HP D2D NAS
Integration with CommVault Simpana® 9

Abstract

This guide provides step by step instructions on how to configure and optimize CommVault Simpana 9 in order to back up to HP StorageWorks D2D devices using a CIFS backup target.

HP Part Number: EH985-90934
Published: February 2011
Edition: 1

Contents

1 Introduction

CommVault Simpana 9® is an Enterprise Data Protection, Archiving and Content indexing software solution that works with a wide selection of disk storage devices, physical tape libraries and even Cloud services. The latest edition (V 9.0) also supports client–side deduplication as a licensable feature.

This implementation guide focuses on the usage model where CommVault deduplication on the media server or Client is disabled and the deduplication is performed entirely on the D2D NAS device using the HP StoreOnce deduplication engine. This approach is known as target-based deduplication.

The objective of this Implementation Guide is:

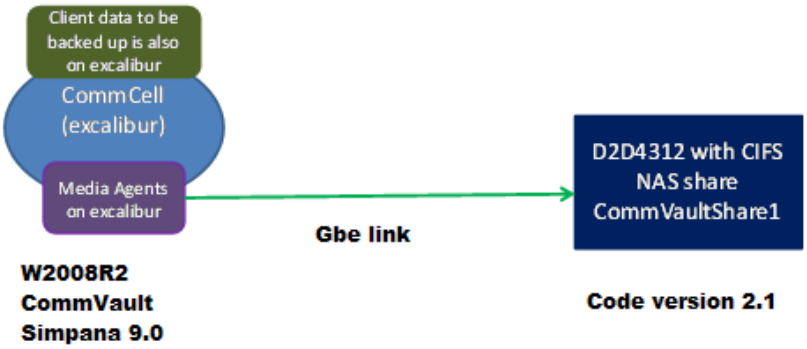
- To provide step by step instructions on configuring a D2D NAS CIFS device on CommVault Simpana 9.0
- To describe the CommVault Simpana 9.0 Disk Library configuration options and identify what settings to use with HP D2D NAS CIFS shares.
- To describe how to implement a full end–to–end recovery solution from a target D2D device with D2D NAS CIFS shares using CommVault Simpana 9.0 in two common scenarios.

Configuration Setup

For CommVault terminology used in this document please refer to Appendix A.

This guide assumes a basic working knowledge of CommVault Simpana 9.0 and that it has been installed correctly by loading the appropriate Media Agents and licences.

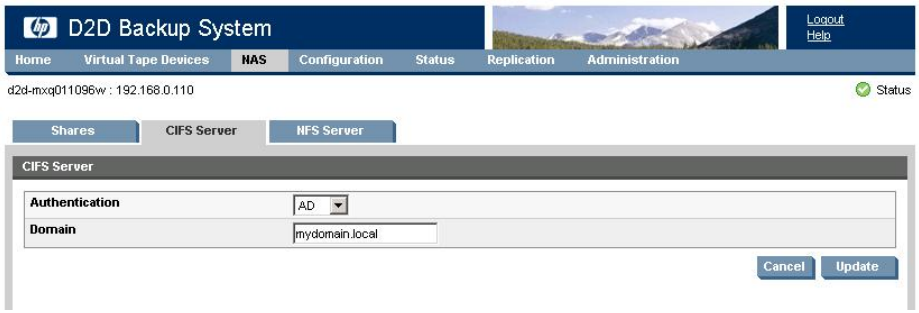
Figure 1 Configuration overview



2 Configure the D2D CIFS server

The first step in configuring the D2D device as a target for backups from CommVault Simpana 9.0 is to configure the CIFS server on the D2D Backup System

On the D2D Web Management Interface navigate to the **NAS — CIFS Server** page and select **Edit**.



The available Authentication options for the CIFS server are:

- **None** – All shares created are accessible to any user from any client (this is the least secure option)
- **User** – Local (D2D) User account authentication
- **AD** – Active Directory User account authentication

More about authentication modes

None: This authentication mode requires no username or password authentication and is the simplest configuration. CommVault will always be able to use shares configured in this mode with no changes to either server or CommVault configuration. However, this mode provides no data security because anyone can access the shares and add or delete data.

User: In this mode it is possible to create "local D2D users" from the D2D Web Management Interface. This mode requires the configuration of a respective local user on the CommVault media server and configuration changes to the CommVault services. Individual users can then be assigned access to individual shares on the D2D Backup System. This authentication mode is ONLY recommended when the CommVault media server is not a member of an AD Domain.

AD: In this mode the D2D CIFS server becomes a member of an Active Directory Domain. In order to join an AD domain the user needs to provide credentials of a user who has permission to add computers and users to the AD domain. After joining an AD Domain access to each share is controlled by Domain Management tools and domain users or groups can be given access to individual shares on the D2D Backup System. This is the recommended authentication mode, if the CommVault Media server is a member of an AD domain.

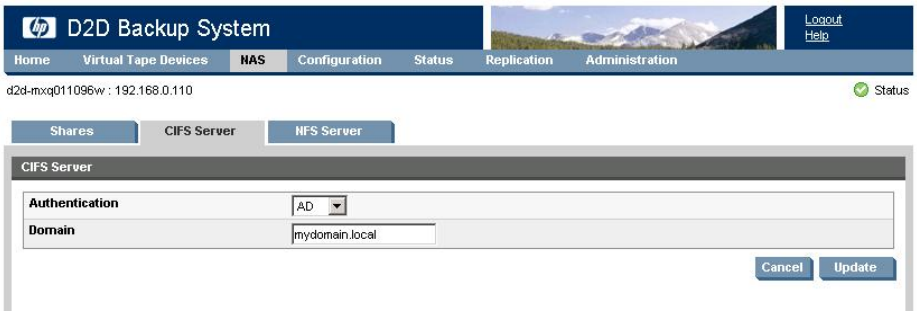
Configuring AD Authentication Mode

These are the steps required in order to configure backups in AD authentication mode:

- Join the D2D CIFS server to the AD Domain and configure DNS.
- Create or specify a user to be used for backups.
- Apply user permissions to D2D shares.
- Configure CommVault to use the correct Domain account.

To join a domain

1. Connect to the D2D Web Management Interface, navigate to the **NAS — CIFS Server** page, click **Edit** and choose **AD** from the drop-down menu. Provide the name of the domain that you wish to join, e.g “mydomain.local”



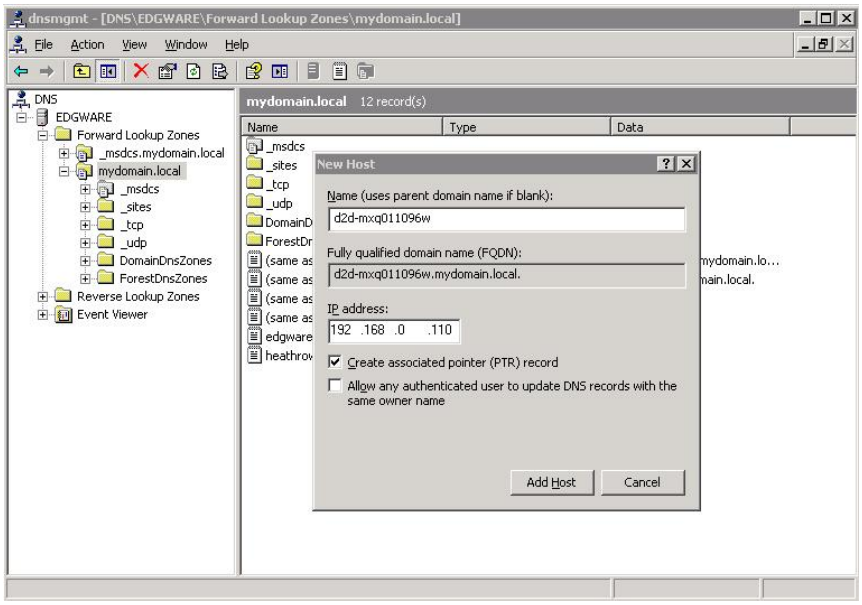
2. Click **Update**. If the domain controller is found, a pop-up box will request credentials of a user with permission to join the domain. (Note that joining or leaving the domain will result in failure of any backup or restore operations that are currently running.) Provide credentials (username and password) of a domain user that has permission to add computers to the domain and click **Register**.

3. After joining the domain, the DNS server should be automatically updated (if a DHCP server is used) with Forward and Reverse Lookup zone entries, however, some DNS configurations do not allow this. In this case, or if a DHCP is not used on the network, the user must also configure the domain's DNS server to be able to correctly manage the D2D shares, as described in the next section.

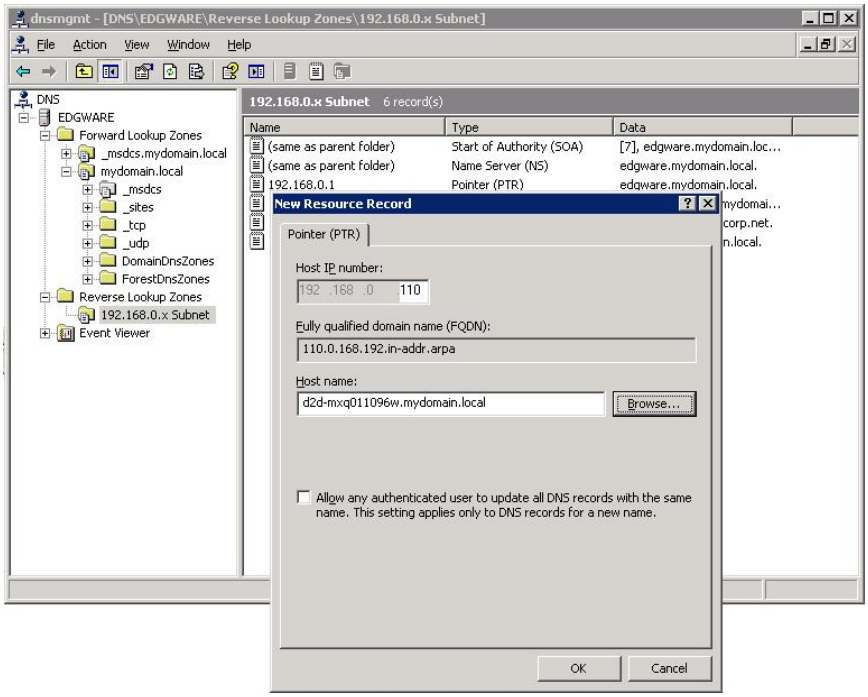
   To configure entries manually if the DNS server does not update automatically

   From a Windows client server that has domain and DNS management tools installed launch the DNS Management Tool. (From the command line type `dnsmgmt.msc` or launch DNS from the Administrative Tools menu).

   Create a new Host(A) record in the forward lookup zone for the domain to which the D2D Backup System belongs with the hostname and IP address of the D2D Backup System.



   Also create a Pointer(PTR) in the reverse lookup zone for the domain for the D2D Backup System by providing the hostname and IP address.

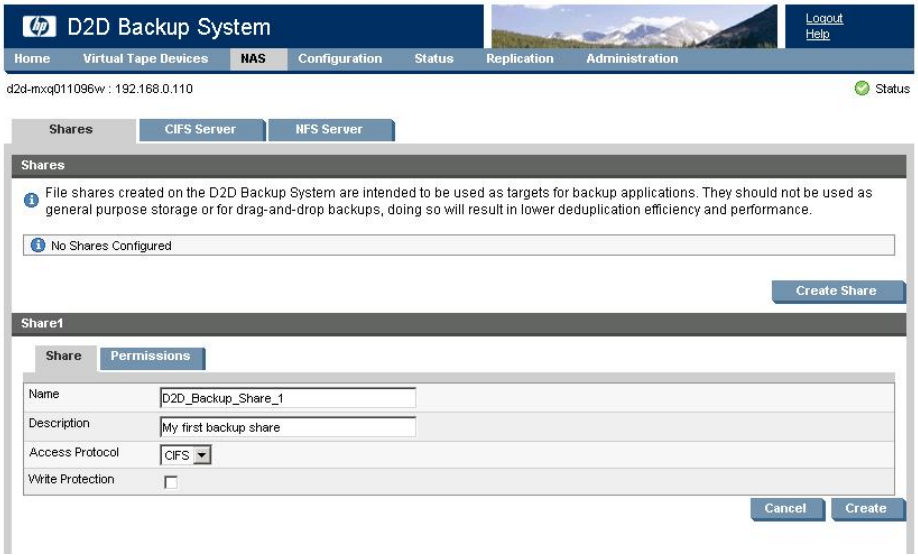


To create shares and grant access permission

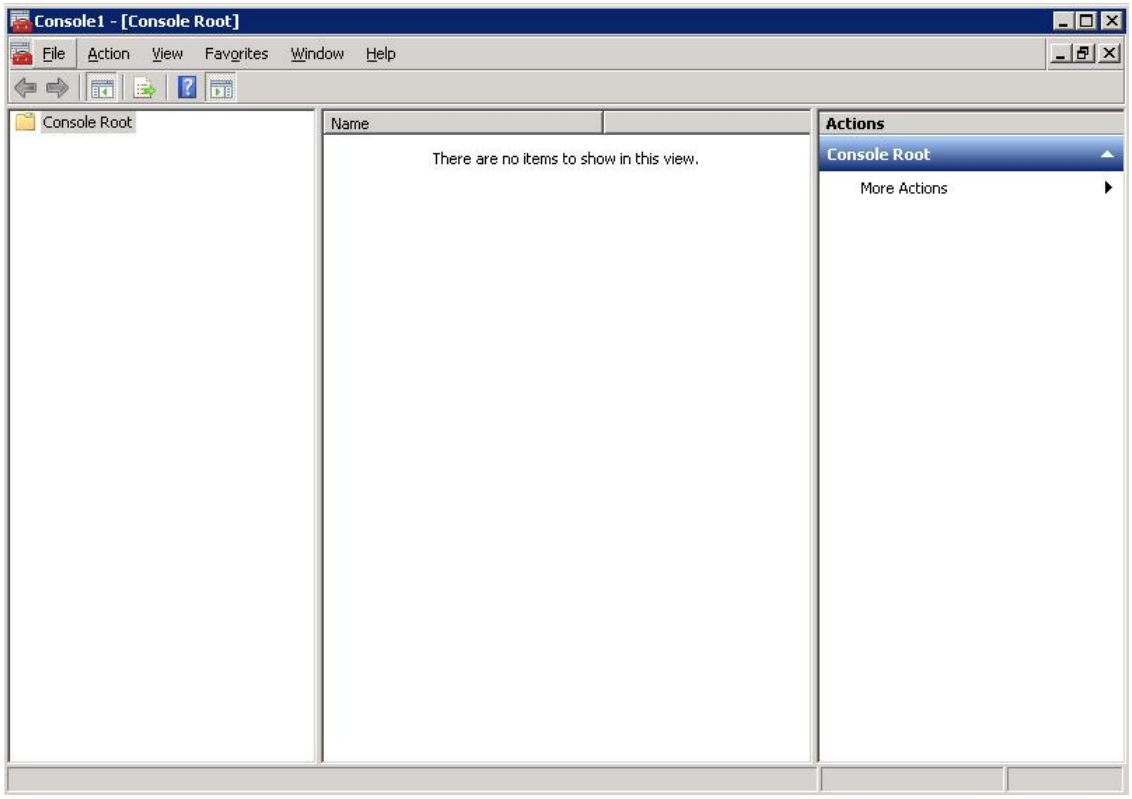
Now that the D2D Backup System is part of a domain and can be managed, it is possible to create shares and grant access permission to them for domain account users or groups.

1. Create a share on the D2D Backup System that is going to be used as a backup target, by selecting **NAS — Shares** from the D2D Web Management Interface and clicking **Create**.

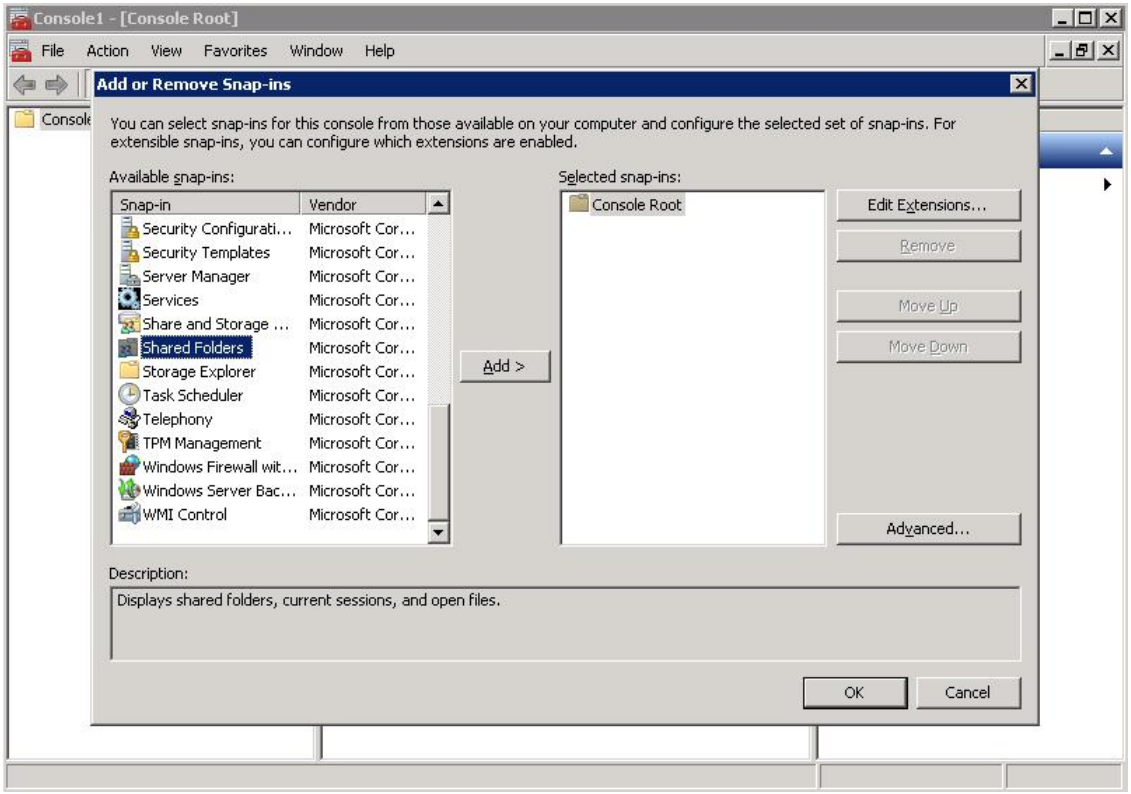
   Provide a share Name and Description, select the **CIFS** protocol and click **Create**.



