HP StoreOnce D2D NAS Integration with Symantec ® NetBackup™

Abstract

This guide provides step by step instructions on how to configure and optimize Symantec ® NetBackup™ in order to back up to HP StorageWorks D2D devices using a CIFS backup target.

HP Part Number: EH985-90936
Published: February 2011
Edition: 1

Contents

1 Introduction

Symantec® NetBackup™ is an Enterprise class data protection application. Its architecture is designed for a large and complex distributed computing environment. NetBackup provides scalable storage servers that can be configured for a variety of tasks such as backup, recovery, archiving and file migration.

NetBackup provides a variety of client agents for different operating systems and applications and a variety of additional functions such as Advanced Disk and the implementation of the Symantec Open Storage API(OST). Symantec NetBackup also has the capability of client side and central server software-based deduplication based on the PureDisk™ technology. NetBackup media servers can use disk or tape for storage targets.

NOTE: It is not the intention of this guide to cover all features of the Symantec NetBackup product. For example: this guide will not cover the Symantec NetBackup deduplication options using PureDisk™ technology because this is a software deduplication option which would not be compatible with a deduplication appliance based solution such as the D2D Backup System.

The objective of this guide is to provide:

1. Step by step instructions on how to configure the D2D NAS share to be used as a disk storage target by a NetBackup media server. The example uses the CIFS protocol.

   The CIFS protocol is used with media servers running on a Microsoft Windows platform to access network-based disk. To use with UNIX systems the NFS protocol must be used.
2. A guide to highlight some of the optional settings when configuring NetBackup.
3. Worked examples showing how to back up to a D2D NAS target and replicate to another D2D systems.
4. An explanation of some of the more complex NetBackup concepts.
5. A worked example showing how to recover data from the replication D2D target system.

As the guide will show, selection of the protocol and network configuration is quite easy using the D2D Web Management Interface (GUI). Symantec NetBackup is a highly scalable product and could easily support multiple D2D systems.

The NetBackup environment

The **NetBackup Master server** manages backups, archives and restores. It is responsible for all media (can be tape or disk) selection and maintains an internal database called the catalog. The catalog tracks backup and media and is used to quickly locate the correct media and backup items.

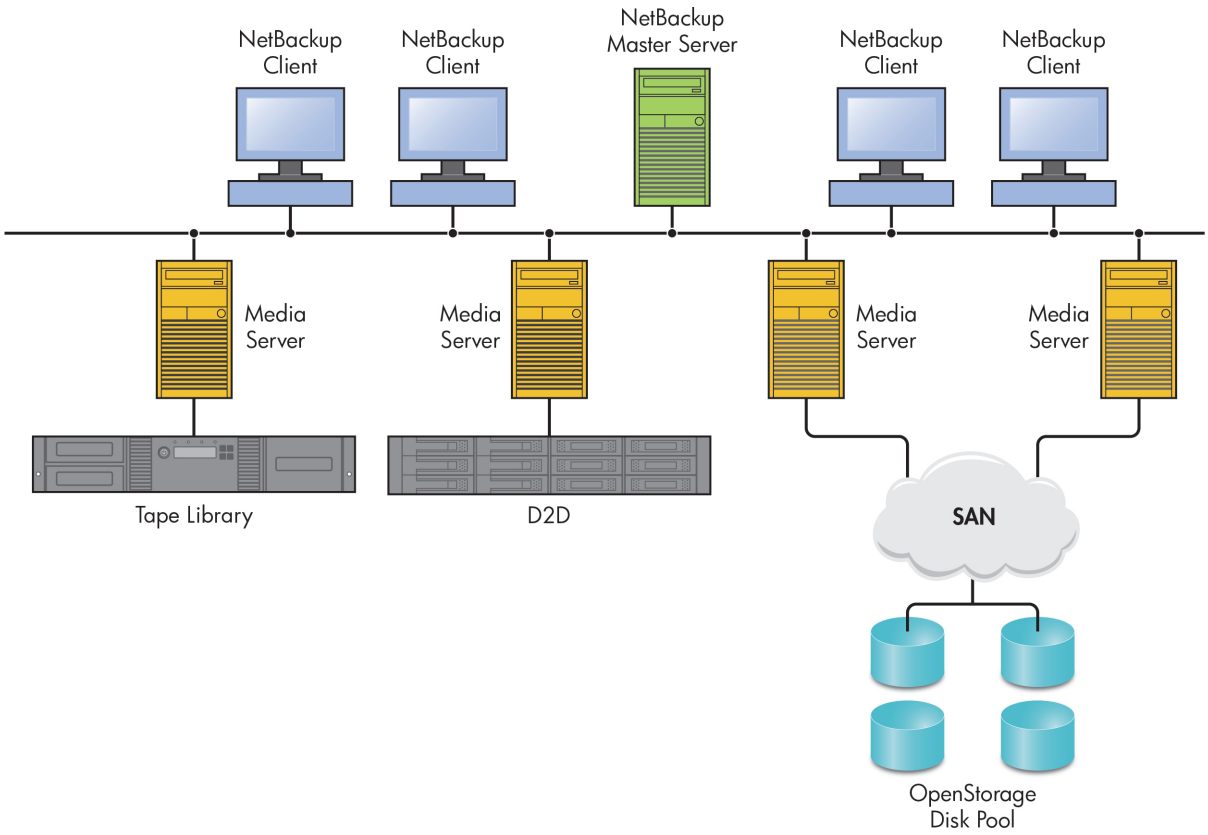
The **NetBackup Media server** distributes the load in large configurations. Storage devices are attached to media servers via SCSI, SAN or network connection. It is possible for a media server to be present on the same physical server as the master server. (A two-tier configuration is often used in smaller configurations.) In this case the media server is on the same server as the master server. A master server can control many media servers. It is possible in large enterprise scale operations to have multiple master servers. Often media servers are referred to in the following terms:

- **Storage Server** – when disks are connected directly to the media server I/O. In this configuration disks can be configured in an OpenStorage disk pool.
- **Device Hosts** – when physical or virtual tape libraries are attached.

- **Data Movers** – send data to external disk-like devices (Open Storage Appliances).
- **Clients** – are servers/workstations which have the NetBackup client software loaded and will back up over the network to their designated media server. See the Glossary for more terminology.

