log on to the second service as domain user and restart the service.
4. Make sure that all NetBackup services are running.
5. Relaunch the NetBackup UI.

Minimum supported backup host versions for different features

Different features of NAS Data Protection policy requires backup host with NetBackup version greater than or equal to the minimum supported backup host version. The following table specifies which feature is supported from which NetBackup version.

Table 3-1 NAS data protection policy features

Supported features	Minimum supported backup host version
Only NFS backup	8.3
NFS and Vendor change tracking	8.3

Table 3-1 NAS data protection policy features *(continued)*

Supported features	Minimum supported backup host version
NFS and Checkpoint restart enabled backups	9.0
NFS and Accelerator enabled backups	9.0.1
NFS, Checkpoint restart, and Accelerator	9.0.1
SMB backups (including CPR, accelerator, Vendor change tracking)	9.0.1

Configuring a backup host pool

Backup hosts and backup host pools are used for NAS-Data-Protection policy based on dynamic multi-streams.

You can use a NetBackup primary server, media server, or a standalone client as a backup host. For the hosts that you add to the backup host pool, their volumes are distributed for backup purposes on the backup hosts. This configuration results in a better backup performance.

Note: A NetBackup primary server running on Veritas Flex Appliance is not supported as a backup host for a NAS-Data-Protection policy.

You can create a backup host pool with different versions of NetBackup hosts. You can create Windows backup host pools only with version 9.0.1 or later. Windows hosts with a version earlier than 9.0.1 are not displayed.

Note the following important points:

- In a backup host pool you can either have Linux hosts or Windows hosts only. A pool does not support hosts with both platforms.
- All the hosts in the backup host pool must use the same OS version. This way each host has the same version of NFS for consistent backups.
- For backup hosts with a multi-NIC setup, add the host name that is already used on the NetBackup primary server. Do not add an alias name or any other host names in the backup host pool.

To configure a backup host pool

1. Open the **NetBackup Administration Console**.
2. Select **NetBackup Management > Host Properties > primary server**.
3. Double-click on the preferred primary server host name.

4. Click **Backup Host Pools**.
5. Click **Add**.
6. In the **Add Backup Host Pool** dialog box, enter a host pool name.
7. (Conditional) This step is applicable only for the clients that you want to add to the list. In the **Enter hostname to add to the list** field, add the client name and click **Add to list**.
8. Select the **OS Type**.
9. Select the backup hosts that you want to add to the list.
10. Click **OK**.

Note: You cannot delete a backup host pool, if it is configured with an existing NAS-Data-Protection policy.

Configuring storage lifecycle policies

To perform backup of NAS volumes using D-NAS policy, you need to specify a Storage Lifecycle Policy (SLP) as the policy storage destination. You must configure the SLP to use snapshot.

For more details, see the *Configuring storage lifecycle policies for snapshots and snapshot replication* chapter in the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*.

Chapter 4

Configure D-NAS policy for NAS volumes

This chapter includes the following topics:

- Configure D-NAS policy for NAS volumes
- Setting up a NAS-Data-Protection policy
- Ordering of backup from snapshot jobs
- About mixed mode volumes

Configure D-NAS policy for NAS volumes

Using the NetBackup™ Snapshot Manager for Data Center you can perform hardware snapshots of NFS and SMB shares. The snapshots are accessed on backup hosts and read by dynamic streams to create point in time backup copies. The following procedure describes how to configure a D-NAS policy to use hardware snapshots of NAS volumes.

Table 4-1 Configuration steps

Step	Description	Reference topic
1	Configure the NetBackup Snapshot Manager server in NetBackup	For more details, refer the *Installation and Upgrade* chapter of the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*.

Table 4-1 Configuration steps *(continued)*

Step	Description	Reference topic
2	Configure the NAS storage array plug-in	For more details, refer the *Configure NetBackup snapshot manager storage array plug-ins* chapter in the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*.
3	Add the backup hosts to a backup host pool. The backup hosts are responsible for data streaming.	See “Configuring a backup host pool ” on page 21.
4	Configure the SLP to use snapshot	For more details about replication, see *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*:
5	Configure a NAS-Data-Protection policy to perform the operations that are specified in the SLP	See “Configuring a backup host pool ” on page 21.

Note: For all the supported NAS storage arrays, refer to the *NetBackup Snapshot Manager* section, under *Snapshot Solutions* in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Setting up a NAS-Data-Protection policy

You must set up NAS data protection policy to protect your assets.