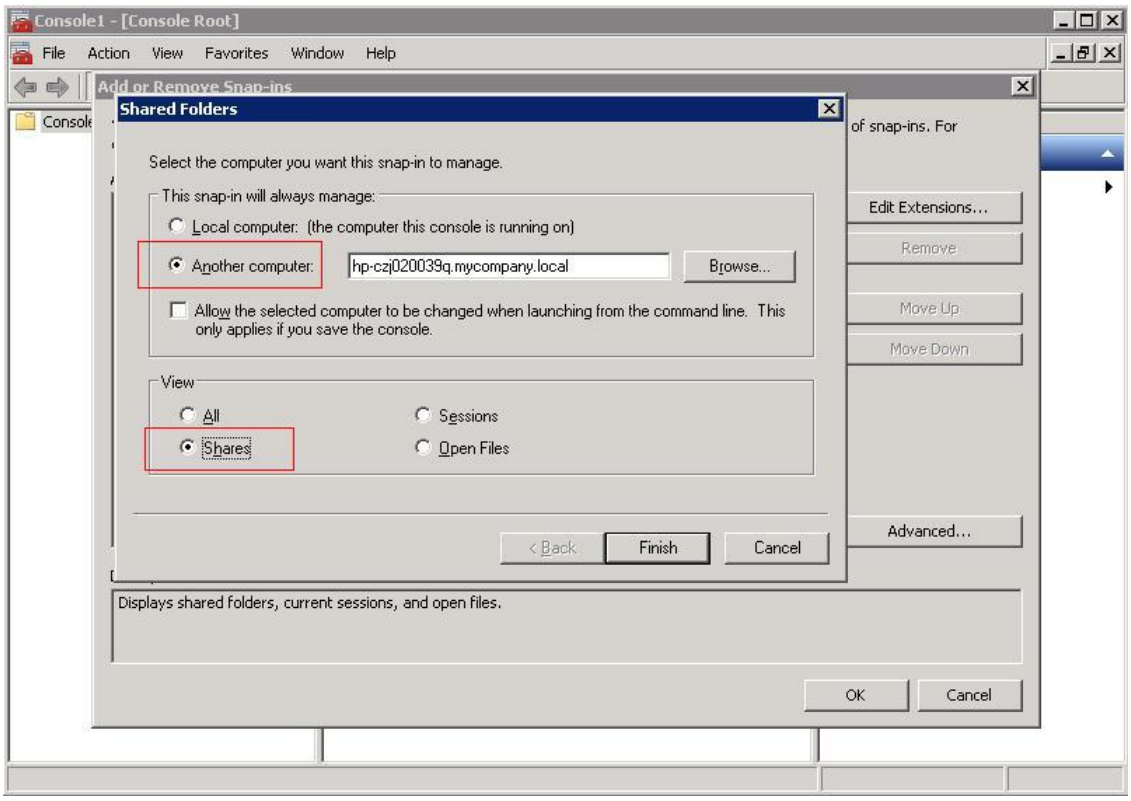
2. Now that the D2D Backup System is a member of the domain its shares can be managed from any computer on the domain by configuring a customized Microsoft Management Console (MMC) with the Shared Folders snap-in. To do this first open a new MMC window by typing `mmc` at the command prompt or from the Start Search box. This will launch a new empty MMC window.



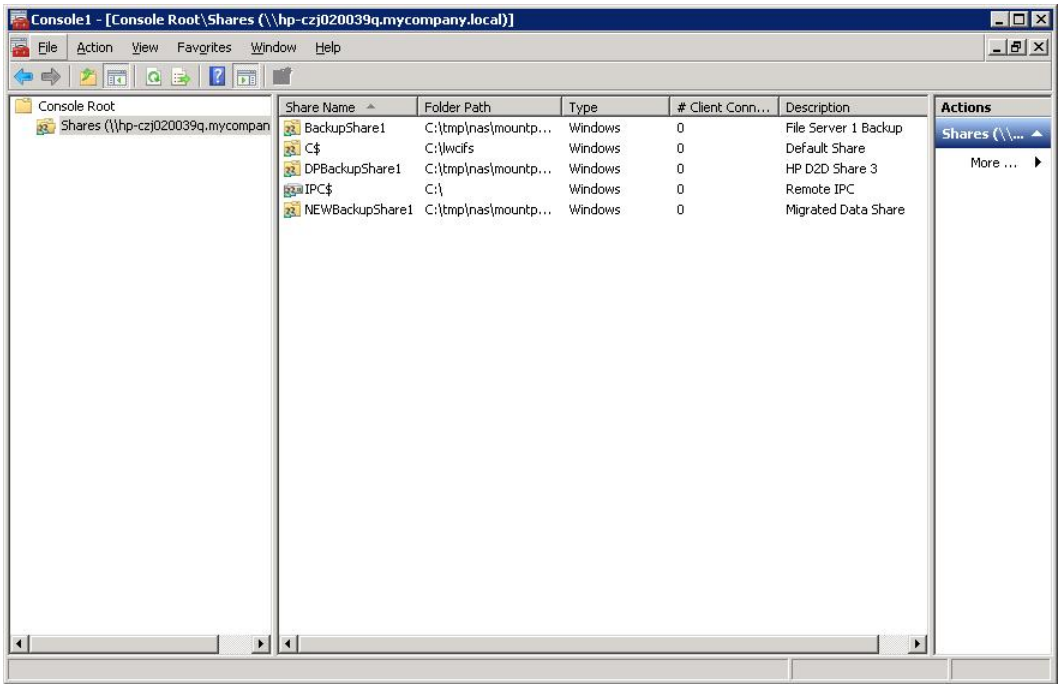
3. To this empty MMC window add the Shared Folders snap-in. Select **File — Add/Remove Snap-in ...,** then select **Shared Folders** from the left-hand pane.



4. Click **Add >** and in the dialog box choose **Another computer** to be managed and select **Shares** from the View options.



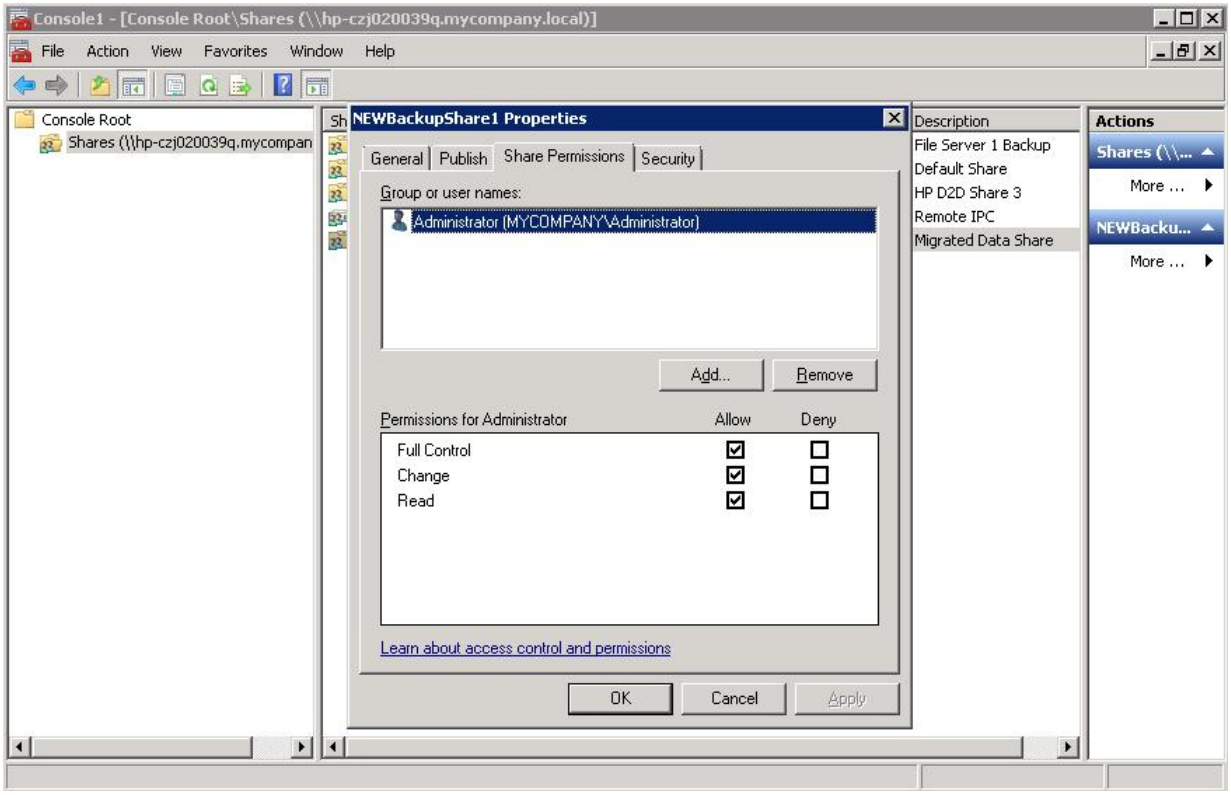
5. Click **Finish** and **OK** to complete the snap-in set up.



Note that the **Folder Path** field contains an internal path on the D2D Backup System.

6. Save this customized snap-in for future use.

7. Select the **Share Permissions** tab and **Add** a user or group of users from the domain. Specify the level of permission that the users will receive and click **Apply**.



8. Now, from any Windows server on the domain, it is possible to access the newly created share using the credentials of anyone who had been given permission to access the share. If a permitted user is logged into Windows, access to the share will be granted automatically with those permissions.

NOTE: In some cases, when switching the D2D Backup System from No Authentication or User Authentication mode to AD mode, it may be necessary to log out and back into a Windows client before it is possible to access the D2D shares.

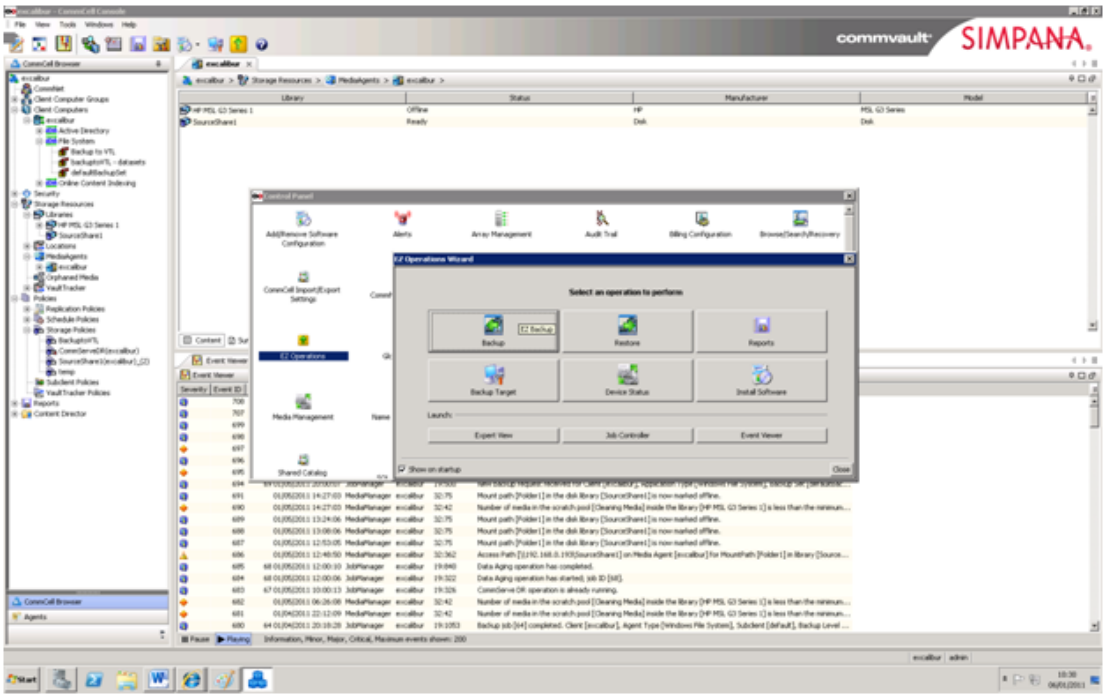
3 Discover the NAS CIFS share in CommVault

NOTE: In CommVault terminology the D2D NAS CIFS share is called a Disk Library.

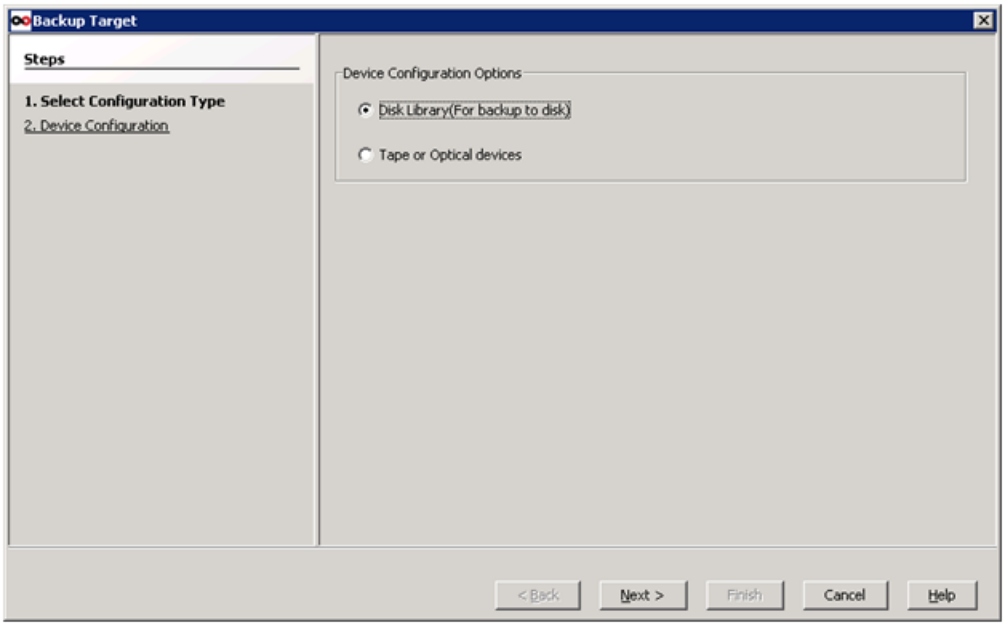
1. Run CommVault and enter your Domain Administrator user name and password. You must be the Domain Administrator because we have configured AD authentication for the CIFS server and the D2D NAS share is only visible to CommVault when it is administered by Active Directory.

   NOTE: Alternatively, you could configure User Authentication and add additional CommVault—based user names to the Share Access Permissions, but this is only recommended if the D2D Backup System is not in an AD domain.

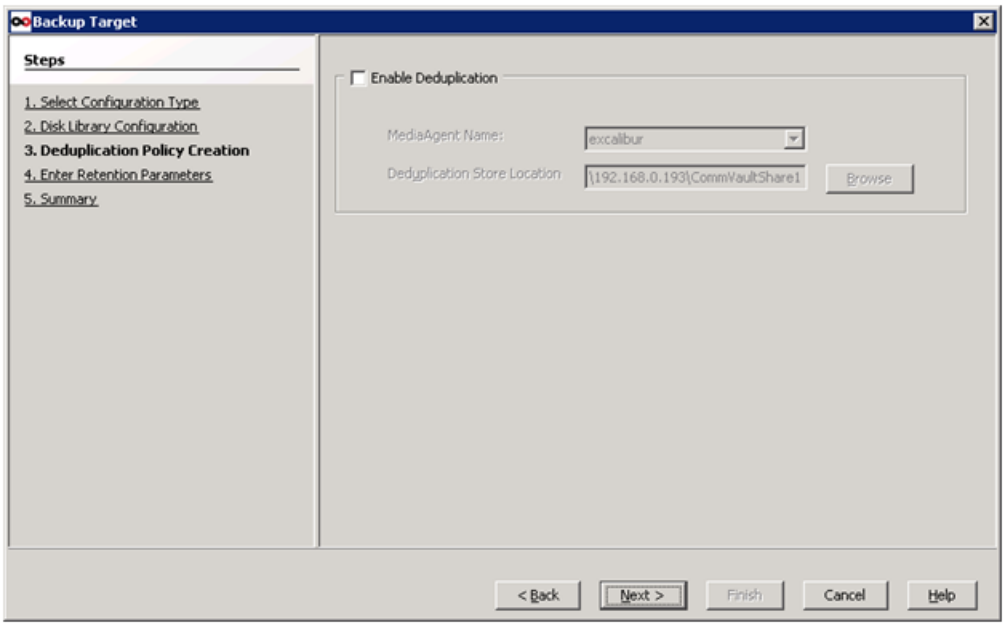
2. On the master screen click the control panel icon and select **EZ Operations**. On the EZ operations menu select **Backup Target**.