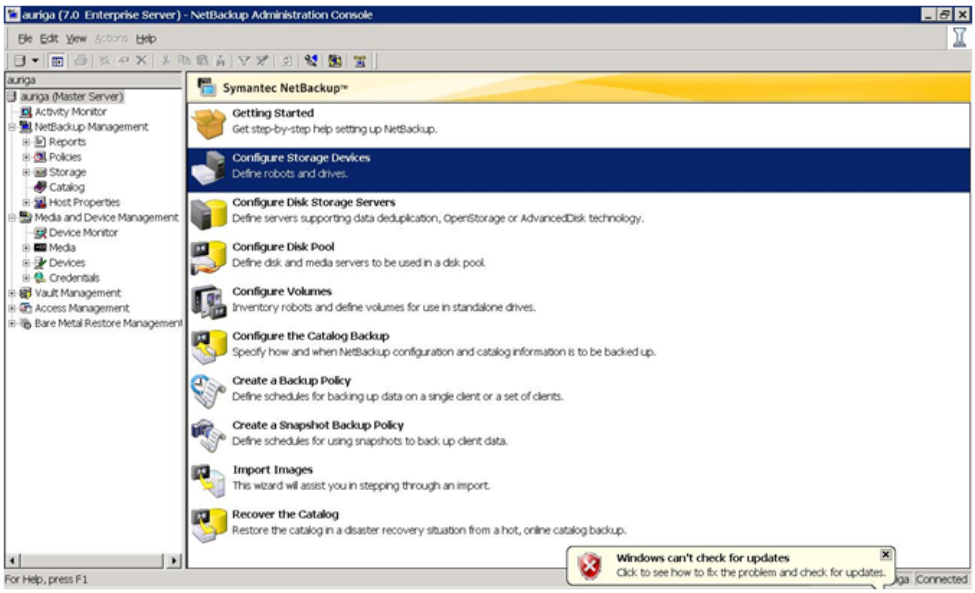
Figure 1 shows how the NetBackup components are interconnected. NetBackup is extremely scalable and can support a large, complex backup solution. Symantec provide guides on performance which must be used in planning a solution. NetBackup Master and Media server software is available for Windows, Linux, HP-UX and Sun Solaris platforms.

Figure 1 The NetBackup environment



NetBackup provides a Windows-based administration console shown in Figure 2. (There is also a scriptable command line interface). Prior to NetBackup(NBU) 7 some functions were only available as command line instructions. There is also a NetBackup backup/recovery client interface which can be used by clients to run backups and recover files. Archive functions are usually when the original file is deleted. There are also methods of copying backups to alternative storage locations for added resilience.

Figure 2 The NetBackup Administration console



The role of the HP D2D Backup System

The HP D2D Backup System provides disk-based data protection with data deduplication. For additional data protection and disaster protection D2D Backup Systems can perform replication of data over low bandwidth WAN links. This is a good solution to move data offsite without the media handling and transport costs. D2D Backup Systems provide either virtual tape or NAS emulation. This guide will only feature the NAS emulation and its implementation with NetBackup.

The D2D NAS targets have deduplication on by default and this cannot currently be changed. The NAS targets can use either the CIFS (Common Interchange File Standard) or NFS (Network File System) protocol. CIFS is used with Windows servers and NFS is used on all LINUX/Unix operating systems. This guide will cover the CIFS protocol for Windows.

NOTE: It is important to note that, besides the more obvious disk capacity specification, there are some important additional NAS specifications such as maximum files per share, maximum number of shares, and maximum number of concurrent open files. These vary depending upon the D2D Backup System model, see Appendix A for details.

Network connection

NAS shares are all accessed from the network connections and use the CIFs or NFS protocol.

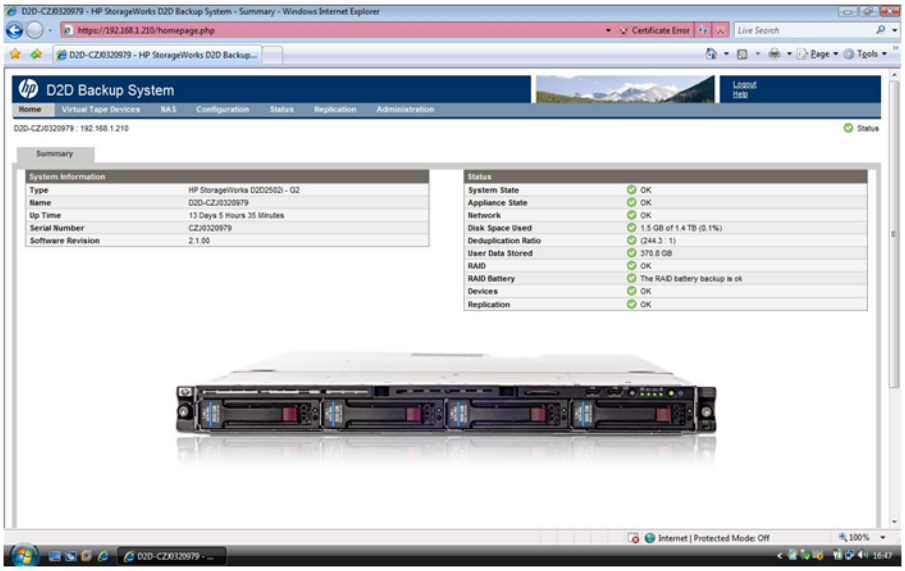
NOTE: It is important to check that the correct network settings are used especially if the D2D Backup System is to join a domain. Ensure that the entries for the DNS server, domain and gateway are correct. (Normally the network admininistrator will provide these).

All D2D Backup Systems have dual 1Gb Ethernet connections; the larger D2D4312 and D2D4324 units have two additional 10Gb Ethernet connections. The network interfaces can be used on different subnets or can be bonded together (not 1GbE to 10GbE) for high throughput or high availability mode. It would be normal to have inter-site replication configured for a different subnet.

The initial IP address can be set using the utility disk supplied with each D2D Backup System. This setup utility uses UDP protocol and 'discovers' all D2D appliances present on its subnet. The alternative is to use the default DHCP setting and allow a DHCP server to provide the networking information. If the dynamic DNS option is set, the D2D Backup System will be entered automatically in the DNS system. Normally, static IP addresses are used for NAS devices configured on the D2D Backup System.

Connect the D2D system to the network logon via the Web Management Interface. (Enter the IP address or D2D name into a standard web browser. This is of the format D2D-xxxxxxxxxx where xxxxxxxxxx = D2D product serial number.) The web browser will issue a security warning because the web browser will not have the D2D web browser certificate installed. The main menu screen is shown below in Figure 3.