To set up a policy for NAS data protection

1. Open the **NetBackup Administration Console**.
2. Click **NetBackup Management > Policies** in the left pane.
3. In the **All Policies** pane, right-click and create a new one.
4. From the **Policy type** list, select **NAS-Data-Protection**
5. From the **Policy Storage** list, select **Storage Lifecycle Policy**.

   See “Configure D-NAS policy for NAS volumes ” on page 23.
6. (Optional) Select the **Take checkpoints every** check box and enter a value in minutes.
7. The **Perform snapshot backups** option is selected by default. Configure the snapshot options:

- **Snapshot Type**: Select the appropriate snapshot type. By default, Auto option is selected which enables NetBackup to automatically determine the snapshot type to be used for array snapshot.
- **Snapshot Manager**: Select the NetBackup Snapshot Manager host which communicates with the storage array to perform the snapshot operations.

Note: The **Snapshot Type** *Auto* is supported only with backup host version 10.0 onwards.

---

8 (Optional) To track changes between two snapshots, select the **Enable vendor change tracking for incremental backups** check box.

Note: At a given time, you can only use either the **Enable vendor change tracking for incremental backups** or the **Use Accelerator** check-box.

---

9 In the **Dynamic Data Streaming Attributes** section, the **Allow dynamic streaming** option is selected by default. Configure the following attributes:

Note: With this setting, the **Allow multiple data streams** option is also selected.

- **Maximum number of streams per volume**
  The number of streams per volume must be between 1 to 20. The default value is 4.
- **Maximum number of files in a batch**
  The number of files in a batch must be between 1 to 2000. The default value is 300.

10 (Optional) Select the **Use Accelerator** check box.

Note: At a given time, you can use either **Enable vendor change tracking for incremental backups** or the **Use Accelerator** check box.

---

11 On the **Clients** tab, from the **NAS Vendor** list, select the preferred vendor.

12 Click **New** to add a new client.

13 On the **Backup Selections** tab, select the preferred protocol.

- **NFS**
- **SMB**

14 (Optional) If you want to want to use volumes that support both NFS and SMB protocol, select the **Include Mixed Volume** option.

15 From the **Backup Host Pool** list, select the preferred pool and click **New**. If no backup host pools of the relevant type are available, you can see a dialog prompting you to create one, click **Yes** in the dialog to create one.

Note: If Backup host pool contains any backup host older than NetBackup 10.0 and **Auto** snapshot type is selected, the job may fail.

---

16 In the **Add Backup Selection** dialog box, click **Browse**.

If you add a subdirectory from volume in the backup selection then the policy validation fails.

17 In the **NAS Assets Selection** section, select the preferred volumes and click **OK**.

18 On the **Exclude Volumes** tab, in the **Volume to exclude** field, add the preferred volumes that you do not want to backup.

19 Click **OK**.

Ordering of backup from snapshot jobs

With the NetBackup 9.1 release, all SLP initiated backup from snapshot jobs for Policy, Client, or Backup selection are scheduled in a sequential manner. One scheduled backup from snapshot job must complete before the subsequent job can start. This behavior applies to the NAS-Data-Protection policy also. For example: If there are two scheduled snapshot jobs T1 and T2, and T1 is scheduled before T2. The ordering ensures that the backup from snapshot job for T1 must complete before the backup from snapshot job for T2 is started.

For NAS-Data-Protection policy, if checkpoint restart is enabled and the backup from snapshot job is in suspended or incomplete state, then that job must be resumed first, so that the next backup from snapshot jobs can get executed.

About mixed mode volumes

Mixed mode volumes are the volumes having multi-protocol access. Storage array vendors allow both NFS and SMB access to a NAS volume. D-NAS policy allows

backup of volumes having multi-protocol access. The protocol used for backup of these volumes depends on the type of backup host pool specified in the policy. If a Linux backup host pool is specified in the policy, these volumes would get backed up using NFS protocol. If a Windows backup host pool is specified in the policy, these volumes would get backed up using SMB protocol.

This mechanism can be used to backup SMB share data using a Linux backup host. For this to happen, enable NFS and SMB acces to the NAS volumes.

Note: When a Linux backup host is used to backup an SMB share, the backup of SMB ACLs does not happen. Only the SMB share data is backed up.