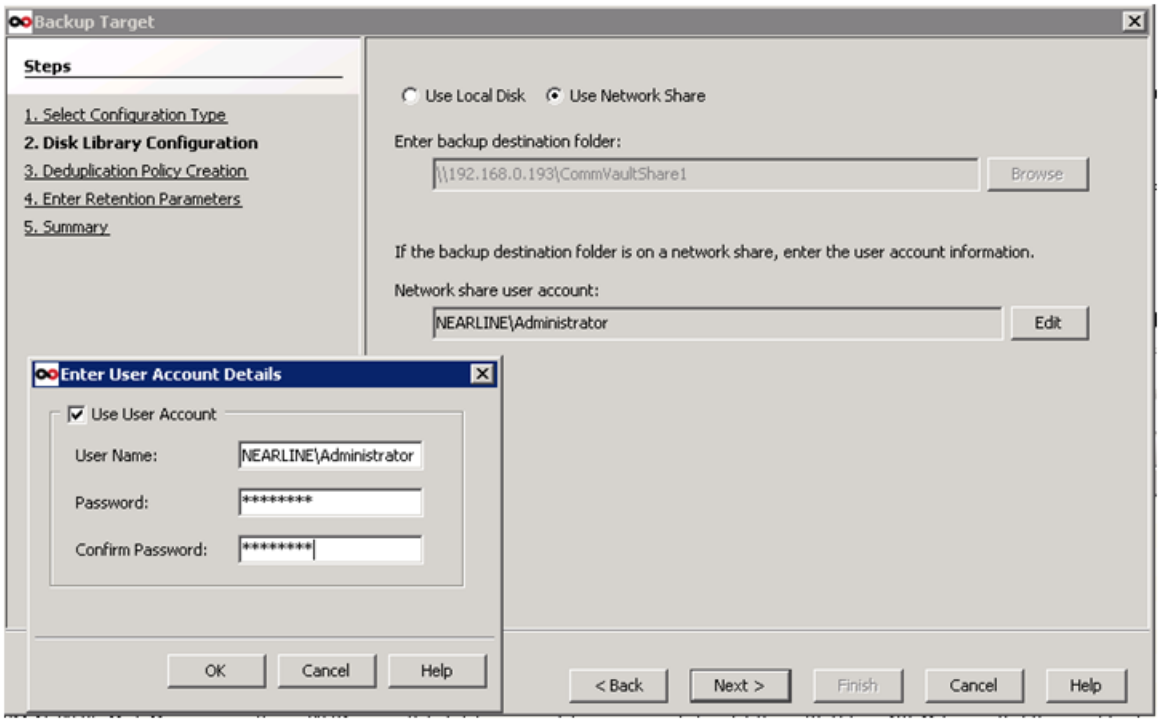
3. Select **Disk Library** and click **Next**.



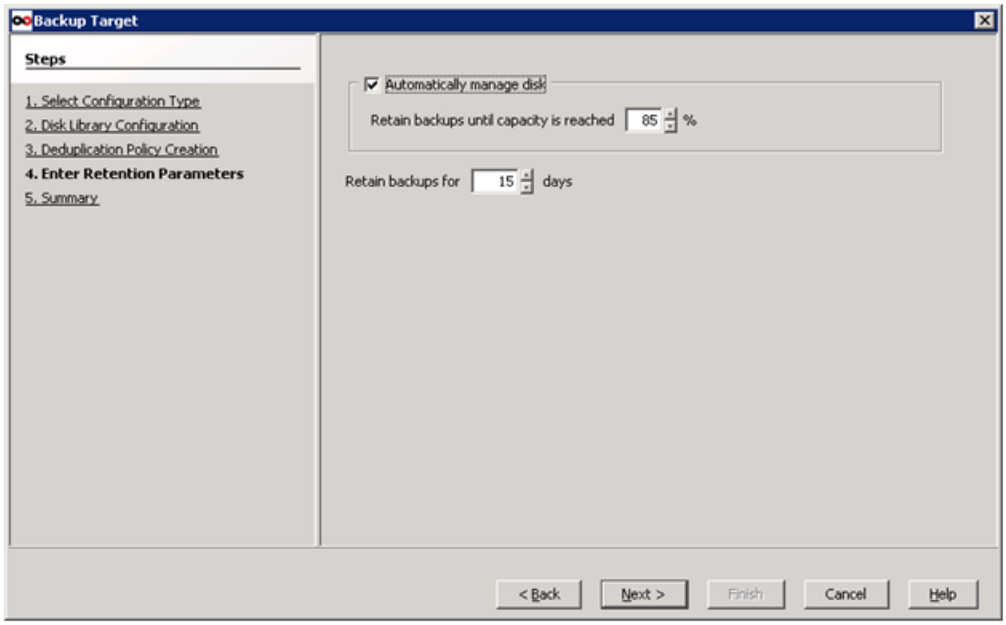
4. Enter the **Network Share** path (you can find this on the D2D NAS Shares tab). We are using AD authentication so there is no need to enter the network share user account details.
5. We do not want to enable CommVault Simpana Deduplication because we shall use the D2D NAS deduplication. Leave the box unchecked and click **Next**.



6. Enter the Domain Administrator User Name and Password for CommVault Simpana 9.0 to be able to access the share. This is required because we have set up Active Directory authentication.

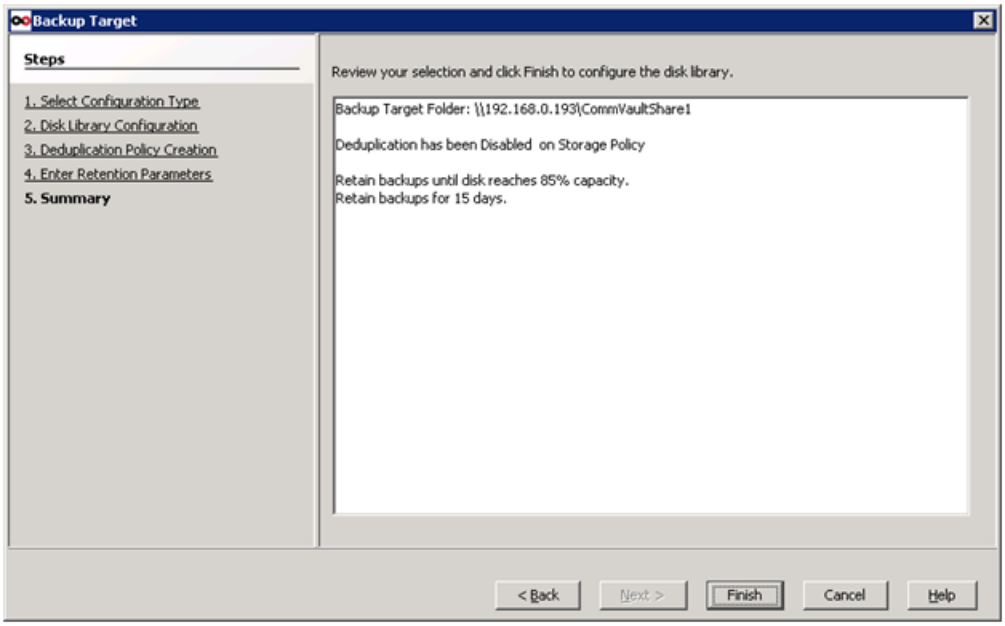


7. Accept the default settings for retention and click **Next**.



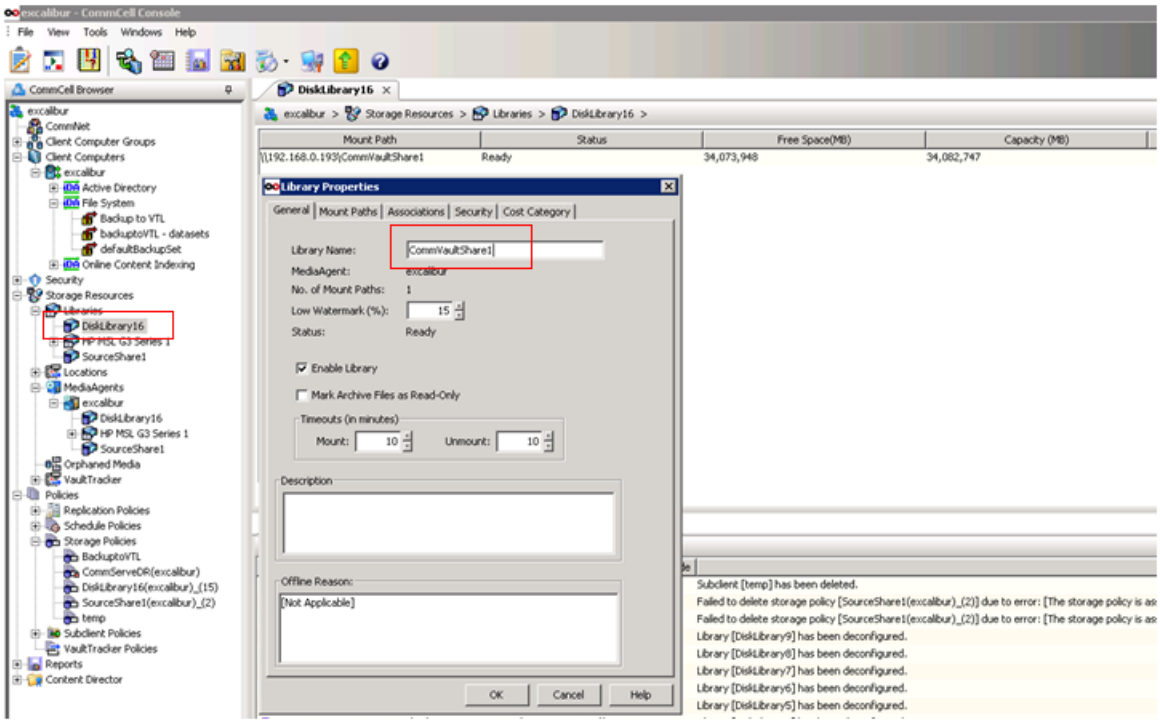
NOTE: Retain backups values (retention period) can be set here or later, from a configuration pane associated with the backup job.

8. Review the Summary screen and click **Finish**.


Backup Target
Steps
1. Select Configuration Type
2. Disk Library Configuration
3. Deduplication Policy Creation
4. Enter Retention Parameters
5. Summary
Review your selection and click Finish to configure the disk library.
Backup Target Folder: \\192.168.0.193\CommVaultShare1
Deduplication has been Disabled on Storage Policy
Retain backups until disk reaches 85% capacity.
Retain backups for 15 days.
< Back
Next >
Finish
Cancel
Help

9. A popup screen should then indicate the Disk Library has been successfully created and on the main CommVault menu the device will appear as a Disk Library.

   Right click on the library (within the Storage Resources-Libraries folder) to display the Library Properties dialog. In our example, we are changing the library name on the General tab to something more meaningful (DiskLibrary16 to CommVaultShare1).

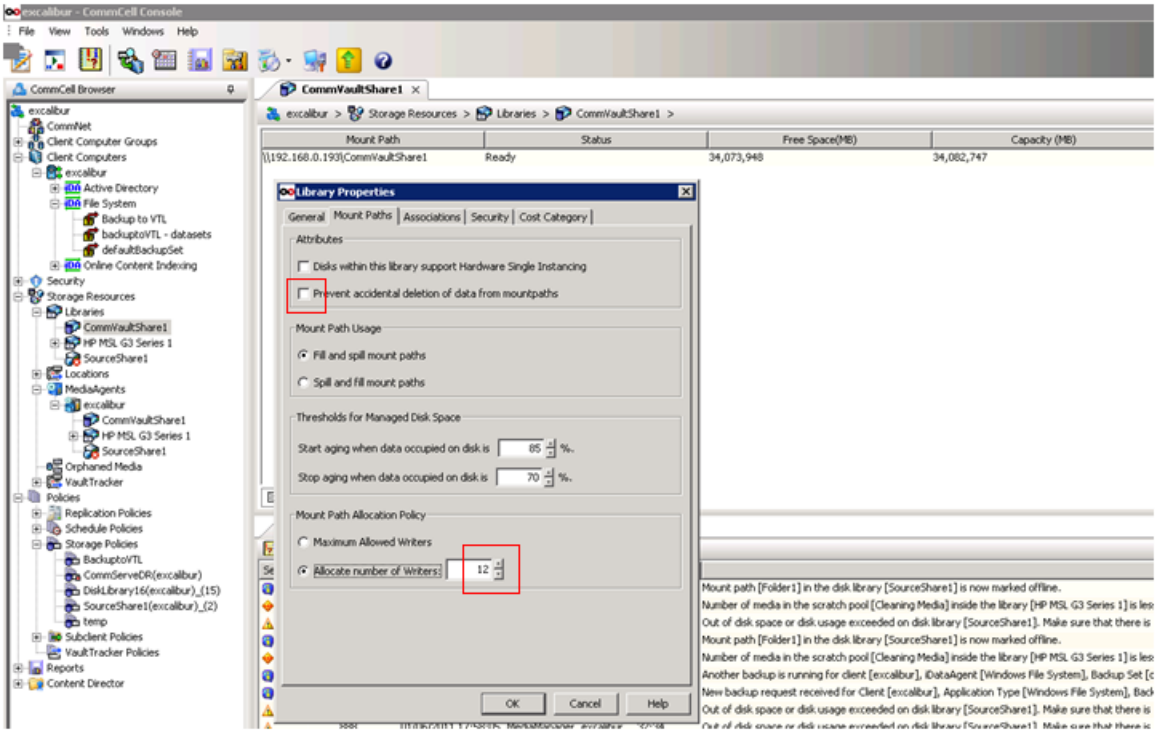


Mount Paths tab

A number of settings on this tab should also be edited.

The Attribute, **Prevent accidental deletion of data from mountpaths**, must be unchecked to allow operation.

The **Allocate number of Writers** value allows you to establish the maximum number of concurrent data protection operations on the disk library. HP recommends setting a specific number of writers per D2D NAS share dependent on the D2D Backup System. For example: the recommended setting is 12 for the HP D2D4312 Backup System. This value is set to ensure that the D2D NAS share does not exceed its maximum open file limit (see Appendix B). This setting is also dependent on the number of data streams set in the Storage Policy.



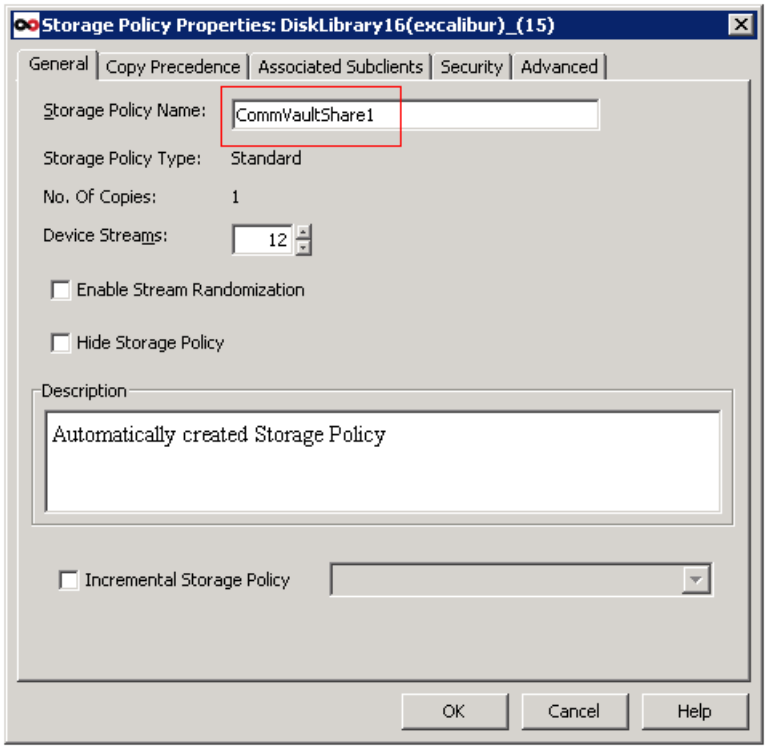
Storage policy

One or more default Storage Policies for the Disk Library have also been created (under the Policies—Storage Policies folder a default Storage Policy has been created for DiskLibrary16 (CommVaultShare1)). The exact number of policies will be different each time – depending on how many libraries have already been configured.

Right click on the Storage Policy to display the Properties dialog.

General tab

The number of Device Streams associated with this SINGLE policy is set on this tab.



Device Streams: Device streams must be spread across the number of storage policies that could run simultaneously to CommVaultShare1. In this case we plan to have only one storage policy to CommVaultShare1, so we can allocate 12 streams. What this means is that we could back up 12 hosts simultaneously to CommVaultShare 1 by setting **Device Streams** (General tab) and **Allocate number of writers** (Mount Paths tab) to 12.

Do not check **Enable Stream Randomization** because this will disrupt the deduplication efficiency of the HP D2D NAS share.

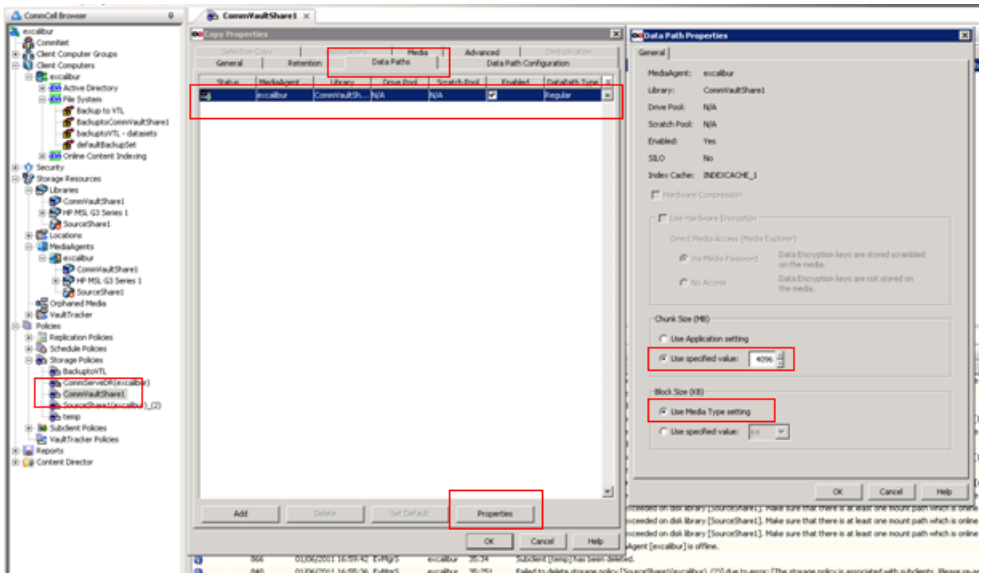
NOTE: If you are backing up multiple hosts, you may like to create separate folders for each host within the CommVaultShare1 library. Use Windows Explorer to do this.

Setting the Container/Chunk size

When using D2D NAS the CommVault backup software allocates a size to the containers (Chunks in CommVault terminology) where the user data files will be stored on the Disk Library. The size of these containers can be changed. D2D NAS has a fixed limit of 25000 files, so the larger we make the containers the more data we can hold on the D2D NAS share. Ideally, the bigger the containers the better as it stops us hitting the 25000 file limit and reduces fragmentation in the backup. Set the container (chunk) size as follows:

1. Select the Storage Policy that we have just created and double click the storage policy in the right—hand navigation window to get the Copy Properties window.
2. Click on the Data Paths tab in the Copy Properties window AND select the path.
3. Now click the **Properties** button at the bottom of the data paths page as shown below

   Edit the **Chunk size (MB)** section to use a specific value and click **OK**. In this case we will change the chunk size from 2048 (default) to 4096. The maximum chunk size is 32 GB, but this can lead to some performance impact so typically a choice of 16 GB chunk size is a good compromise.