Figure 3 Home — Summary page, example shows HP D2D2502i



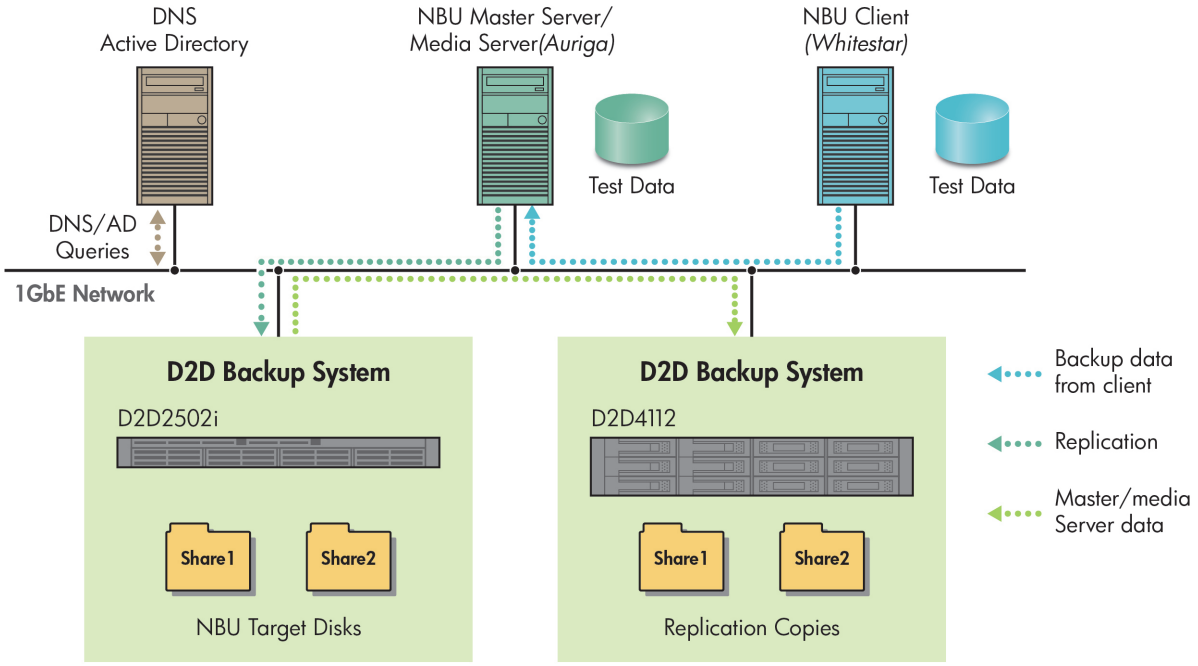
HP D2D Backup System licensing

HP D2D Backup Systems require licenses for capacity upgrades and when acting as a target for replication. Series 4100 and 4300 D2D Backup Systems have the capability to add more disk 'shelves' in order to expand the capacity. As well as the actual hardware, capacity licenses must also be loaded. The licenses normally ship with the disk expansion products. (The Series 2500 D2D Backup Systems cannot be expanded.) In an active-active configuration both D2D systems act as targets and require replication licenses.

Test setup

Figure 4 shows a simple test setup for HP D2D Backup Systems configured as a NAS target for Symantec NetBackup. This configuration will be used as an example in this guide.

Figure 4 Test setup



NOTE: The server Auriga is also in effect a 'client' as far as backups are concerned.

For more information

Symantec NetBackup is a very feature-rich data protection application. This guide is only intended to cover basic use for filesystem backup using the D2D Backup System with NAS shares and to use the low-bandwidth replication feature to move data 'offsite'.

The guide covers the basic procedure for backup/restore and disaster recovery. It also stresses the importance of regular catalog backups and illustrates the recovery onto a new server in the event of a disaster which may have damaged the master server.

Some advanced features such a the granular recovery option for Microsoft Exchange Server will not work with the D2D Backup System because they perform multiple random read/writes. Workarounds are shown for this issue on the Symantec website.

For more information refer to:

- Manuals available from the Symantec website at: http://www.symantec.com

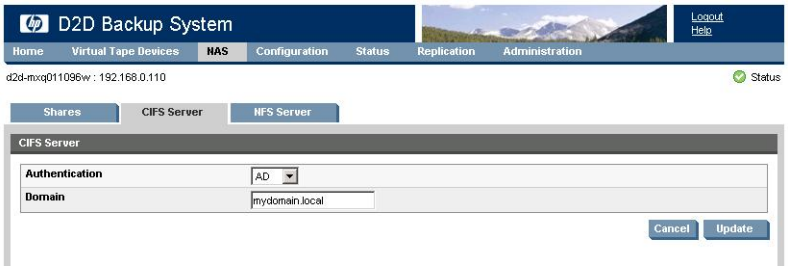
  Symantec NetBackup user guide Vol 1/Vol II
  Symantec NetBackup Tuning guide
  Symantec NetBackup Troubleshooting guide

- General D2D information at: http://http://www.hp.com/go/D2D
- The D2D Best Practices Guide at: http://http://bizsupport2.austin.hp.com/bc/docs/support

2 Configure the D2D CIFS server

The first step in configuring the D2D device as a target for backups from Symantec NetBackup is to configure the CIFS server on the D2D platform.

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 (least secure)
- **User** – Local (D2D) User account authentication
- **AD** – Active Directory User account authentication

NOTE: NFS assigns access by IP address and essentially maintains an access control list.

More about authentication modes

None: This authentication mode requires no username or password authentication and is the simplest configuration. NetBackup will always be able to use shares configured in this mode with no changes to either server or NetBackup 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 NetBackup media server and configuration changes to the NetBackup services. Individual users can then be assigned access to individual shares on the D2D. This authentication mode is ONLY recommended when the NetBackup 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. This is the recommended authentication mode, if the NetBackup Media server is a member of an AD domain.