Chapter 5

Using accelerator

This chapter includes the following topics:

- Accelerator for D-NAS
- About the track logs for accelerator
- Track log sizing considerations
- Notes on accelerator for D-NAS

Accelerator for D-NAS

NetBackup accelerator provides faster full backups at the cost of incremental backups, eventually reducing the backup window for customers. With this solution, more data is protected in the specified backup window and less bandwidth consumption.

After an initial full backup that protects all data from the filer, NetBackup accelerator backs up only the changed data from the filer to the media server. The media server combines the changed data with any previous backup images to create a new full backup image. If a file or portion of a file is already in storage and has not been changed, the media server uses the copy in storage, rather than reading it from the filer to complete the backup image. The result is a faster NetBackup NDMP backup.

To configure Accelerator for D-NAS, select the **Use Accelerator** check box that is found on the policy **Attributes** tab.

Benefits of accelerator for D-NAS policy

Here are some benefits of using accelerator with D-NAS:

- Creates a compact backup stream that uses less network bandwidth between the filer and NetBackup servers.
- Reduces the I/O and CPU overhead on the media server and backup host.

- Independent of storage arrays. Works with all the supported NAS storage arrays.

About the track logs for accelerator

NetBackup accelerator uses track log to detect the new, change, and modify files in the subsequent Full and Increment backups. The track log is a binary file that you should not attempt to edit. For D-NAS policy each backup stream maintains its own track log. The number of backup streams depend on the policy attribute **Maximum no of streams per volume**.

Track log location on backup host:

Windows:

Install_path\NetBackup\track\master_server\storage_server \client\policy_name\backup selection\S1

Linux:

Install_path/netBackup/track/master_server/storage_server /client/policy_name/backup_selection/S1/

Track log location on primary server:

Windows:

```
Install_path\NetBackup\db\track\master_server\storage_server\
client\policy_name\backup selection\S1\
```

Linux:

```
Install_path/NetBackup/db/track/master_server/storage_server/
client/policy_name/backup_selection/S1/
```

Where `S1, S2… Sn` are the number of streams.

You can manually delete track logs safely if any of the follow situations occur:

- You disable the **Use Accelerator** option.
- The backup selections are changed.
- The policy is renamed.
- The storage server that is used to perform the backup is changed.
- The primary server that is used to control the backups is changed.

Track log sizing considerations

The accelerator track log stores file system metadata, and the unique fingerprints of files (128KiB segments). The track log size is relative to the size of the file system, and the number of backup files. Different track logs are created for each policy, client, and stream combination.

Here are some general guidelines, but the requirements in a specific environment might be different. Environments with a high rate of data change may require a larger track log size.

For D-NAS policy, the track log is stored on the backup host, and transferred to the primary server in-line during the backup operation. You can use the following formula to calculate the approximate size:

Total Track log size in Bytes for a NAS volume backup job = 2*((Number of files * 200) + ((Total used disk space in KiB/128KiB) * 20))

For example, 1 TB NAS volume with one million files = ~ 701 MiB total track log size. If four streams are configured for backup and one million files are equally distributed amongst four streams, streams, then each stream's track log can be of ~175 MiB in size.

Notes on accelerator for D-NAS

In-line track log persistence on primary server:

- The track log contents are synced in-line with the primary server.
- If the backup host changes for subsequent backup, the track log is copied from primary server to the current backup host.

Impact of changing the number of backup stream:

- If the number of backup streams are changed [policy attribute **Maximum no of streams per volume**] then in the next backup, the existing track logs are not used. A new base line is created for the subsequent backups. After changing the number of backup streams the accelerator optimization becomes “0” in the next backup and all the contents of the volume is backed up.

Chapter 6

Replication using D-NAS policy

This chapter includes the following topics:

- Replication using D-NAS policy

Replication using D-NAS policy

Using the NetBackup™ Snapshot Manager for Data Center you can replicate the hardware snapshots of NFS and SMB shares. The replicated snapshots are accessed on backup hosts and read by dynamic streams to create point in time backup copies. The following procedure describes how to configure a NAS-Data-Protection policy to use hardware snapshots and replication of NAS volumes.