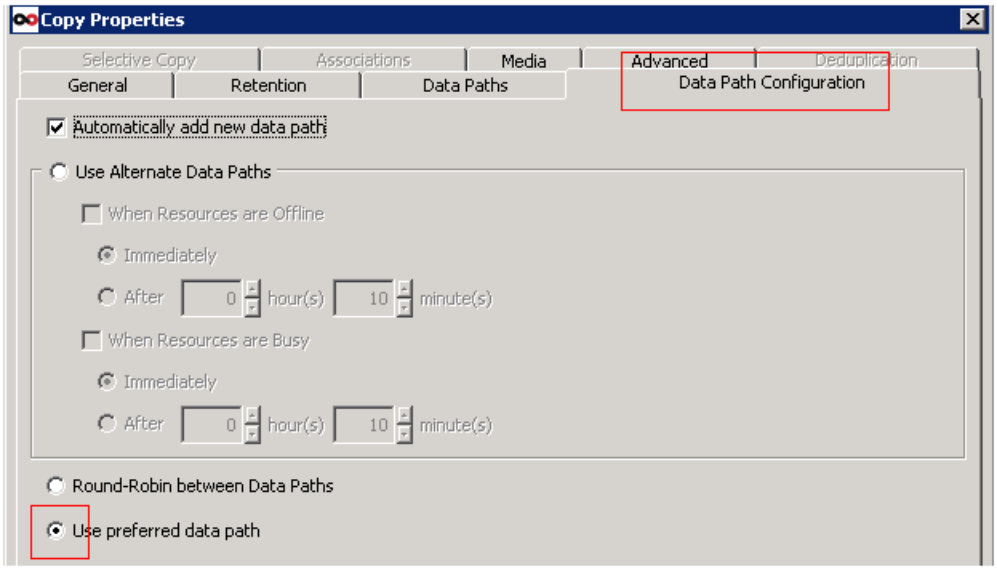


Block size: The Data Path Properties tab also has an option for block size. Leave this at the default which means it is set as appropriate for the media type.

- **Use media type setting** fixes the block size at 64K.
- **Use specific value** should take into account other considerations, see the information about VTL emulations in *Performance Tunables for Media Management* in CommVault Simpana 9.0 Books Online.

In general NAS share performance is much less affected by block size (unlike physical tape performance which is affected by block size).

4. Select the Data Path Configuration tab. By default, there are no alternative data paths created and we use the preferred data path. We do not use the round-robin between data paths which load balances backups across available disk libraries. These settings are important because we do not want to exceed the open files limits on the D2D NAS share (see later section).

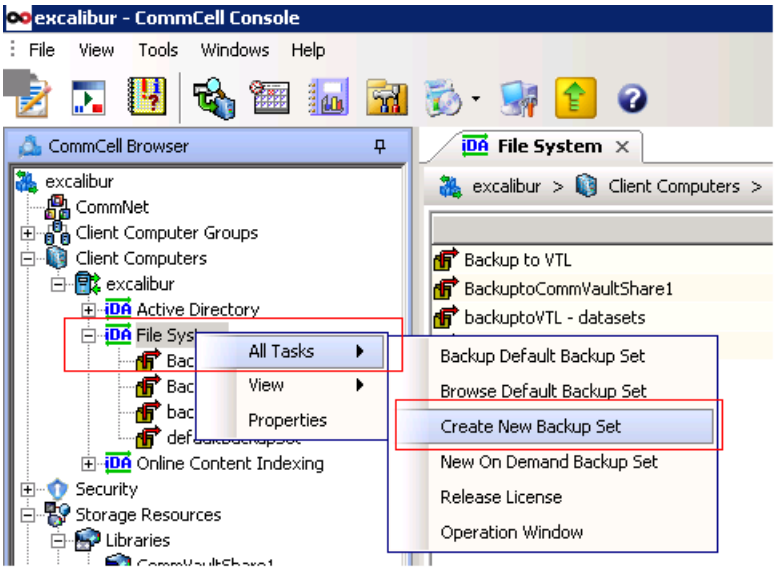


If additional Storage Policies are required use the Storage Policy creation wizard by right clicking Storage Policies in the main left-hand menu tree.

4 Backing up to and restoring from a D2D NAS Share

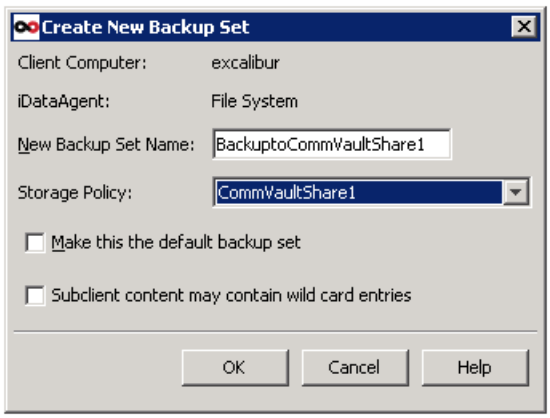
Configure a backup to the D2D NAS share

1. For a simple filesystem backup right click the File System icon in the left-hand navigation section of CommVault Simpana 9.0 and select **All Tasks — Create New Backup Set**,

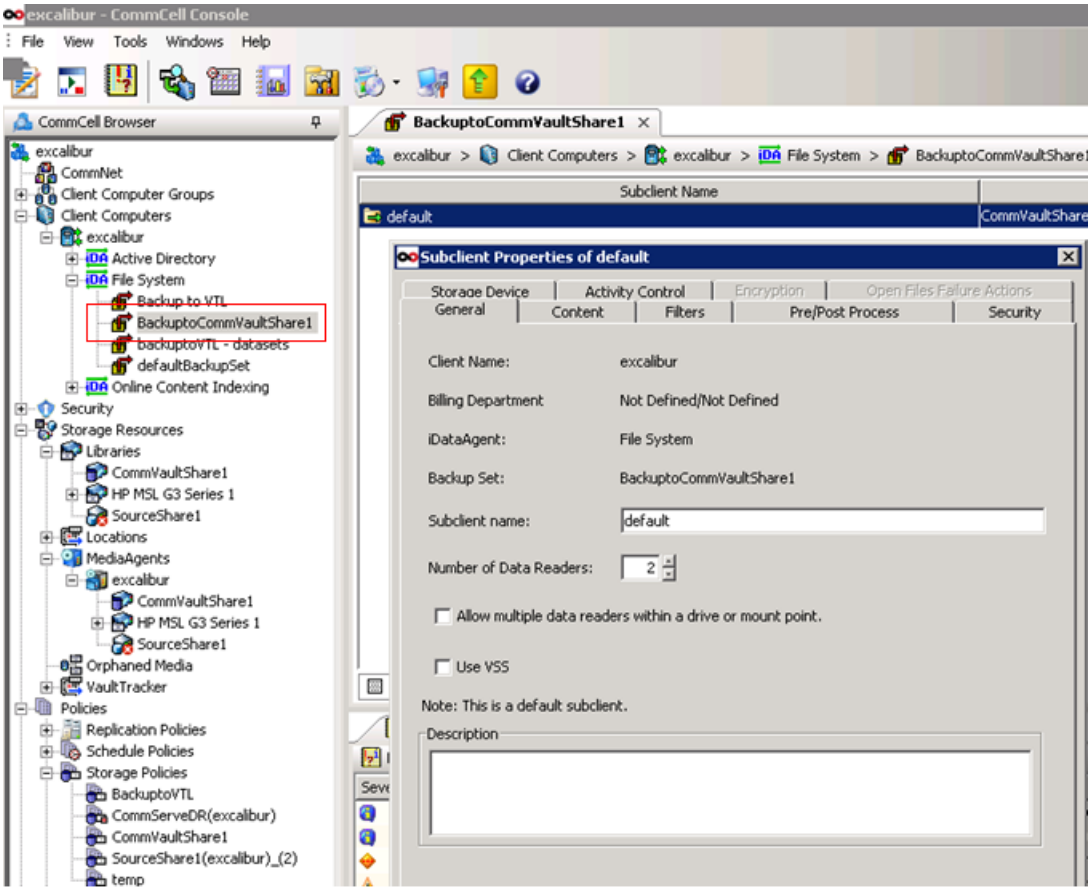


NOTE: Backup job configuration should be done at the policy level whenever possible and Subclients should never be altered unless it is absolutely necessary. The method shown here is intended to show key parameters that may otherwise be overlooked when doing everything through a storage policy.

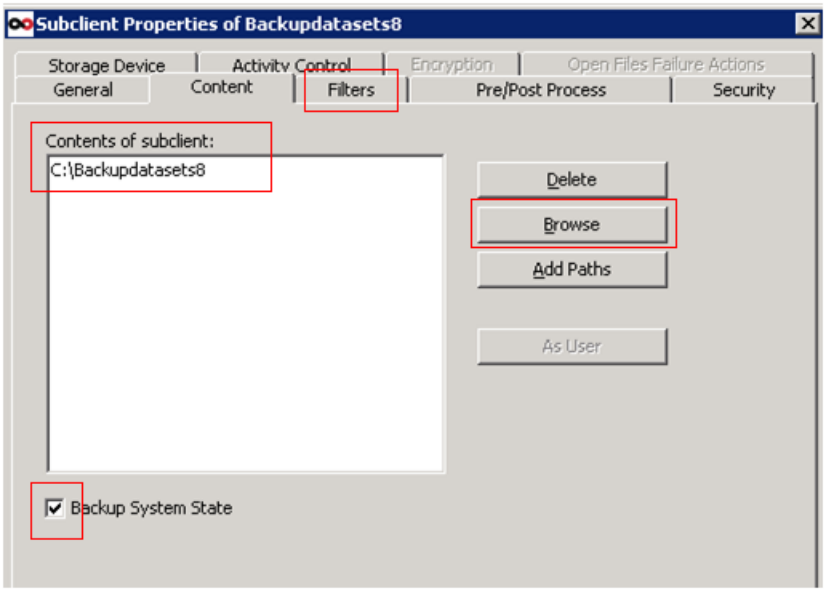
2. Give the backup set a name and assign a Storage Policy.



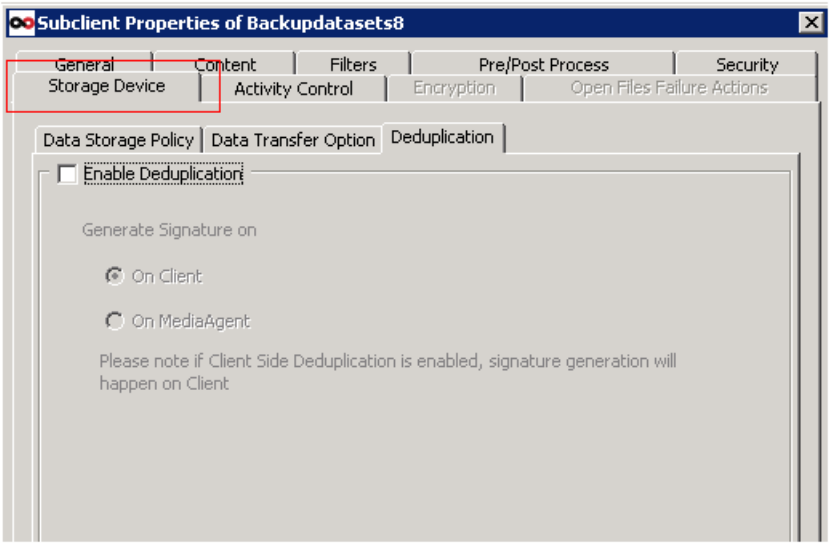
3. Click on the Filesystem backup you have defined to display “default” in the right-hand navigation window. Double click on default to display the Default settings for our newly defined backup job.



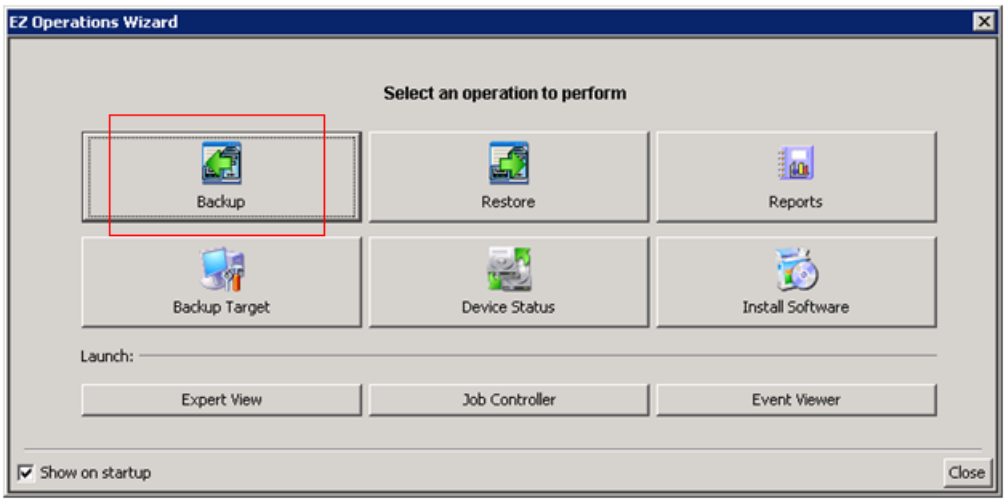
4. Go to the **Content** tab and use the **Browse** button to select the data that you wish to back up. In our example we have chosen an 8 GB dataset (called Backupdatasets8) consisting of many files of different sizes and the **Backup System State** box is checked. (This is one of the default settings. If you do not want to back up system state files, go to the **Filters** tab and set the System state files to ignore.) Click **OK**.



5. Go to the **Storage Device — Deduplication** tab and uncheck **Enable Deduplication** because all the deduplication is going to take place on the D2D NAS share. Click **OK**.



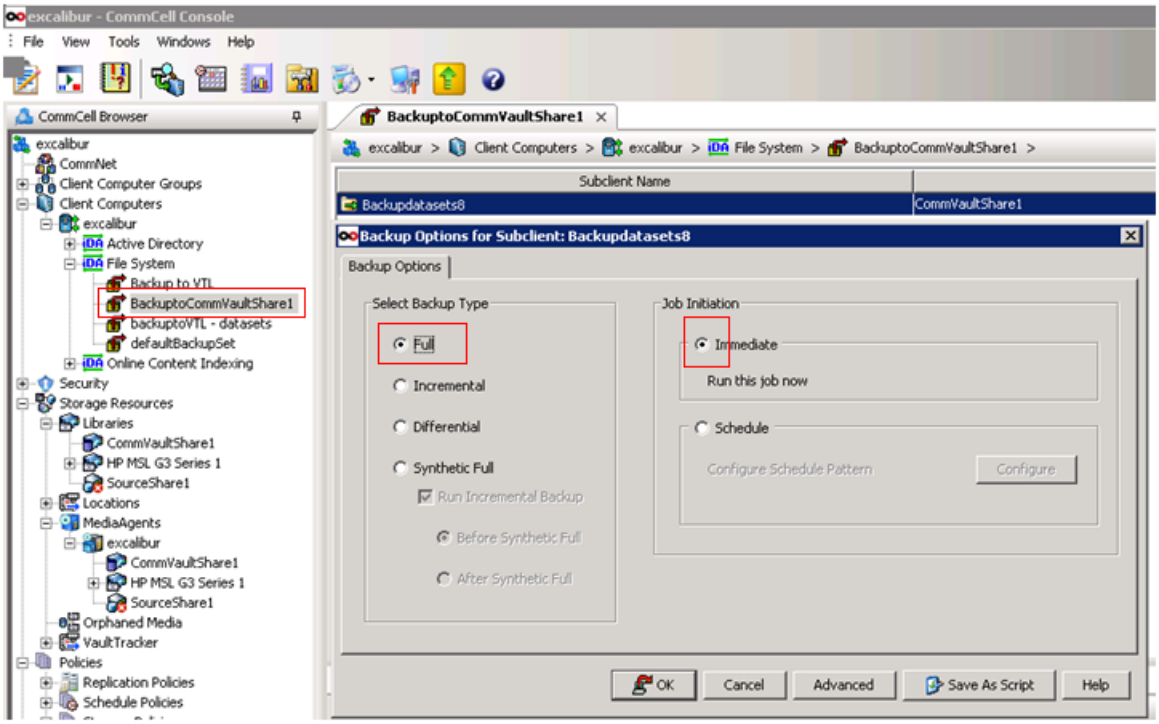
NOTE: Alternatively you can use the EZ Operations wizard to set up a backup job as we did to configure the backup target previously.



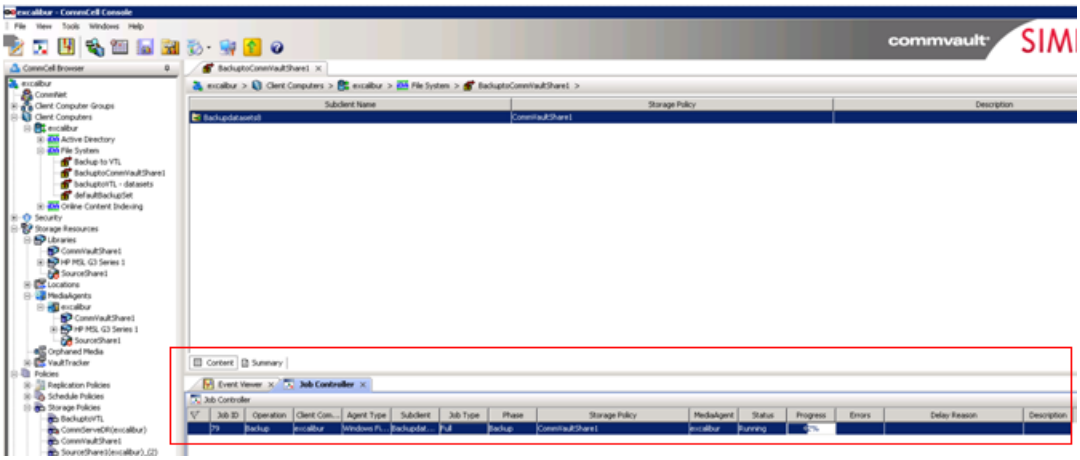
Perform the first backup

We are now ready to perform our first backup.