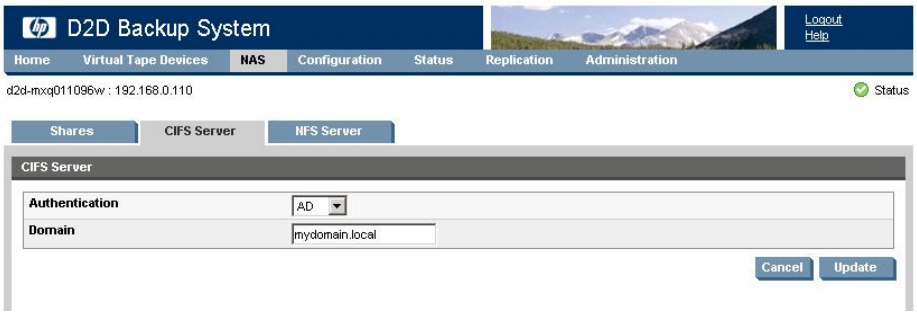
Configuring AD Authentication Mode

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

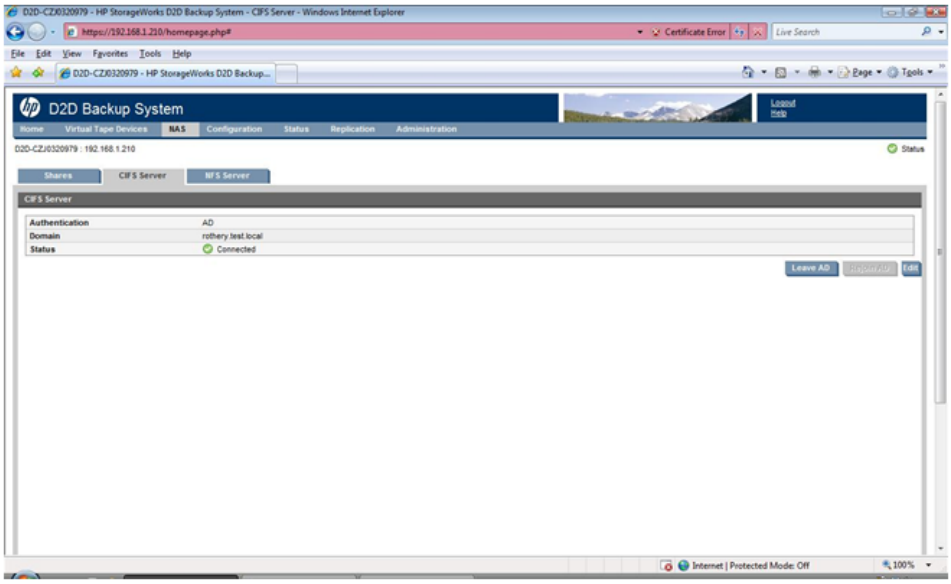
- Join the D2D CIFS server to the AD Domain.
- Create or specify a user to be used for backups.
- Apply user permissions to D2D shares.

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. Select **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. If successful, a message is displayed and the CIFS Server screen is displayed.



More about DNS

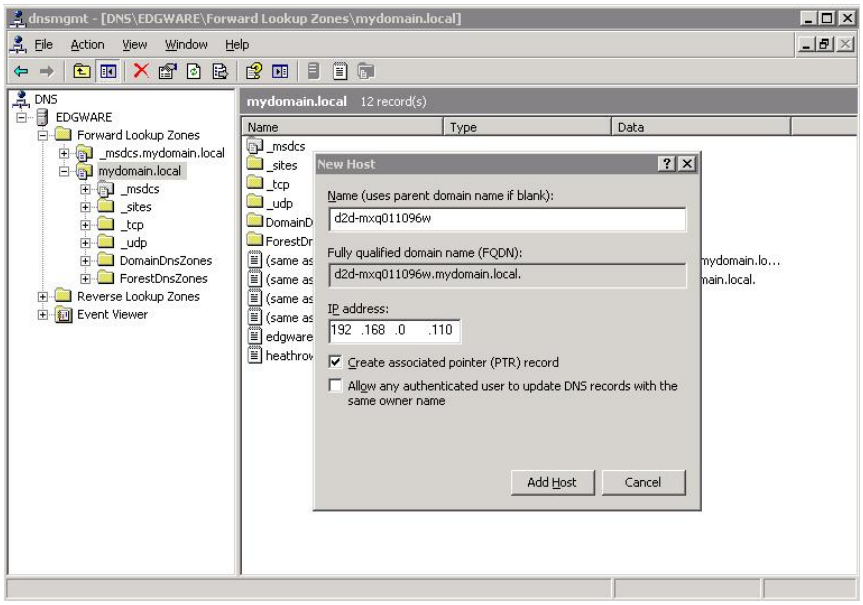
Normally joining the Active Directory Domain updates the DNS entries automatically. DNS is an essential component of Active Directory.

NOTE: If there are problems check that the D2D Backup System has an entry in the DNS (Domain Name System) server. Use the command line to check that the D2D hostname resolves to an ip address and vice versa. (Use `nslookup <IP address>` and `nslookup <D2D hostname>`.)

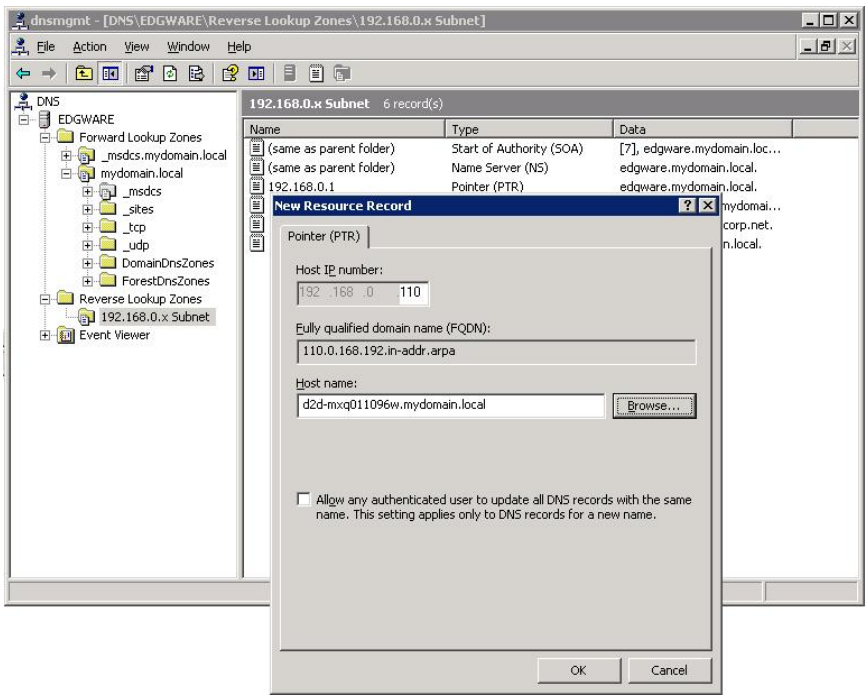
After joining the domain, the DNS server should be automatically updated with Forward and Reverse Lookup zone entries, however, some DNS configurations do not allow this. In this case, the user must also configure the domain's DNS server to be able to correctly manage the D2D shares, as follows:

From a windows client server that has domain and DNS management tools installed launch the DNS management tool. (From 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 belongs with the hostname and IP address of the D2D.