Note: For all the supported NAS storage arrays for replication, refer to the *NetBackup Snapshot Manager* section, under *Snapshot Solutions* in the *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Table 6-1 Configuration steps

Step	Description	Reference topic
1	Configure the NetBackup Snapshot Manager server in NetBackup	For more details, refer the *Installation and Upgrade* chapter of the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide.*

Table 6-1 Configuration steps *(continued)*

Step	Description	Reference topic
2	Configure the NAS storage array plug-in	For more details, see the *Configure NetBackup snapshot manager storage array plug-ins* chapter of the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*.
3	Add the backup hosts to a backup host pool. The backup hosts are responsible for data streaming.	See “Configuring a backup host pool ” on page 21.
4	Configure the SLP to use snapshot and replication	For more details about replication, refer these chapters in the *NetBackup™ Snapshot Manager for Data Center Administrator's Guide*: ■ Storage array replication ■ Configuring storage lifecycle policies for snapshots and snapshot replication ■ Supported storage arrays in data center
5	Configure a NAS-Data-Protection policy to perform the operations that are specified in the SLP	See “Setting up a NAS-Data-Protection policy ” on page 24.

Chapter 7

Restoring from D-NAS backups

This chapter includes the following topics:

- Restoring from D-NAS backups
- Original location restores for D-NAS Policy
- Point in time rollback

Restoring from D-NAS backups

You can use the Backup, Archive, and Restore interface to restore individual files or directories, or a volume.

Points to remember before restoring:

- Original location restore is not supported for NAS-Data-Protection policy.
- The destination client for restore must be a NetBackup host. For example, a media server or backup host.
- If you select either of the following rename options, ensure that you change the destination path:
  - Rename hard links
  - Rename soft links

Original location restores for D-NAS Policy

Even though the **Restore everything to its original location** option is disabled for D-NAS policy, it is possible to restore data to the original location. Use the following methods:

- **NFS Shares**: Manually mount the NFS share to one of the NetBackup hosts. Use that host as the destination client and the mount path as the destination location.
- **SMB Shares**: Specify the UNC path of the SMB share as the destination and one of the NetBackup hosts as the destination client. For example: `\\<IP or FQDN>\<SMB_Share_Name>\<Dest>`

Restore data backed up using D-NAS policy:

1. Start the Backup, Archive, and Restore interface.
2. Click the **Restore Files** tab.
3. Click **Actions > Specify NetBackup Machines** to specify the server, source client, policy type, and destination client.
4. For the Restore Type, select **Point in Time Rollback**.

   The Browse directory field should be root (/).
5. Click **Restore**.
6. In the **General** > **Destination** option, select the mount point in the option **Restore everything to a different location (maintaining existing structure)**
7. (Optional) To overwrite the original data, select **Overwrite existing files**.

   Check restore progress in the Task progress tab in the Backup, Archive, and Restore interface or the Activity Monitor.

Point in time rollback

You can also restore a snapshot of an entire file system or volume with minimal I/O. This type of restore is called point in time rollback. All the data in the snapshot is restored; single file restore is not available in a rollback.

Warning: Rollback deletes all files that were created after the creation-date of the snapshot that you restore. Rollback returns a file system or volume to a given point in time. Any data changes or snapshots that were made after that time are lost.

Also, if there are multiple logical volumes on a single disk or volume group and if you perform a Point in Time Rollback of a specific logical volume, the entire disk or volume group is restored to the point in time.

Rollback is available only when you restore the file system or volume to the original location on the client.

Performing rollback using snapshot:

1. Start the Backup, Archive, and Restore interface.
2. Click the **Restore Files** tab.
3. Click **Actions** > **Specify NetBackup Machines** to specify the server, source client, policy type, and destination client.
4. For **Restore Type**, select **Point in Time Rollback**.

   The Browse directory field is grayed out, with root (/) as default.

   Instant Recovery backups are displayed in the **Backup History** window, for all dates (you cannot set a range).
5. Select an image from the list, and click **OK**.

   The image contents are displayed in the **Directory Structure** pane of the **Restore Files** tab.
6. Select a volume for rollback, click **Restore**.

Chapter 8

Troubleshooting

This chapter includes the following topics:

- Troubleshooting
- Setting the log level
- Logging directories for Linux platforms
- Logging folders for Windows platforms
- Restore from a snapshot fails with status 133
- Backup from snapshot fails with error 50
- Backup from snapshot parent job fails with error 4213: Snapshot import failed
- Backup host pool creation fails with the error "Failed to fetch host list"
- Snapshot job fails and the snapshot command does not recognize the volume name
- Accelerator enabled incremental backup of NetApp NAS volume
- Snapshot method: Auto

Troubleshooting

You can resolve many problems on your own by creating logging directories, reproducing the problem, and checking the logs. For an in-depth description of NetBackup logs, refer to the *NetBackup Troubleshooting Guide*.