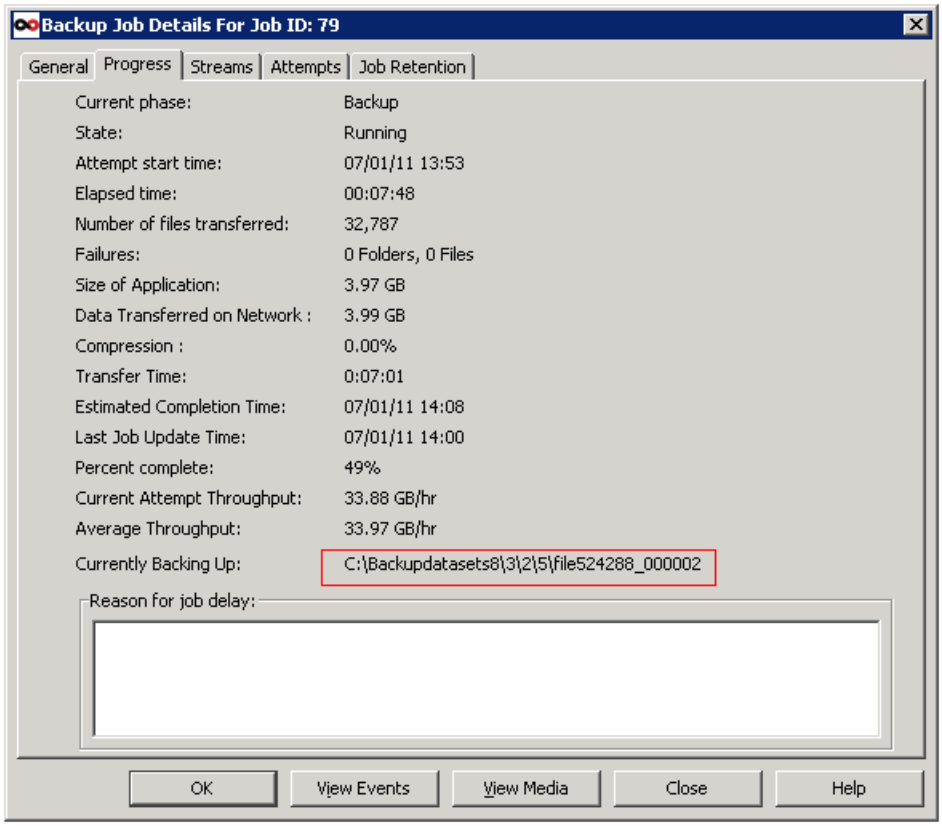
1. Click on the backup job in the File System folder. Double click on the backup job name and select the backup type in this case FULL. Click **OK** to run the job immediately.



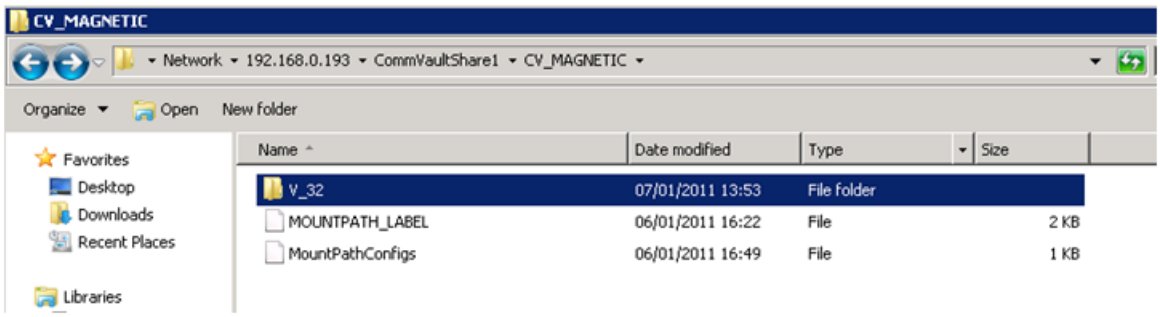
2. Look in the Job Controller Window to monitor progress.



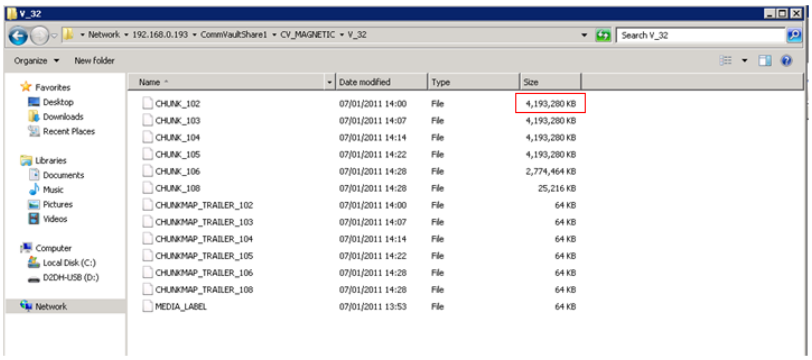
3. Double click on the Job Controller entry for more details on progress.



4. Windows Explorer also shows the types of files created.



CommVault creates a folder per mount path such as V_32.



The example shows the backup to CommVaultShare1 has been split into 4GB containers (called CHUNKS by CommVault) as we set in our Storage Policy. Also note the CHUNKMAP TRAILER which links the chunks together.

The index information for the job is appended to the last CHUNK file. CommVault software generates an index of the data whenever a data protection job is initiated. The index contains a list of all the data objects (files/subdirectories, database objects, mailbox objects and so on) along with the path to the archive file that stores the data in the media.

NOTE: By default index files are stored locally on the server that is the Media Agent server and connected to the disk library. If you have multiple Media Agent servers, you can configure a shared index location where indexes from all the Media Agent servers are stored.

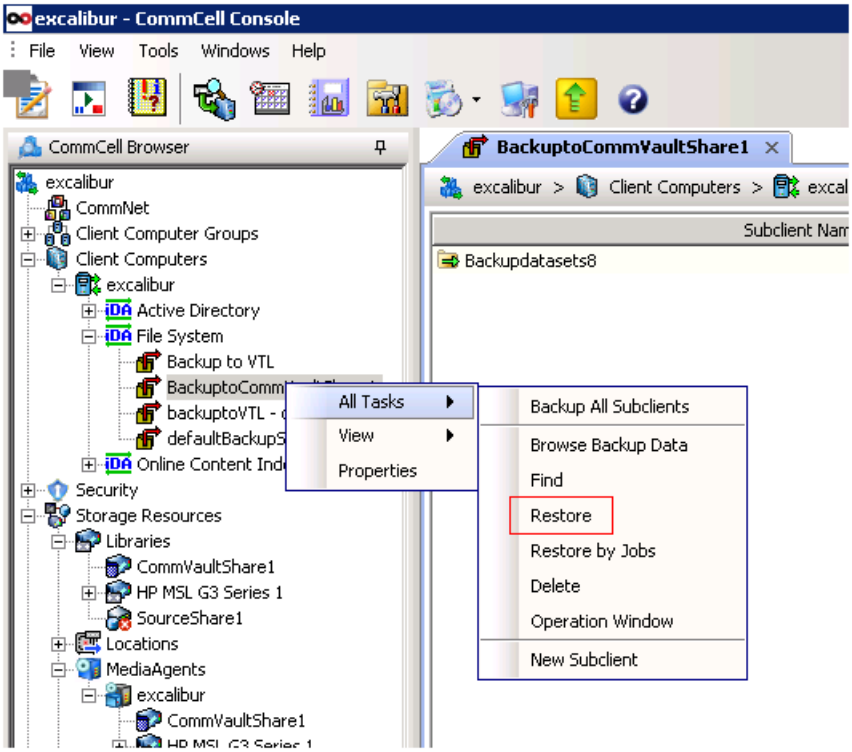
5. We have successfully backed up the user data directory, backupdatasets8 + Excalibur System State, to the D2D NAS share, CommVaultShare1

Restore from HP D2D NAS share

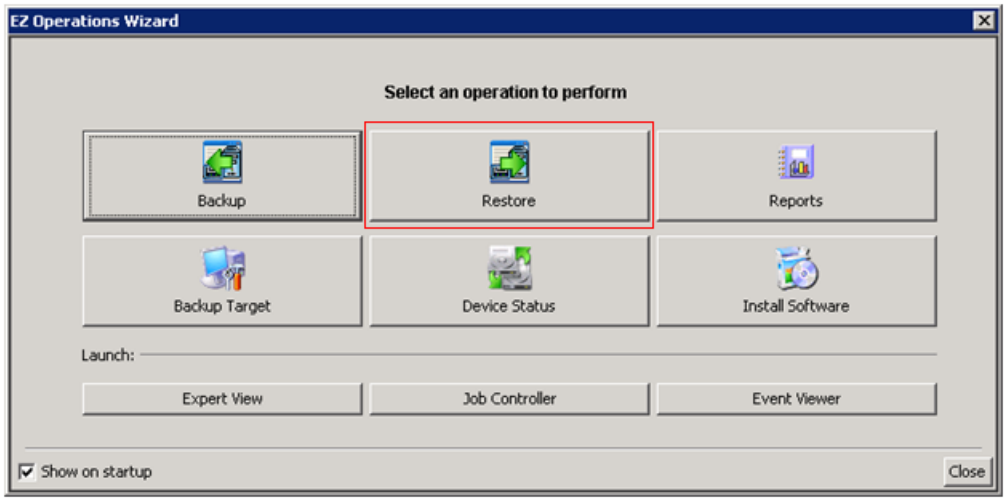
Index data is key in the recovery process following a complete disaster to the backup catalog. The index also provides quick access to the data in a browse/restore operation.

There are two ways to restore from the HP D2D NAS share:

- Using the Main screen

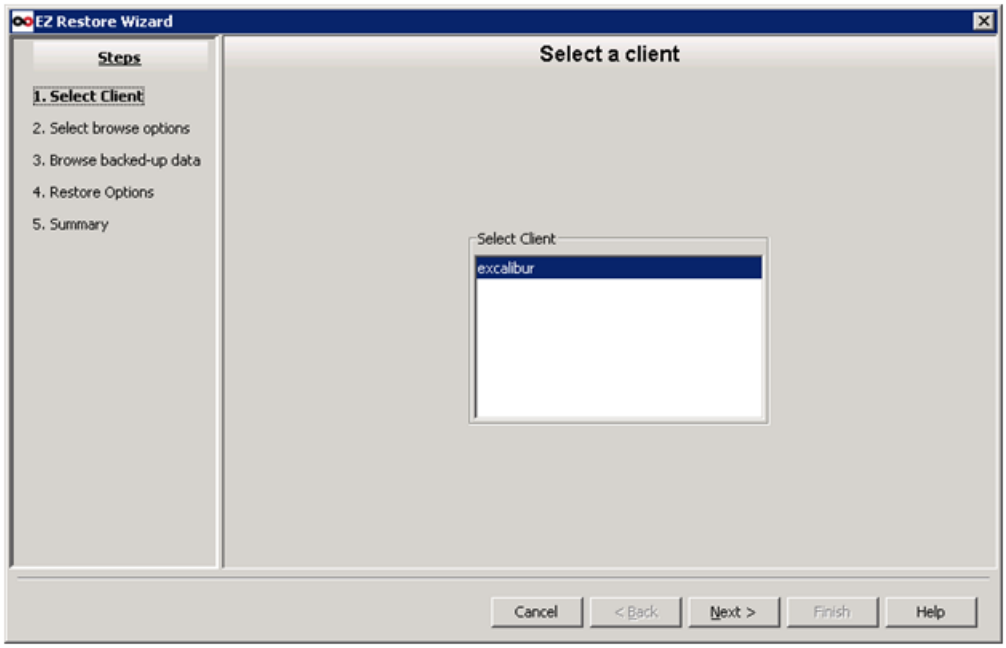


- Using the EZ Operations wizard

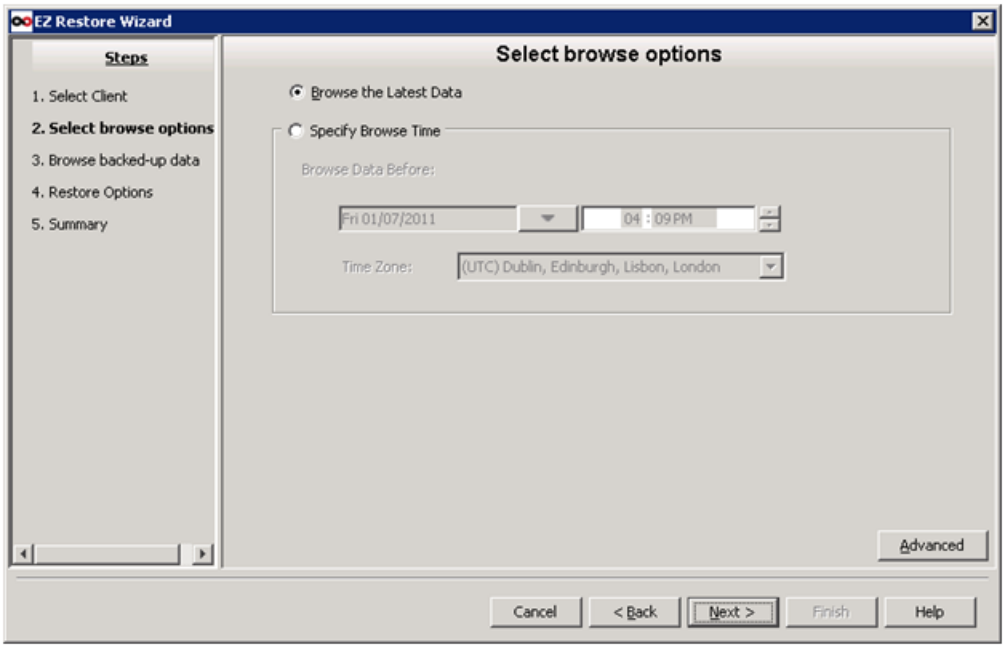


For our worked example we will use the EZ Operations Wizard.

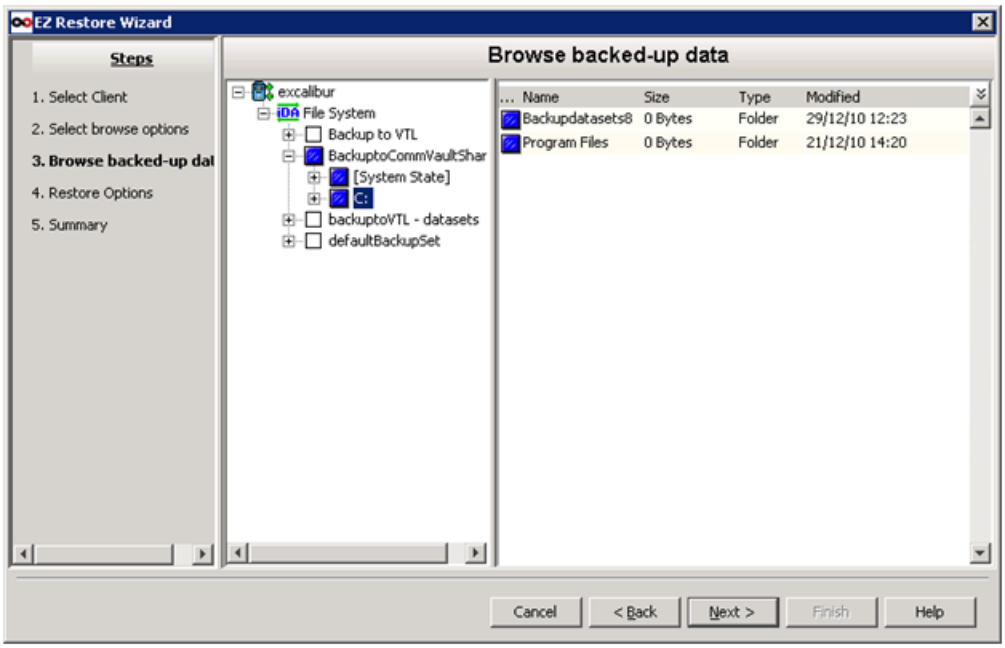
1. Click **Restore**.
2. Select the client and click **Next.**



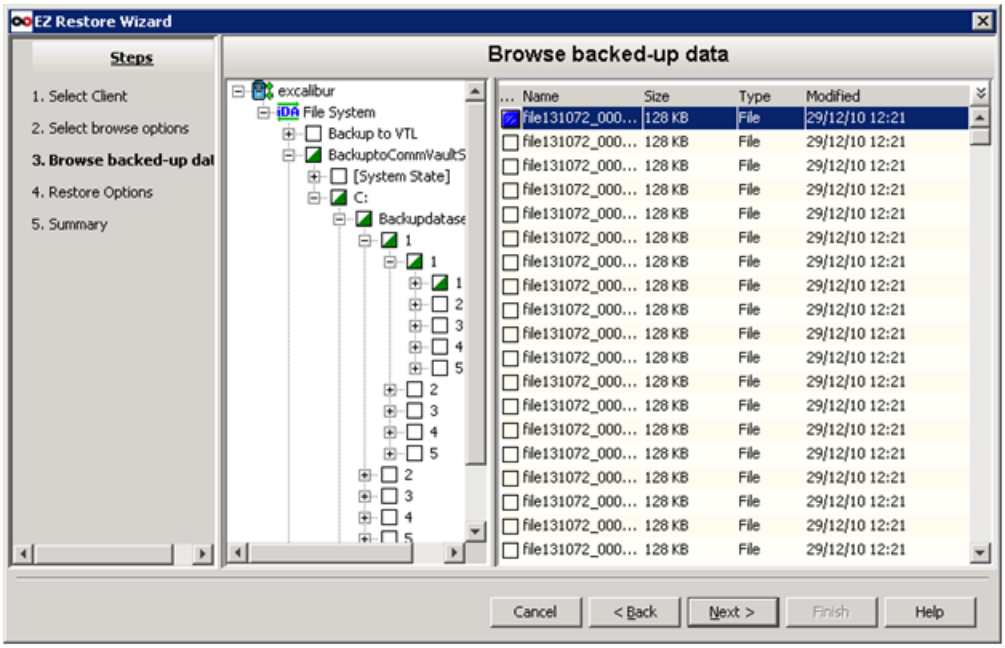
3. Select the latest backup, or browse to the data at a point in time. and click **Next.**