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



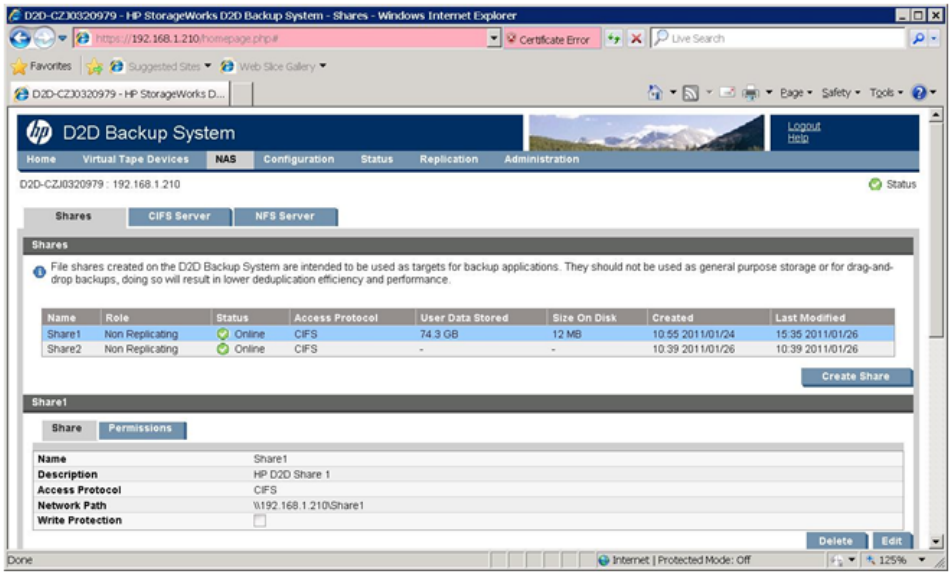
To create shares and grant access permission

Now that the D2D 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**.

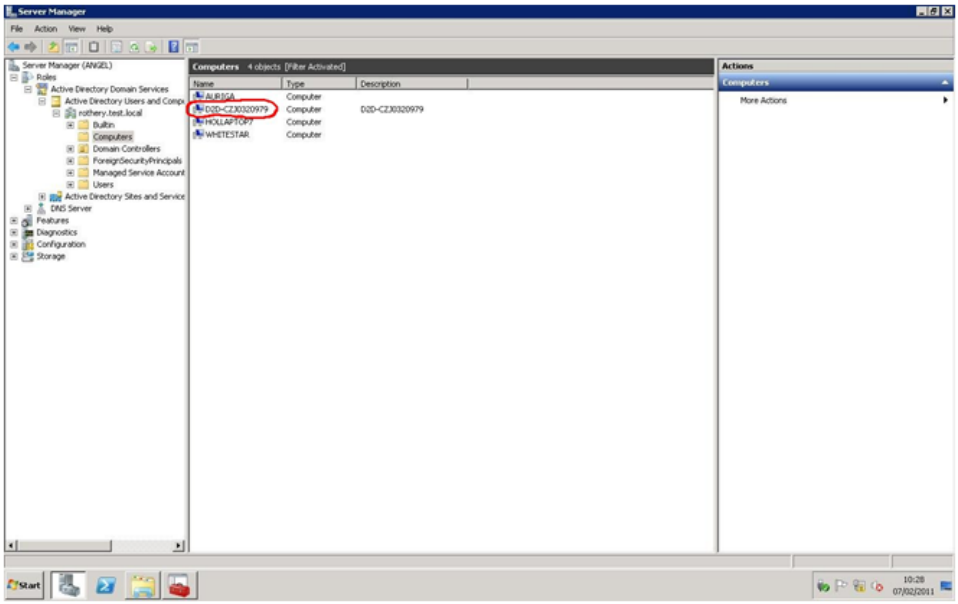
   The shares have default names of Share1, Share2 etc. but these can be changed if desired. Provide a share Name and Description, select the **CIFS** protocol and click **Create**.

   The following example shows configured shares. The Permissions tab will indicate that authorization is managed by Active Directory.

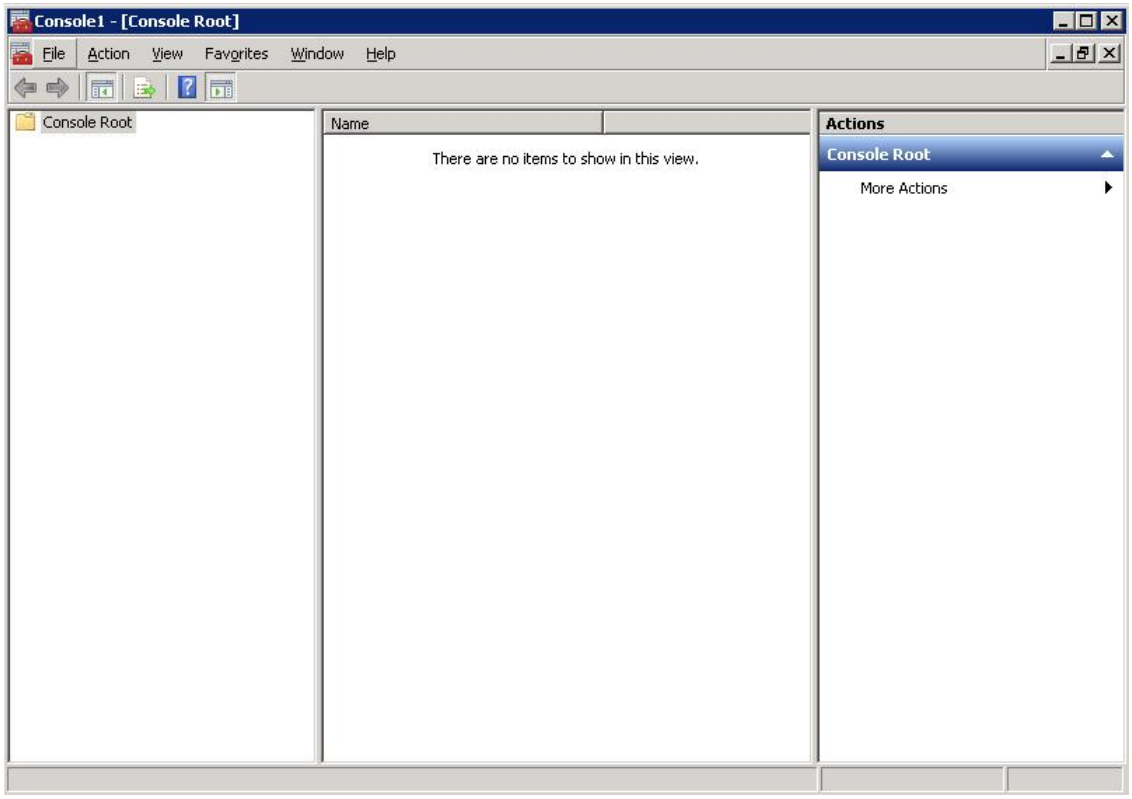


NOTE: Normally a particular media server may be assigned one share in the backup application but it is possible to create sub-directories under the Share1 level for individual servers using Windows Explorer. To view a share with Windows Explorer enter the IP address and share name into the top box in the format \\192.168.1.210\Share1. If you have set Active Directory authentication, you will need to allow the domain login access rights first.