For explanations of NetBackup job status codes, refer to the *NetBackup Status codes Reference Guide.*

Setting the log level

To create detailed log information, place a *VERBOSE* entry in the `bp.conf` file on the NetBackup primary and client server. Alternatively, set the Global logging level to a high value in the **Logging** dialog, under both **Master Server Properties** and **Client Properties**.

These directories can eventually require a lot of disk space. Delete them when you are finished troubleshooting and remove the *VERBOSE* option from the `bp.conf` file. Alternatively, reset the Global logging level to a lower value.

Logging directories for Linux platforms

To create logging directories use the `/usr/openv/netbackup/logs/mklogdir` script. You can also create the directories using an access mode of 755 so NetBackup can write to the logs.

Table 8-1 Linux logging directories for snapshot operation

Path of log directory	Where to create the directory
`/usr/openv/netbackup/logs/bprd`	NetBackup primary server
`/usr/openv/logs/nbjm`	NetBackup primary server
`/usr/openv/netbackup/logs/bpbrm`	NetBackup media server
`/usr/openv/netbackup/logs/bpfis`	NetBackup backup host client

Table 8-2 Linux logging directories for backup operation

Path of log directory	Where folder is created
`/usr/openv/netbackup/logs/bprd`	NetBackup primary server
`/usr/openv/logs/nbjm`	NetBackup primary server
`/usr/openv/logs/nbstserv`	NetBackup primary server
`/usr/openv/netbackup/logs/bpdbm`	NetBackup primary server
`/usr/openv/netbackup/logs/bptm`	NetBackup media server
`/usr/openv/netbackup/logs/bpbrm`	NetBackup media server

Table 8-2 Linux logging directories for backup operation *(continued)*

Path of log directory	Where folder is created
/usr/openv/netbackup/logs/bpfis	NetBackup backup host client
/usr/openv/netbackup/logs/bppfi	NetBackup backup host client
/usr/openv/netbackup/logs/bpbkar	NetBackup backup host client
/usr/openv/logs/ncfnbcs	NetBackup backup host client

Table 8-3 Linux logging directories for index from operation

Path of log directory	Where folder is created
/usr/openv/netbackup/logs/bprd	NetBackup primary server
/usr/openv/logs/nbjm	NetBackup primary server
/usr/openv/logs/bpdbm	NetBackup primary server
/usr/openv/netbackup/logs/bptm	NetBackup primary server
/usr/openv/netbackup/logs/bpbrm	NetBackup media server
/usr/openv/netbackup/logs/bpcd	NetBackup backup host client
/usr/openv/netbackup/logs/bppfi	NetBackup backup host client
/usr/openv/logs/ncfnbcs	NetBackup backup host client

Table 8-4 Linux logging directories for single file restore from snapshot copy

Path of log directory	Where folder is created
/usr/openv/netbackup/logs/bprd	NetBackup primary server
/usr/openv/logs/bpbrm	NetBackup primary server

Table 8-4 Linux logging directories for single file restore from snapshot copy *(continued)*

Path of log directory	Where folder is created
/usr/openv/netbackup/logs/bpcd	Restore host client
/usr/openv/netbackup/logs/bpbkar	Restore host client
/usr/openv/netbackup/logs/bpfis	Restore host client
/usr/openv/netbackup/logs/bppfi	Restore host client
/usr/openv/logs/tar	Destination client where the files are restored.

Table 8-5 Linux logging directories for point-in-time rollback

Path of log directory	Where folder is created
/usr/openv/netbackup/logs/bprd	NetBackup primary server
/usr/openv/nebackup/logs/bpbrm	NetBackup primary server
/usr/openv/netbackup/logs/bpcd	Restore host client
/usr/openv/netbackup/logs/bpbkar	Restore host client
/usr/openv/netbackup/logs/bpfis	Restore host client
/usr/openv/netbackup/logs/bppfi	Restore host client

Table 8-6 Linux logging directories for create replication operation

Path of log directory	Where folder is created
/usr/openv/logs/nbjm	NetBackup primary server
/usr/openv/logs/nbstserv	NetBackup primary server
/usr/openv/logs/nbrb	NetBackup primary server
/usr/openv/netbackup/logs/bpdm	NetBackup media server