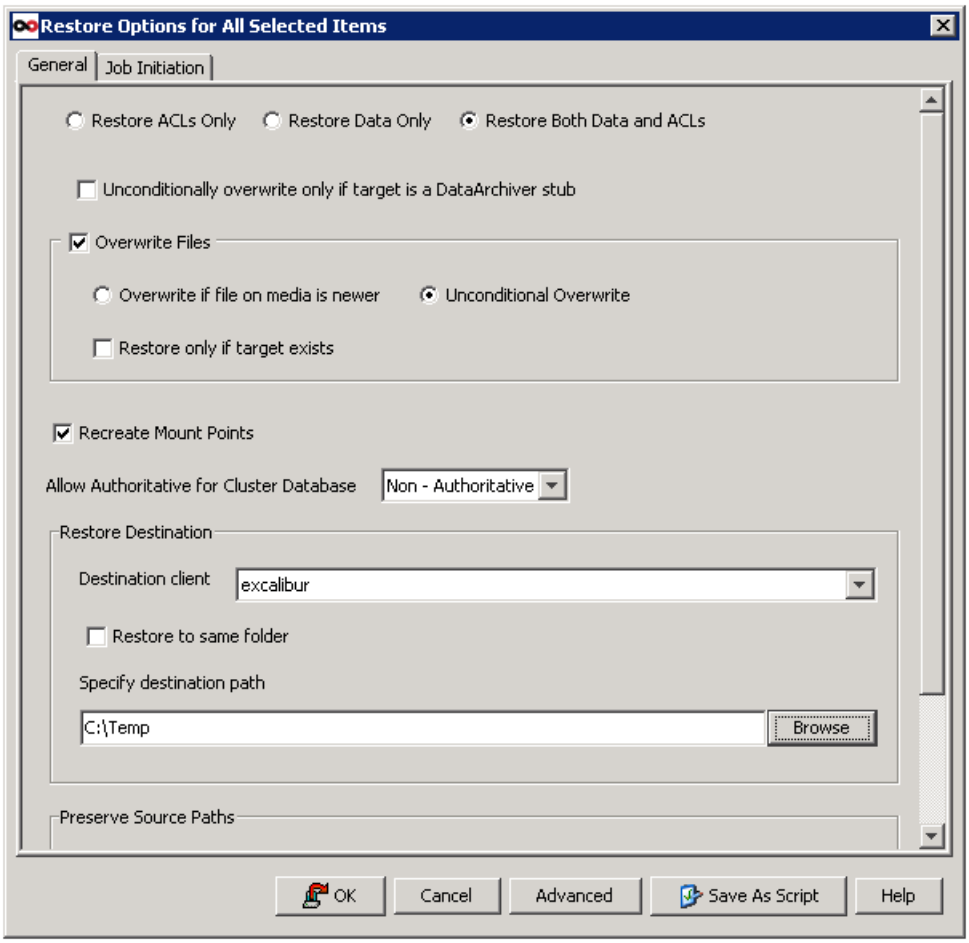
4. Select the data file or directory to be restored by drilling down and then select an individual file or all copies of that file to be restored. Click **Restore.**



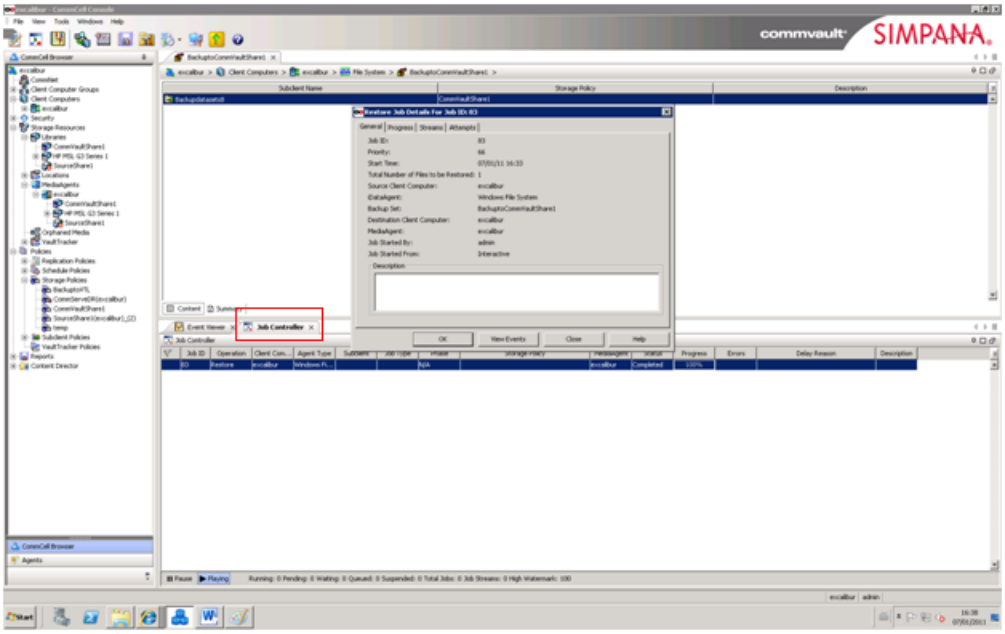
5. Double click on the file to be restored and select the required version.



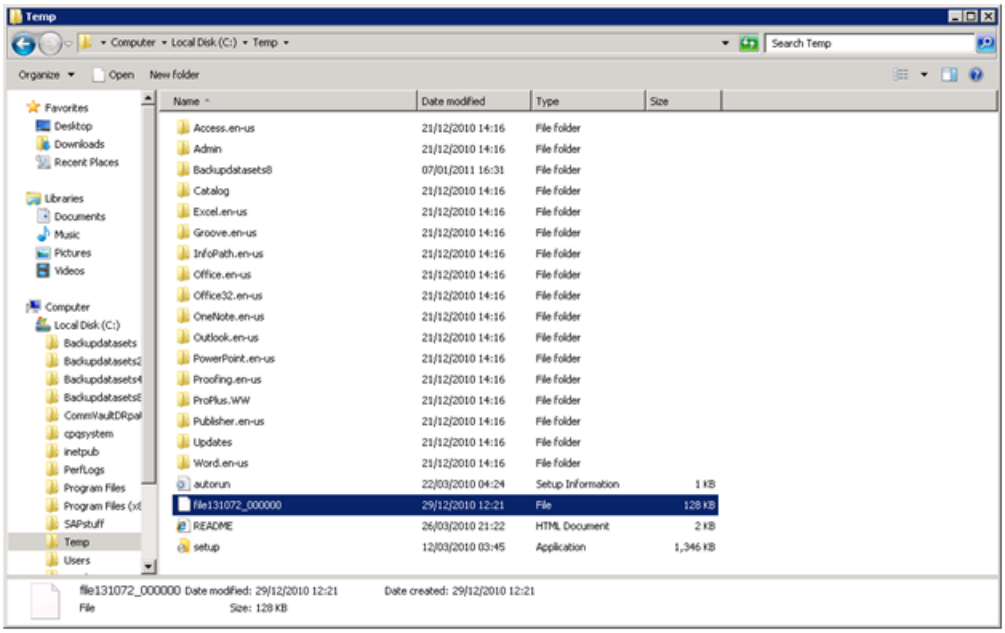
6. Select the **Overwrite Files** option and specify a new destination path, if required. It is OK to use unconditional overwrites if you are restoring to a temporary directory.



7. Click **OK** to go back to the EZ Wizard, followed by **Next** to display the Summary screen.
8. Click **Finish** and watch the job run on Job Controller; double click the job in Job Controller to get more details.



9. On completion the file is restored to C:\Temp.



5 Other considerations

Ensuring you do not exceed D2D maximum open file limits

The HP D2D NAS share has strict allocations for the number of open files it can have open at any given time (See Appendix B).

Should these limits be exceeded a lost connection may occur, causing the backup to fail and there will be an entry in the D2D Event log. Possible causes for this situation might be:

- **Too many simultaneous backup streams going to a given D2D NAS share:** In this case the number of writers being used or the number of backup jobs scheduled at the same time should be reduced.
- **CommVault Data Aging process:** This is selectable as an attribute of the CommVault Storage Policy and frees up space after the retention period has been exceeded. It is recommended to schedule it to run outside of the backup window. See below for more information.
- **CommVault GridStore technology:** This is an additional licensable feature that allows the automatic failover of backups to an alternative path or for a device to be accessed by a separate media agent should the primary path become inaccessible. It is possible that a race condition can occur as follows:
  1. We exceed the number of open files to a D2D NAS share, causing a "lost connection" as seen from CommVault.
  2. This triggers the Grid Store technology to re-send the backups on a round robin basis to another device that already has a high load.
  3. We then exceed the open file limits on that D2D NAS store which, in turn, gives lost connection and so it continues.

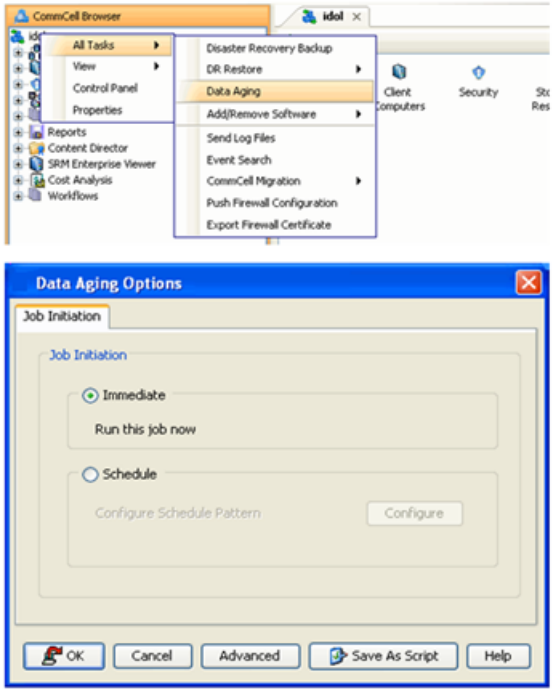
  See below for more information.

Data Aging Scheduling in CommVault Simpana 9.0

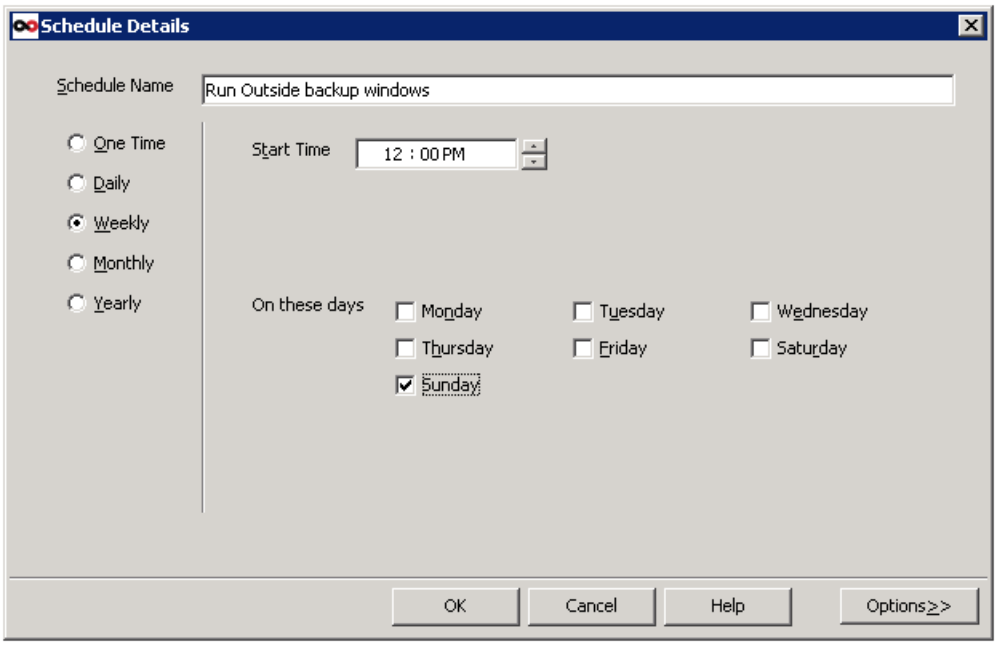
Data Aging is a process in CommVault Simpana 9 that frees up space once a backup device data retention period has expired. This process needs to be managed because data aging involves data overwrites which in turn generates housekeeping.

If a housekeeping blackout window is set, this should limit the impact of the data aging process. If a housekeeping blackout window is NOT set, schedule the data aging process to run outside of the backup windows as shown below:

1. Display the **Data Aging Options**.



2. Select the **Schedule** option and configure data aging to run outside of the backup windows.

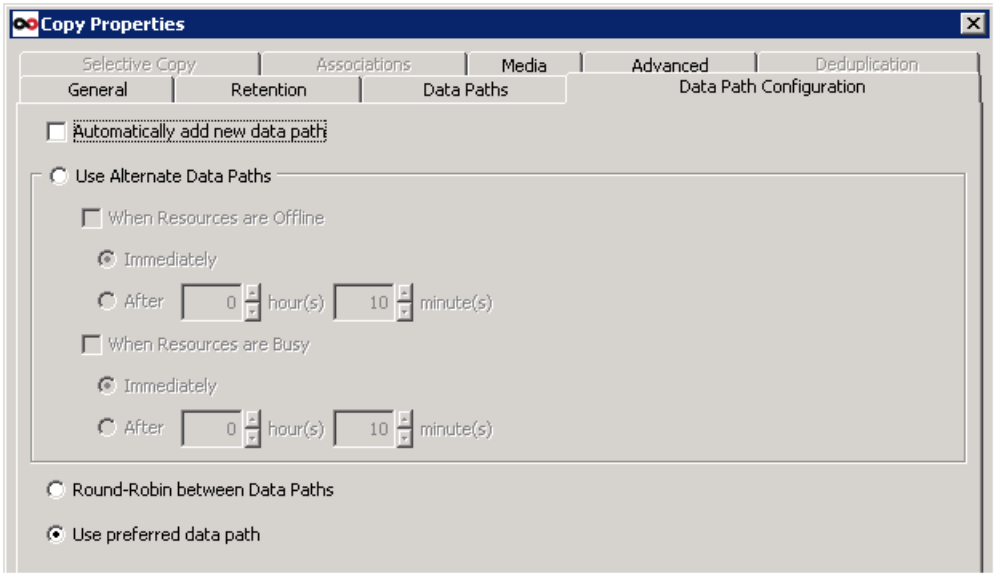


GridStore (Alternate Data Path) setup

GridStore is a licensable feature in CommVault Simpana 9.0; if licensed, the Round Robin between data paths implementation causes issues with HP D2D NAS and should not be used. The Alternate data path (using another media agent) or preferred data path options however can still be used. Set as follows:

1. Click on Storage Policies to get the primary path displayed in the right—hand window, then highlight the path and right click to display Properties. Select the **Data Path Configuration** tab.

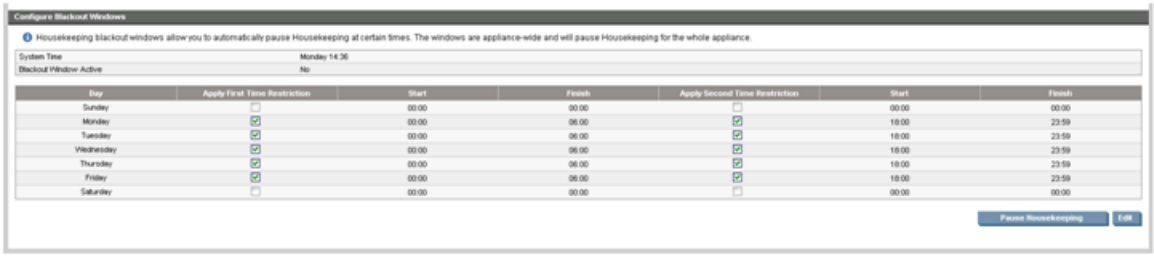
2. Make sure that **Robin between Data Paths** (load balancing across all disk libraries) is set. Make sure that **Use preferred data path** or **Alternate Data Paths** is set, but do not use **Round Robin**.



D2D housekeeping configuration

It is a standard best practice with HP D2D Backup Systems to schedule housekeeping (space reclamation) to occur outside of backup windows to ensure there is no I/O contention on the device and ensure maximum backup performance. To set the Windows when housekeeping should be allowed to run, proceed as follows:

1. From the Web Management interface select **Administration — Housekeeping**. Up to two periods per day may be selected when housekeeping must not run (blackout). In the example below D2D housekeeping will not run, Monday to Friday between 18:00 and 06:00 (when backups are running).



2. It is also important to ensure that when housekeeping does run it has sufficient time to clear all the outstanding housekeeping jobs as shown below and there is sufficient “idle” time on the appliance.

Device allocation

In order to get the best deduplication ratio from a D2D device type HP recommend that similar data types be directed to the same device (VTL or NAS Share). This approach can tend to go against the CommVault Simpana automated storage management techniques and may require some manual configuration overrides.

Multiple Media Agents and secondary mount paths

CommVault allows some sophisticated approaches to using Disk Libraries, mainly shared access disk libraries and secondary mount paths.