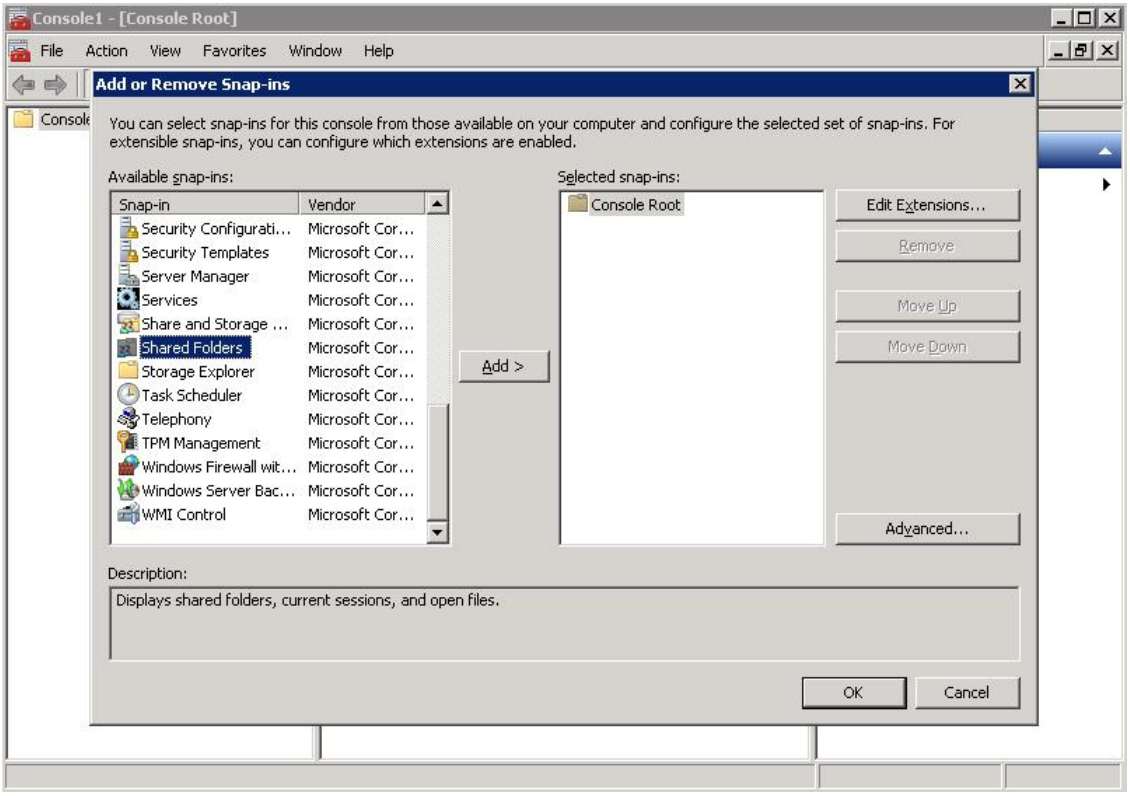
2. To configure access rights, log in to the Active Directory server as Administrator. Run server manager and check that the D2D Backup System is shown under **Computers**. In the following example, the D2D Backup System is highlighted.



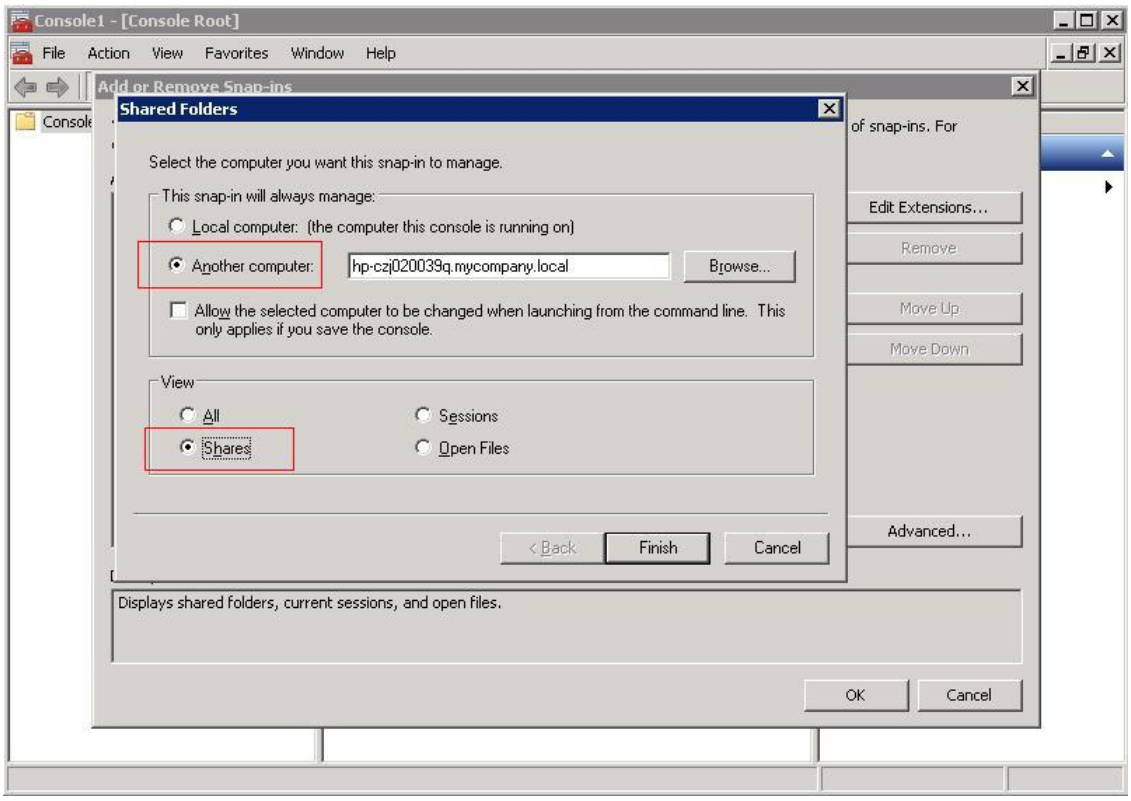
3. Now that the D2D Backup System is a member of the domain its shares can be managed from any computer on the domain by configuring a customized Microsoft Management Console (MMC) with the Shared Folders snap-in. To do this first open a new MMC window by typing `mmc` at the command prompt or from the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