Table 8-7 Linux logging directories for delete replication operation

Path of log directory	Where folder is created
`/usr/openv/netbackup/logs/bpdm`	NetBackup media server
`/usr/openv/netbackup/logs/admin`	NetBackup media server (for `bppficorr` logs)

Logging folders for Windows platforms

Table 8-8 Windows logging directories for snapshot operation

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bprd`	NetBackup primary server
`install_path\NetBackup\logs\nbjm`	NetBackup primary server
`install_path\NetBackup\logs\bpbrm`	NetBackup primary server if Instant Recovery backup is set to snapshot only; otherwise, on media server
`install_path\NetBackup\logs\bpfis`	Backup host client

Table 8-9 Windows logging directories for backup operation

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bprd`	NetBackup primary server
`install_path\NetBackup\logs\nbjm`	NetBackup primary server
`install_path\NetBackup\logs\nbstserv`	NetBackup primary server
`install_path\NetBackup\logs\bpdbm`	NetBackup primary server
`install_path\NetBackup\logs\bptm`	NetBackup primary server
`install_path\NetBackup\logs\bpbrm`	NetBackup primary server
`install_path\NetBackup\logs\bpfis`	Backup host client
`install_path\NetBackup\logs\bppfi`	Backup host client
`install_path\NetBackup\logs\bpbkar`	Backup host client

Table 8-9 Windows logging directories for backup operation *(continued)*

Path of log directory	Where folder is created
`install_path\NetBackup\logs\ncfnbcs`	Backup host client

Table 8-10 Windows logging directories for index from snapshot operation

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bprd`	NetBackup primary server
`install_path\NetBackup\logs\nbjm`	NetBackup primary server
`install_path\NetBackup\logs\bpdbm`	NetBackup primary server
`install_path\NetBackup\logs\bptm`	NetBackup primary server
`install_path\NetBackup\logs\bpbrm`	NetBackup primary server
`install_path\NetBackup\logs\bpcd`	Backup host client
`install_path\NetBackup\logs\bppfi`	Backup host client
`install_path\NetBackup\logs\ncfnbcs`	Backup host client

Table 8-11 Windows logging directories for single file restore from snapshot copy

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bprd`	NetBackup primary server
`install_path\NetBackup\logs\bpbrm`	NetBackup primary server
`install_path\NetBackup\logs\bpcd`	Remote host client
`install_path\NetBackup\logs\bpbkar`	Remote host client
`install_path\NetBackup\logs\bpfis`	Remote host client
`install_path\NetBackup\logs\bppfi`	Remote host client
`install_path\NetBackup\logs\tar`	Destination client where the files are restored.

Table 8-12 Windows logging directories for single file restore from point in time rollback

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bprd`	NetBackup primary server
`install_path\NetBackup\logs\bpbrm`	NetBackup primary server
`install_path\NetBackup\logs\bpcd`	Remote host client
`install_path\NetBackup\logs\bpbkar`	Remote host client
`install_path\NetBackup\logs\bpfis`	Remote host client
`install_path\NetBackup\logs\bppfi`	Remote host client

Table 8-13 Windows logging directories for single file restore from create replication operation

Path of log directory	Where folder is created
`install_path\NetBackup\logs\nbjm`	NetBackup primary server
`install_path\NetBackup\logs\nbstserv`	NetBackup primary server
`install_path\NetBackup\logs\nbrb`	NetBackup primary server Remote host client
`install_path\NetBackup\logs\bpdm`	NetBackup media server

Table 8-14 Windows logging directories for single file restore from delete replication operation

Path of log directory	Where folder is created
`install_path\NetBackup\logs\bpdm`	NetBackup media server
`install_path\NetBackup\logs\admin`	NetBackup media server (for `bppficorr` logs)

Restore from a snapshot fails with status 133

Restore from snapshot fails with status code 133 and displays the Invalid request message.

Explanation

The restore fails, if you select a path other than the path mentioned in the backup selection.

For example, say the backup selection contains `/ifs/vol1/parent/dir1`. During a restore if you select only `/ifs/vol1/parent`, which is the parent directory of the path mentioned for backup selection, the restore fails with status code 133.

Workaround

For a successful restore from the snapshot copy, you must select the original path mentioned in the **Backup elections** tab, that is `/ifs/vol1/parent/dir1` or the sub-directory or file inside the backup selection.