Shared access disk libraries

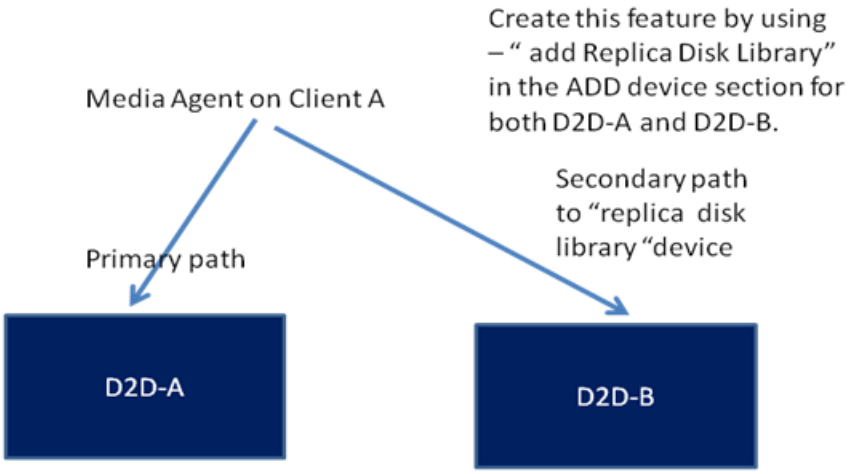
Two types of shared access disk libraries can be configured. They are:

- Disk libraries with a dynamic mount path (this refers to Disk Libraries based on FC disk arrays and so is not relevant to HP D2D NAS shares which are connected via Gbe or 10GbE)
- Disk libraries with a static mount path – this can be applied to D2D NAS shares

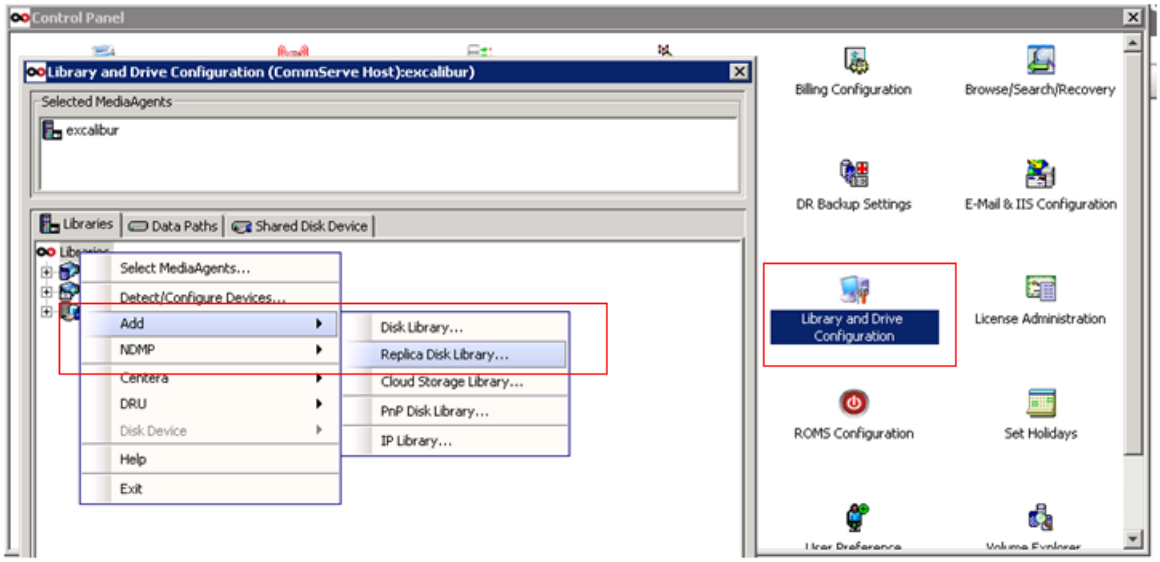
Paths

Secondary mount paths can be used to create some end to end disaster recovery capabilities using HP D2D NAS shares.

This technique allows a single Media Agent to have two paths and these two paths can be to different devices that are replicas of each other – this becomes very useful in recovery scenarios for ROBO sites as we will see later.

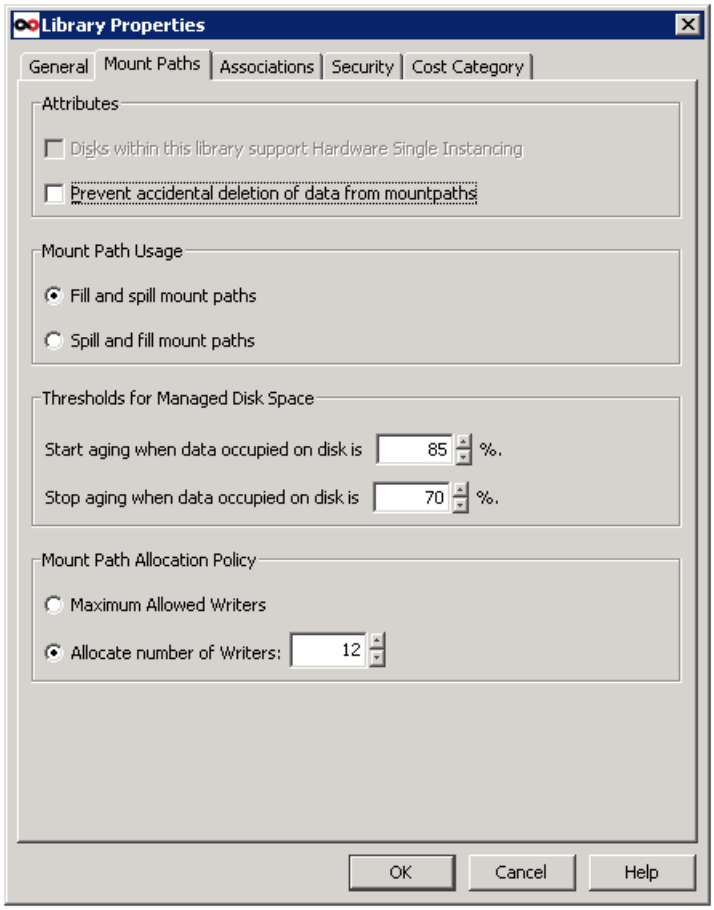


The screen shot below shows how to create a replica Disk Library for use in this type of scenario.



In addition mount paths can be configured for data load balancing.

Right click on the Libraries tab of Storage Resources, select **Properties — Mount Path** and check **Mount path usage** is set to Fill and Spill.



NOTE: A typical D2D based Disk Library configuration will have only one mount path, i.e. the share used to create it in the first place. Therefore, this setting is only relevant if multiple network share paths are created during the setup of the Disk Library.

- Fill and spill mount paths: This specifies that the system should completely consume (fill) the free space in a mount path before utilizing another mount path.
- Spill and fill mount paths: This specifies that the system should round-robin (spill) between the available mount paths for each job.

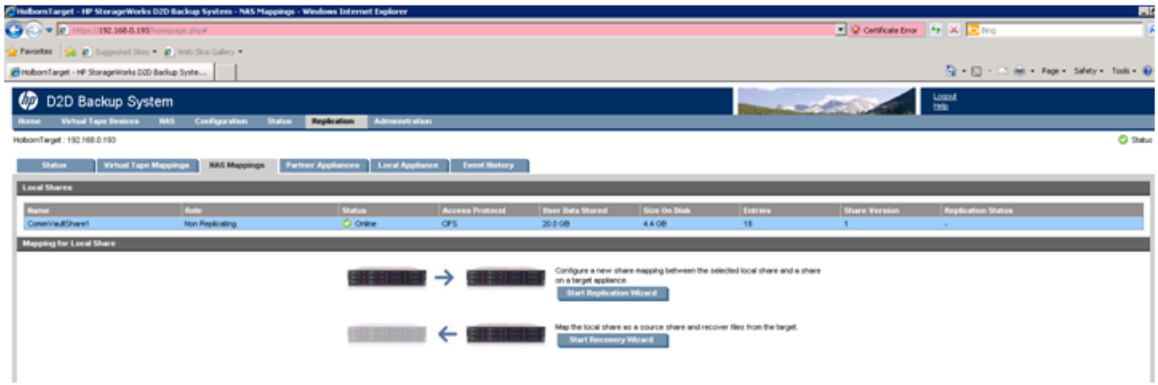
For HP D2D NAS shares the preferred setting is "Fill and Spill" because we do not want unmanaged jobs switching between multiple D2D NAS shares which may cause the number of open file limits to be exceeded.

6 D2D NAS replication

One of the major benefits of HP D2D Backup Systems with StoreOnce deduplication is the ability to replicate the data stored over low bandwidth links to another D2D Backup System on a Disaster Recovery site. Here we will briefly show how replication for D2D NAS shares is configured.

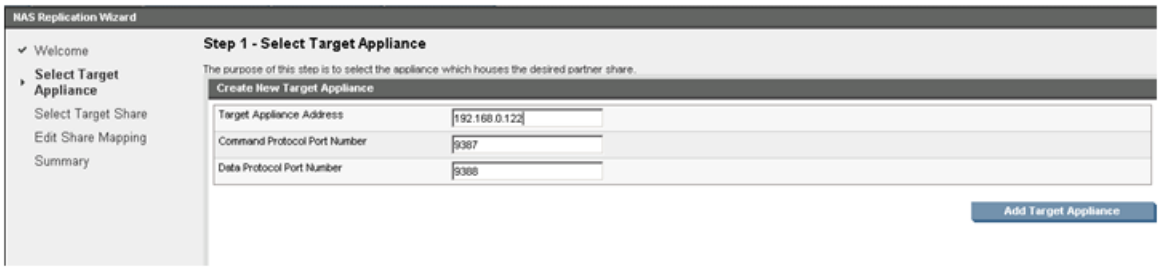
See the next chapter for more information about using CommVault Simpana 9.0 to recover from a D2D Backup System at a Disaster Recovery site

1. On the D2D Web Management Interface go to **Replication — NAS Mappings** and click **Start Replication Wizard**.

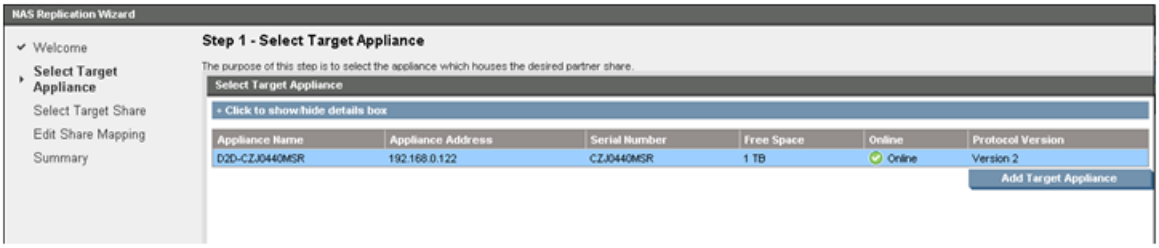


2. At the Welcome screen click **Next**.

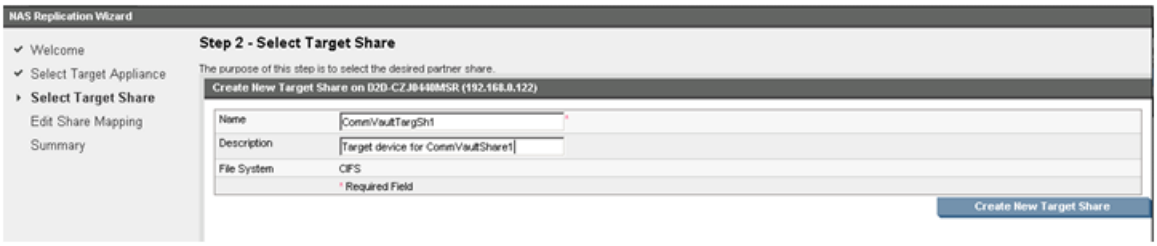
3. Type in the IP address of another D2D Backup System that you want to act as a target for replication from your source D2D Backup System.



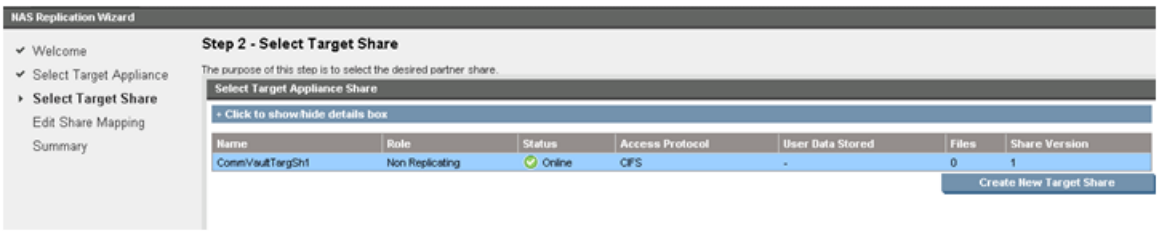
4. Click **Add Target Appliance**. The target is accessed and placed **online** for the source device. Click **Next**.



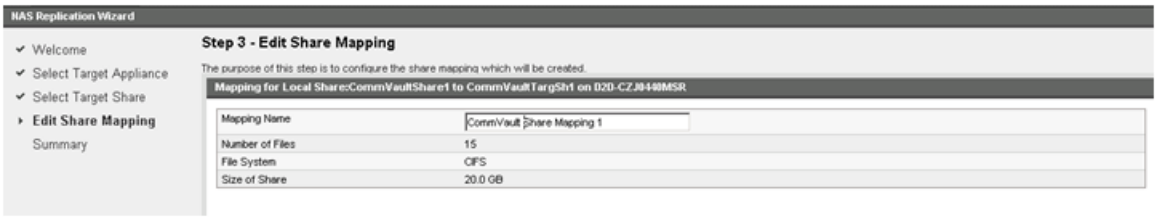
5. No target shares are created so we will create a new target share (from the source D2D Backup System). Enter details and click **Create New Target Share**.



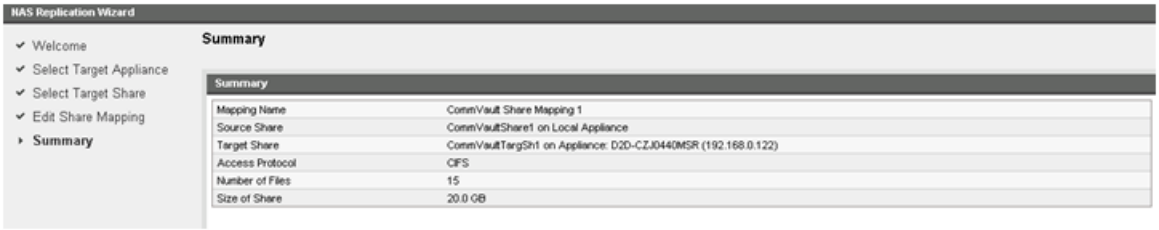
6. The target share is created and placed online for the Source. Click **Next**.



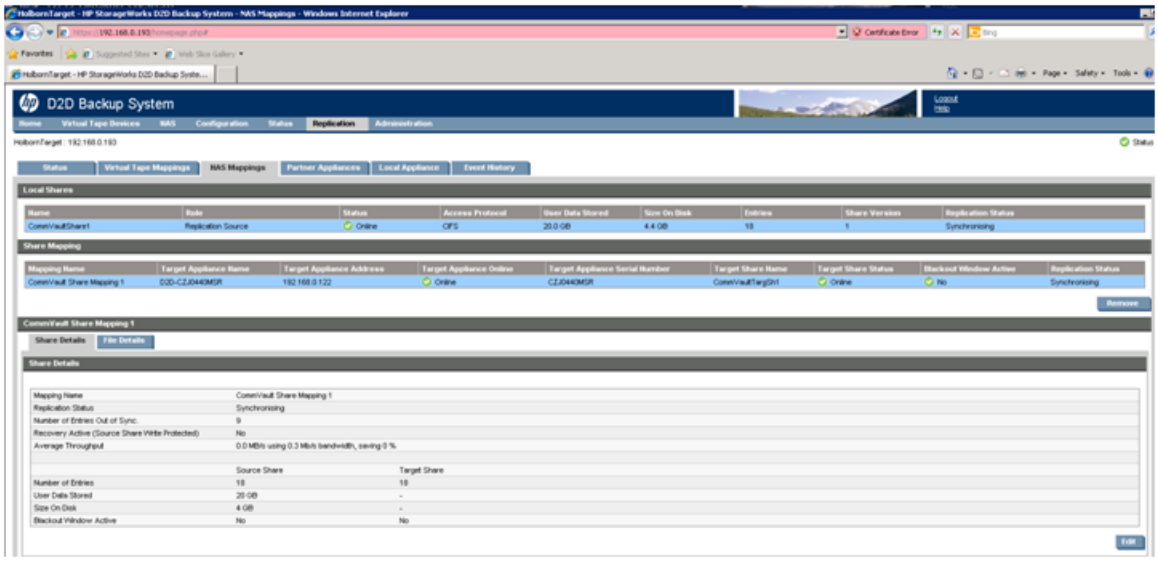
7. NAS Replication relationships are termed **Mappings** and are 1:1 in structure. Enter a unique name for this relationship and click **Next** .



8. Replication is now configured and a Summary screen is displayed. Click **Apply**.



9. You are returned to the **Replication —NAS Mappings** screen, which now shows the mapping relationship. The source now starts to “synchronise” with the target in a process known as “seeding” – this is a one-off process where the current total contents of the source are transferred to the target. Subsequent backups to CommVaultShare1 will result in only unique changed data being replicated to the target D2D Backup System.



7 End to End Disaster Recovery Process

In this section we will explain the process for recovering from a replica D2D NAS share having made use of the low bandwidth replication feature of HP D2D NAS.

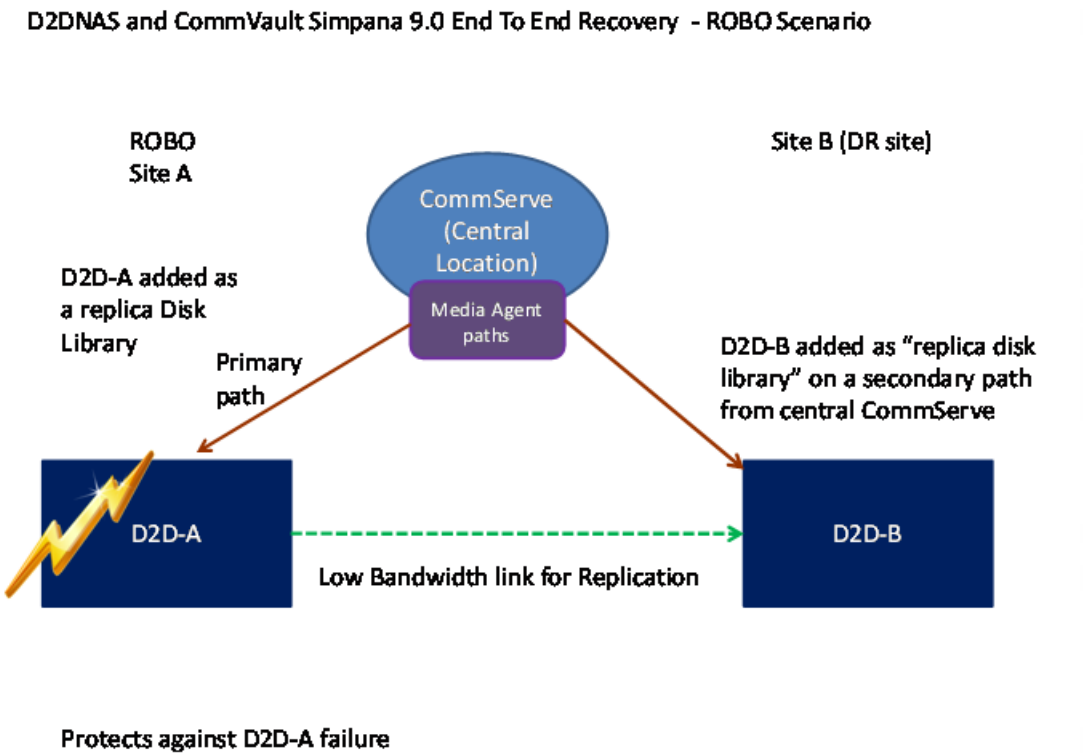
We will cover three scenarios:

- A ROBO site where the CommCell is still available but the local data is lost (recover data from the Disaster Recovery site)
- A Data Center to Data Center scenario where a complete CommCell installation has been lost (total recovery from Disaster Recovery site)
- A scenario where the D2D Backup System at the target site is also copied to physical tape for archiving and security

End to End Recovery – ROBO Scenario

This typical usage model is a large ROBO deployment with the Commserve in a central location. In this scenario, there are two D2D Backup Systems, one located at a ROBO site and one located at the central location. Low Bandwidth Replication is configured between the two D2D Backup Systems to enable data written at the ROBO location (Site A) to be replicated to the Disaster Recovery location (Site B). A CommVault Media Agent server, in this case the Commserve, is configured to utilize both D2D Backup Systems, one as the primary read/write device; the other as a secondary read-only device.