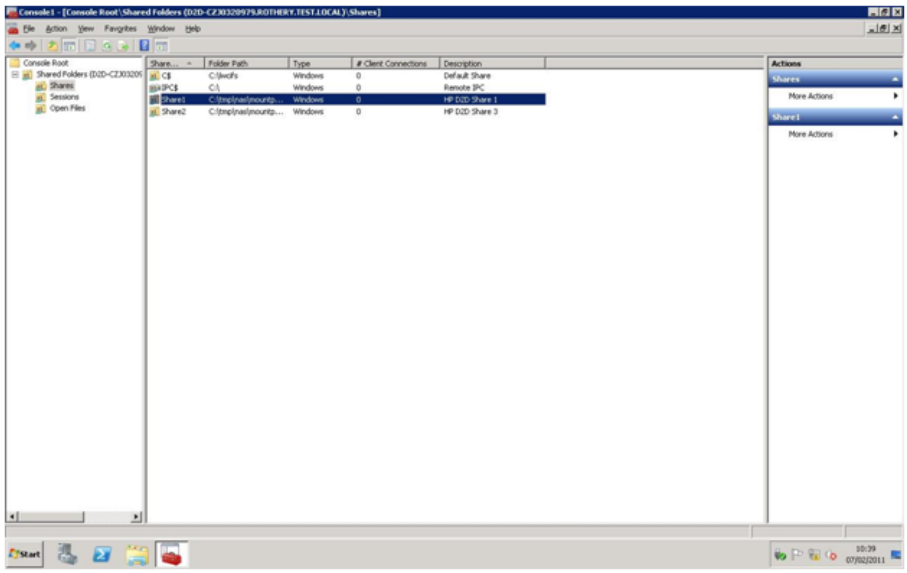
4. To this empty MMC window add the Shared Folders snap-in. Select **File — Add/Remove Snap-in ...,** then select **Shared Folders** from the left-hand pane.



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

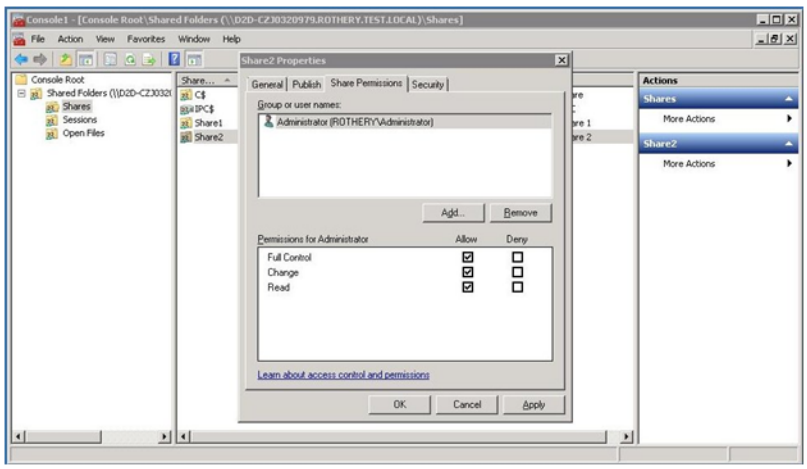


6. Click **Finish** and **OK** to complete the snap-in set up.



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

7. Save this customized snap-in for future use.
8. 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**.



9. 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.

This completes the process. To test access login as the domain administrator and use Windows Explorer to show the D2D share.

The NetBackup Services (which can be listed using the **Activity Monitor** from the NetBackup administration console) must be changed from local account to domain administrator logon if AD is used to control access to the D2D file shares. Each service must be stopped and restarted for each account change. The logon is changed from the Windows 'Services' configuration. (See page 383 of the NetBackup Administrators guide).

Having set up the shares the Symantec NetBackup administration console can be used to set up the Storage Units, as described in the next chapter.

3 Configuring disk-based storage

Once you have set up the shares the Symantec NetBackup administration console should be used to set up the Storage Units.

NetBackup Storage has three basic categories:

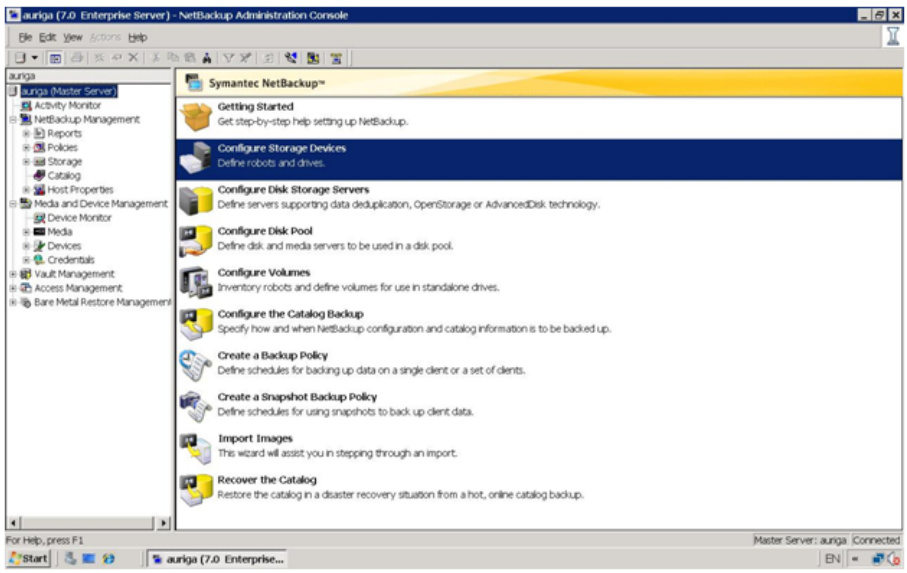
- disk, which is the category used with the D2D NAS configuration for NetBackup Storage
- media manager, which is for tape libraries and should be used for real tape devices and virtual tape libraries
- NDMP, which is a special protocol designed to instruct NAS devices (filers) to back up to a real tape drive directly attached to the NAS peripheral. Data can then be moved from the NAS share to tape.

Disk-based storage in NetBackup 7 can be one of the following categories:

1. **Basic Disk.** This is locally-attached disk storage or network-attached disk storage presented as a filesystem to the media server. The directory structure is specified when the storage unit is created. This is the standard configuration for D2D NAS. Basic disk cannot be used in a storage lifecycle policy.
2. **NearStore**. This is a special configuration for NetApps NAS only. This is also on OpenStorage option.
3. **SnapVault.** This option is only usable if the NetBackup snapshot client is licensed. (NetApps NAS devices only).
4. **OpenStorage (vendor name).** This is used for intelligent storage devices which are OST protocol aware. This option is vendor specific.
5. **Advanced Disk.** This option allows NetBackup to use dedicated disk storage (can be network attached from NetBackup 7 onwards). This allows disks to be part of a storage 'pool'. Advanced disk is licensed under the 'Enterprise Disk License'. Storage Lifecycle Policies can be used with Advanced disk.
6. **PureDisk** can only be used if this license installed. This provides software based deduplication.