Backup from snapshot fails with error 50

This error occurs when the NetBackup Client and NetBackup Legacy Network services are not restarted properly after configuration for the domain user.

Explanation

This error occurs when the NetBackup Client and NetBackup Legacy Network services are not restarted properly after configuration for the domain user.

Workaround

If you are using master or media as backup host then follow these steps to troubleshoot:

1. Stop all NetBackup services using the `bpdown.exe`.
2. Logon to the NetBackup Client and NetBackup Legacy Network services as the domain user. But, do not start these services immediately after logon.
3. Start all the services together using `bpup.exe`.

Backup from snapshot parent job fails with error 4213: Snapshot import failed

Job details shows an error like:

"Snapshot export failed. Failed to export share: data_lif is not online. Please check data_lif status on vserver: VSERVER_1."

where, VSERVER_1 is the vserver that is offline.

Explanation:

For a NAS-Data-Protection policy, all the vservers are listed in the client's section of the policy, irrespective of their state. So, you are able to include backup selection

from offline SVM, and policy validation succeeds. However, at the time of backup-from-snapshot, export operation for those shares fails if the corresponding vserver is offline.

Workaround

To overcome this error, check the status of the vserver and whether that vserver is reachable. Whenever client and vserver connection is established, SLP retry is successful.

Backup host pool creation fails with the error "Failed to fetch host list"

Explanation:

This issue appears if the NetBackup services are not started properly, with the domain user.

Workaround:

1. Make sure that the NetBackup client service is running.
2. Log on as the domain user to the NetBackup client service.
3. Restart the NetBackup Client service.
4. Make sure that the NetBackup network legacy service is running.
5. Log on as the domain user to the NetBackup network legacy service.
6. Restart the NetBackup network legacy service.
7. Make sure that all NetBackup services are running.
8. Relaunch the NetBackup UI.

Snapshot job fails and the snapshot command does not recognize the volume name

Explanation:

A snapshot job fails if the volume name exceeds 15 characters.

When you create and name a volume, a prefix or a suffix is added to the volume name. If the volume name contains more than 15 characters, addition of prefix or suffix may make the volume name exceed the limit of 27 characters. When you run the `vxassist snapshot`, command, it does not recognize the lengthy snapshot volume name and the snapshot job fails.

For example, if the primary volume name is **PFItest123456789vol** and the suffix *00043c8aaa* is added to it, the volume name exceeds the limit. The command `vxassist snapshot` does not recognize the name *PFItest123456789vol_00043c8aaa* and the snapshot job fails.

Workaround:

Veritas recommended that you limit the primary volume names to up to 15 characters to create the VxVM mirror snapshots.

Accelerator enabled incremental backup of NetApp NAS volume

Accelerator enabled NAS-Data-Protection policy backups complete volume instead of only the incremental data. This also affects the run optimization.

This issue occurs under the following conditions:

- The policy type is NAS-Data-Protection.
- In the policy's Snapshot options, the value of Access Protocol is Default or NFS3.
- Backup selection has NetApp NAS volumes.

The Accelerator technology optimizes a backup by sending only changed blocks over a network for backup. A two-step process is used to identify the changed files and changed blocks in these files. File attributes and index node (inode) are the key parameters to identify a change. If the files are accessed over NFS version 3, a file on NetApp NAS volume behaves different because of the inode numbers. Same file has different inode numbers across snapshots of the volume if accessed over NFS3. All schedules of backup are based on the snapshot that is created for the run of the policy. A new snapshot with different inode numbers than the previous ones makes accelerator to identify these files as new files. Because of this issue, all files are backed up instead of incremental data only.

To resolve this issue, avoid using NFS version 3 to access the snapshot for accelerator-enabled backups. You can change the Access Protocol to NFS4 for the affected policy. For more details, refer to the NetApp documentation.

Snapshot method: Auto

Error scenario 1: Policy validation fails, after a primary server upgrade, if you create a policy with VSO FIM for older clients and select Snapshot Method as Auto in the NetBackup 10.0 UI.

Error scenario 2: Snapshot jobs fail, if you configure DNAS policy with backup host pool containing older version backup hosts and select Snapshot Method as Auto in the NetBackup 10.0 UI.

The Snapshot Method, Auto is supported only in NetBackup 10.0 onwards. If your environment contains older version backup hosts, select another snapshot method.