Figure 2 End to end recovery, ROBO scenario



Recovery steps are as follows.

1. Configure D2D NAS shares on Site A and Site B from the D2D Web Management Interface.
2. Configure replication between the D2D-A & D2D-B NAS shares.

3. Configure Media Agent and shared disk devices for both D2D libraries on Commserve.
4. Configure a replica disk library (CommVault terminology) for both D2D-A and D2D-B associated with the same Media Agent on Commserve.

If we have a disaster on Site A but Commserve remains operational, it is possible to recover the data from Site B by selecting the Media Agent path for the replica disk library and restoring over the secondary path link (GbE).

As Commserve at Site A did not physically write the data to D2D-B (it was written by the low bandwidth replication process), and there are no entries in the CommCell database for D2D-B, you might think that recovery is not possible. However, since D2D-A and D2D-B share the same Media Agent, a full recovery from Site B is possible because, with CommVault, meta data about the contents of a backup is held in an index that is appended to each backup set.

When completing a restore from D2D-B, the first time a recovery is undertaken, the index information for the backup set has to be retrieved from the backup in order to select which files to recover. This index is recovered to the local index cache on the Media Agent (in this case the Commserve), and is therefore available immediately for subsequent restores.

The index cache directory is the directory in which index data resides. Each Media Agent maintains an index cache for the data protection operations performed using that Media Agent. The index data maintained in the index cache is accessed by the system during data protection, browse, and data recovery operations.

The index cache is maintained on a least recently used (LRU) basis. As the capacity of the cache is reached, those index data files that have been least recently accessed are overwritten with the new index data. If a data protection, browse and data recovery operation requires index data that is either no longer in the cache or not accessible to the operation, the index data is recovered from the media.

To ensure that other files do not use up disk space that is needed for index data, you can create a partition specifically for the index cache directory. The partition must be large enough to accommodate four percent of the estimated amount of data managed by the Media Agent.

During the Media Agent installation, the install program prompts for an index cache location for the specific Media Agent. This information can be viewed or modified from the Catalog tab of the Media Agent Properties dialog box.

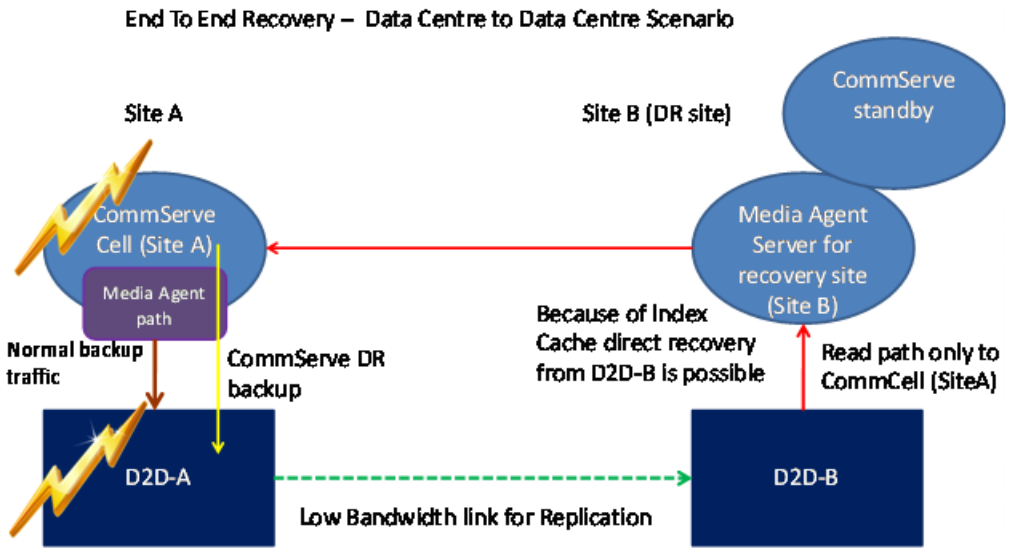
End to end recovery – data center to data center

In this scenario there are data centers in two locations. Site A is the production location, where live backups of the production data takes place; and Site B is a Disaster Recovery location.

Two D2D Backup Systems are provided, one in each location, together with dedicated Media Agent servers for each library. At Site A, the Commserve acts as the Media Agent for the local D2D Backup System (D2D-A), whilst the second Media Agent server is connected to D2D–B at the Disaster Recovery location (Site B).

Both D2D Backup Systems and Media Agents are configured as a CommVault replica disk library, with the primary path (read/write) through Media Agent connected to D2D-A; and a read-only path via Media Agent connected to D2D-B.

Figure 3 Data Center to Data Center recovery



To facilitate a full end to end recovery, two CIFS share will be created on the D2D Backup System:

- BackupShare – To be used as the mount point for the replica disk library
- CommcellDR – To be used for the Commcell DR backup

During normal operation, the Media Agent at Site A writes backup data to the replica disk library D2D-A, which is subsequently replicated to D2D-B via LBR. Regular Comcell DR backups are scheduled on the Commserve and are written to the second share on D2D-A (CommcellDR) with LBR replicating a copy to D2D-B.

This configuration enables recovery from both a failure of D2D-A at Site A and also in the event of a total disaster of Site A.

Should D2D-A fail, then data can be recovered from D2D-B via the Media Agent at Site B. In this case, when recovering the data via a restore operation; the Media Agent at Site B would be selected as the source path and the data read from D2D-B and restored to Site A via the WAN connection. This situation is similar to the previous scenario, i.e. ROBO configuration.

In the event of a total disaster at Site A where we lose the CommCell and/or the D2D-A, proceed as follows to recover Site A data at Site B:

- Recover CommServe at Site B
- Recover production data from D2D-B via Media Agent server at Site B

Recover CommServe at Site B

1. Recover the Commserve to the standby server at Site B.

   Using the CommcellDR backup from the replica copy on D2D-B and the CommServe disaster recovery tools, read the DR backup from the CommcellDR backup share on D2D-B, and recover the CommServe to the standby server.

2. Once the CommServe has been recovered access to replicated copies of the backup data can be achieved via the Media Agent server at Site B.

   If it is not possible to retrieve the Commcell DR backup from the share, due to some form of corruption; use the CommVault Resource Kit utility 'Media Explorer' to read the DR backup from the D2D-B share. Once the Commcell DR backup files have been recovered, the CommServe can be rebuilt.

Recover site production data

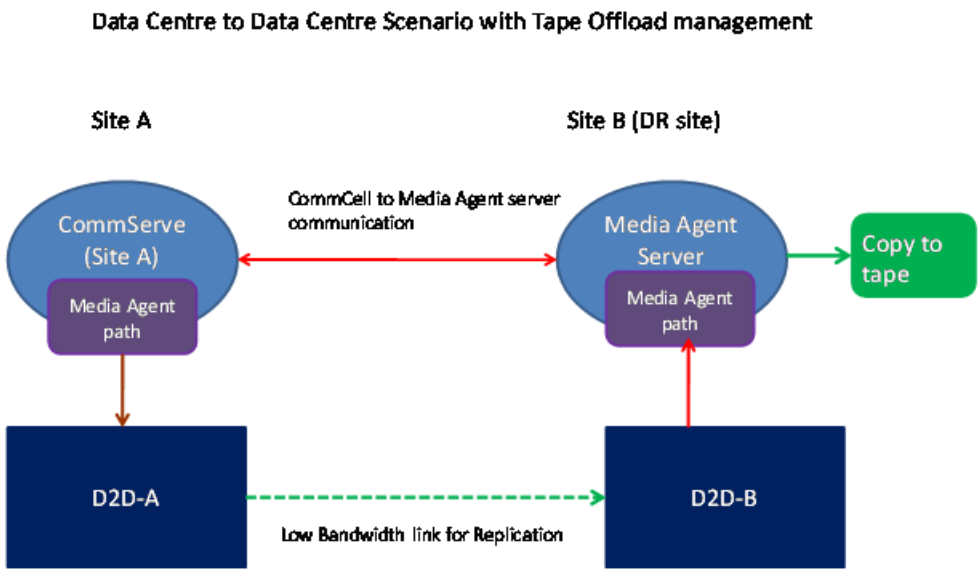
Having recovered the Commserve at Site B, recovery operations can now take place from D2D-B. From a CommVault Simpana perspective, the replica disk library continues to be accessible via the secondary path through the Media Agent at Site B. This enables recovery operations to be performed for production data.

When restore operations are requested, instead of selecting the Site A Media Agent, which is no longer available; the Administrator can select Media Agent at Site B for the recovery and recover data from D2D-B. The first time a recovery is undertaken, the index information for the backup set must be retrieved from the backup in order to select which files to recover. This index is recovered to the local index cache on the Media Agent at Site B, and is therefore available immediately for subsequent restores.

Data center to data center with physical tape offload at DR site

The typical usage model here is for D2D-A to D2D-B to Tape with archive tape copies being maintained at the DR site.

Figure 4 Data center to data center recovery with physical tape offload



In this scenario, there are two locations:

- Site A is the production site where data is backed up to a local D2D Backup System.
- Site B is used for DR purposes to maintain a secondary copy of the data and to archive copies to tape.

Two D2D Backup Systems are provided, one in each location, together with dedicated Media Agent servers for each library. At Site A, the Commserve acts as the Media Agent for the local D2D device (D2D-A); whist the second Media Agent server is connected to D2D –B at the DR location (Site B).

D2D-A is configured to replicate data stored to it to D2D-B via Low Bandwidth Replication (LBR). In addition, the Media Agent server at Site B is also connected to a Tape Library. Both D2D Backup Systems and Media Agents are configured as a CommVault replica disk library, with the primary path (read/write) through Media Agent connected to D2D-A; and the read-only path via Media Agent connected to D2D-B. An additional Tape Library is configured for the Media Agent at Site B.

Using this configuration it is possible for archive copies to tape to be performed solely from Site B, i.e. without impacting on Site A or the WAN connection between the sites, whilst being under the control of the CommServe at Site A.

This is achieved by scheduling an Auxiliary Copy of the backup data (CommVault terminology for a second copy) that would use Media Agent at Site B to read the data from D2D-B (replica D2D), and to copy the data by writing it out to the tape library also configured on the same Media Agent.

More Information

See:- CommVault Disk Libraries

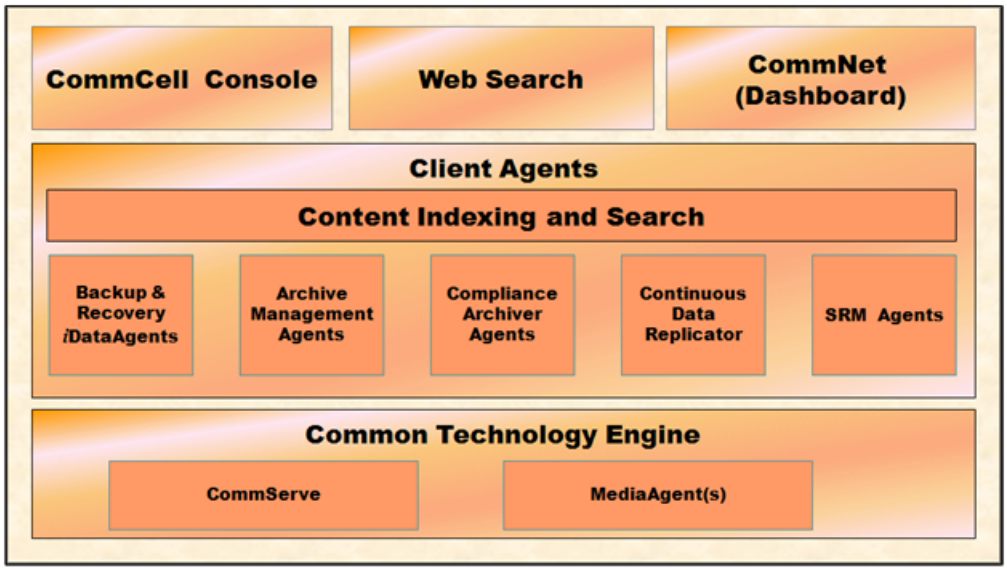
A Terminology

Commserve Storage manager :

This is the command and control centre of the CommCell.

CommCell

These are integrated software modules that can be integrated into common console.



The system consists of integrated software modules which can be grouped together in a CommCell® configuration. Each CommCell configuration consists of the following main components:

- One or more of the following Client Agents:

  iDataAgents that perform the backup and restore operations
  Archive Management Agents which includes agents for Migration Archiving and Compliance Archiver agents
  ContinuousDataReplicator to perform data replication from a source Client to a destination Client
  Storage Resource Manager (SRM) Agents for analyzing and reporting of information on local storage resources.

- Common Technology Engine (CTE) components consisting of:

  One CommServe®
  One or more MediaAgents

Once installed and configured, these CommCell® elements can be controlled and monitored from a single unified CommCell® Console. Data in the entire CommCell - both stored and online data - can be searched for data discovery and other purposes using the Content Indexing and Search component. Data from several CommCells can be monitored and administered using the CommNet which serves as a dashboard for administering multiple CommCells.

Disk Library

This is CommVault terminology for a simple disk-based backup device.

B Open file limits and recommended streams per NAS share for D2D Backup Systems

Table 1 Open file limits and recommended streams per share

	HP D2D2502i	HP D2D2504i	HP D2D4106	HP D2D4112	HP D2D4312	HP D2D4324
Max files per share	25000	25000	25000	25000	25000	25000
Max Open files per share > 24 MB (DD threshold)	32	48	64	64	128	128
Max Open files per appliance > 24 MB (DD threshold)	32	48	64	64	128	128
Max Total Open files per share	96	112	128	128	640	640
Suggested maximum concurrent operations per share	4	4	6	6	12	12
Suggested maximum concurrent operations per appliance	16	32	48	48	64	64

Max Nos of files per share is set at 25000 because of replication considerations. To actually store more data most backup software allows the size of the D2D NAS "Containers" to be increased. For example, with CommVault the default container size is 2 GB but the user can easily change this to 16 GB or more.

The HP D2D NAS target for backup does not deduplicate the first 24 MB of any file for performance reasons. Some backup applications generate control files during backup to NAS that are constantly changing – to try and deduplicate constantly changing files slows down the deduplication process.

For any single D2D NAS share there are specific limits as to how many "Open Files" can be open at any one time – this is because of the memory allocation within the D2D Backup System. Generally, typical Filesystem backups like CommVault will open a single large container one at a time , but it is possible due to overlapping operations that two may be open at the same time for a small period of time. It is important NOT to send too many backup jobs to the same NAS share to avoid exceeding the NAS > 24MB open file limit per share and per appliance. (Appliance is the whole D2D Backup System). Failure to observe these limits can result in unstable operation. Stay within the recommended concurrent operations above to prevent this.

For example: A D2D4312 has 4 shares configured on it. We are running filesystem backups which open up a single container file at a time. The maximum number of backup jobs that can go to each share is 12 so we can have a total of 48 backup jobs running simultaneously and, even allowing for 2 files overlapping and being monitored as open at the same time, we would have a maximum of 96 files open on the appliance in a worst case scenario. This is well within the appliance limit of 128 open files.

About this guide

This guide:

- Provides step by step instructions on configuring a D2D NAS CIFS device on CommVault Simpana 9.0
- Describe the CommVault Simpana 9.0 Disk Library configuration options and identifies what settings to use with HP D2D NAS CIFS shares.
- Describes how to implement a full end–to–end recovery solution from a target D2D Backup System with D2D NAS CIFS shares using CommVault Simpana 9.0.

Intended audience

This guide is intended for users who install, operate and maintain the HP D2D Backup System.

This guide assumes a basic working knowledge of CommVault Simpana 9.0 and that it has been installed correctly by loading the appropriate Media Agents and licences.

Related documentation

In addition to this guide, the following documents provide related information:

- *HP StoreOnce Backup System Concepts Guide*: If you are new to the HP StoreOnce Backup System, it is a good idea to read this guide before you configure your system. It describes the StoreOnce technology.
- *HP StoreOnce Backup System User Guide*: This guide contains detailed information on using the Web Management Interface. It also contains troubleshooting information, including details on replacing failed or failing hard disks.
- *D2D Best Practices for VTL, NAS and Replication implementations*: This white paper advises how to plan the workload being placed on the HP StoreOnce Backup System in order to optimize performance and minimize the impact of deduplication, replication and housekeeping operations competing for resources. It is regularly updated.

You can find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click **Storage Solutions** and then select your product.

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: Table 2 (page 48)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis

Table 2 Document conventions *(continued)*

Convention	Element
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

⚠ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/ebs
- http://www.hp.com/go/connect
- http://www.hp.com/go/storage
- http://www.hp.com/service_locator
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to storagedocs.feedback@hp.com. All submissions become the property of HP.

Index