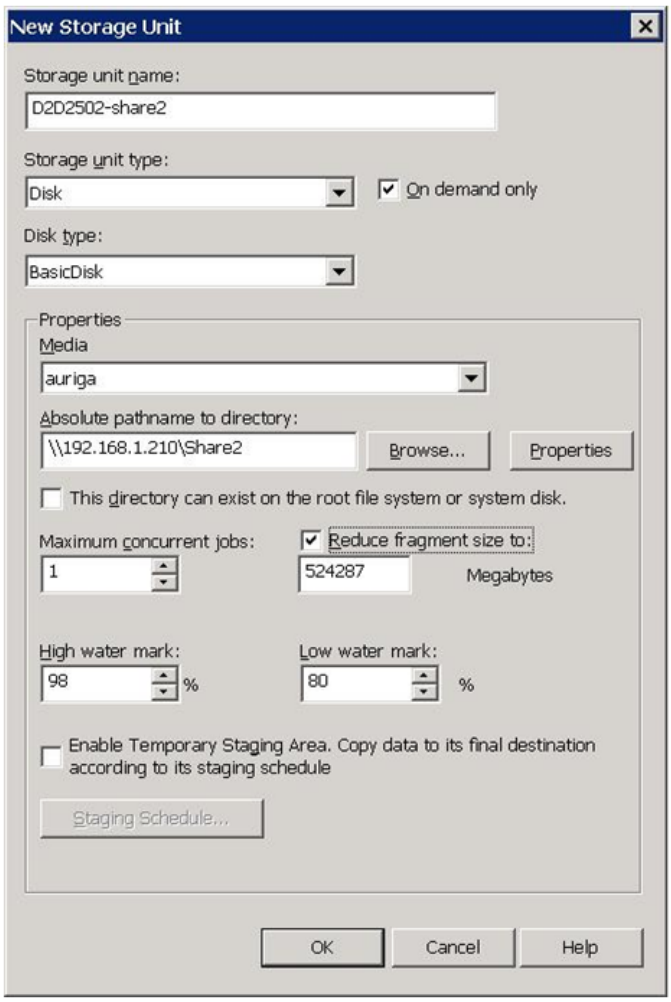
To configure storage devices

1. Run the Symantec NetBackup management console and click on the **Configure Storage Devices** icon in the wizard.



2. To configure the D2D NAS share select **BasicDisk**.

   The following example shows the configuration screen for a new storage unit for the media server in the test configuration shown in Figure 4. The share is specified as the IP address and sharename. The media server has the name of the media server 'auriga'.



NOTE: The Storage Units define the logical link between backup destinations and media servers. It is possible in advanced configurations to specify a 'group' of Storage Units. Symantec do not recommend configuring multiple storage units to the same share. This is because the individual storage units will assume that they have exclusive access.

In order to increase the number of streams to optimize D2D performance, increase the **Maximum concurrent jobs** for the storage unit. (This equates to number of tape drives in a real tape library.) However, be careful that the maximum streams the D2D can manage is not exceeded (see Appendix A). It is good practice to group servers together by application. For example, arrange that file and print servers are backed up to the same share if they are likely to contain some degree of duplicate data because this will improve deduplication results.

In order to increase the number of streams to optimize D2D performance, increase the **Maximum concurrent jobs** for the storage unit. (This equates to number of tape drives in a real tape library.) However, be careful that the maximum streams the D2D can manage is not exceeded (see Appendix A). It is good practice to group servers together by application. For example, arrange that file and print servers are backed up to the same share if they are likely to contain some degree of duplicate data because this will improve deduplication results.

The maximum **fragment size** defaults to 524287. The data is stored on disk in fragments to ensure that the backups do not exceed the maximum size file allowed by the file system. The

space is not pre-allocated so there is no concern about lost disk space. NetBackup will automatically create new fragments as required. This parameter can be left at default.

If the **On demand only** checkbox is set, only backup policies that are specifically assigned to this storage unit can use it. If this option is set and policies do not specify a storage unit, they will not run, so take care.

The **High** and **Low water mark** are parameters used by NetBackup to determine when to release disk space occupied by expired backup policies. Once the high water mark is reached expired policies will be deleted until none remain or the low water mark is reached. Deleting expired backup will cause housekeeping overhead and this needs to be monitored (from the D2D Web Management Interface) to ensure it is within sensible limits. Housekeeping should normally not be increasing week on week. See the *D2D Best Practices Guide* for more information about monitoring housekeeping.

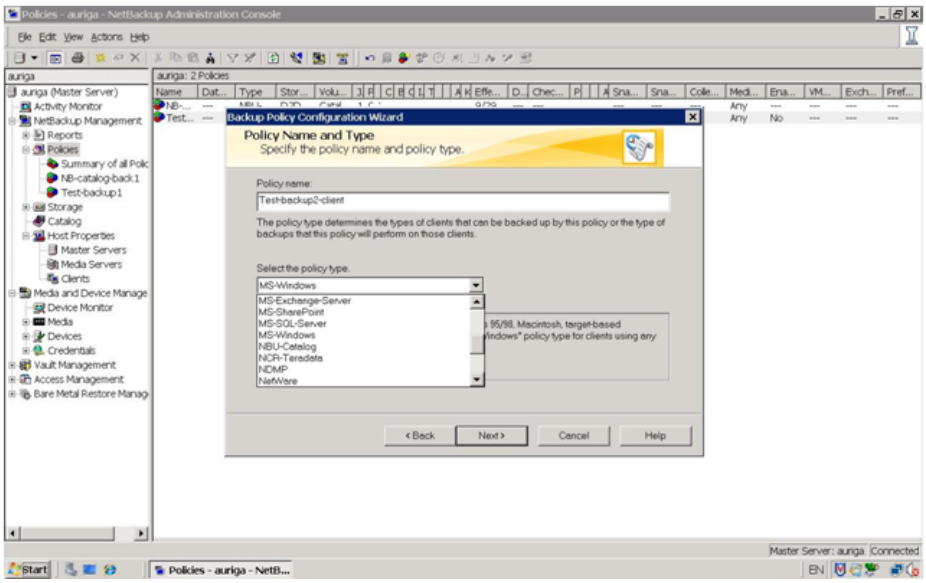
3. Click **OK** to save the configuration settings.

4 Backing up to and restoring from D2D NAS shares

Creating a backup policy

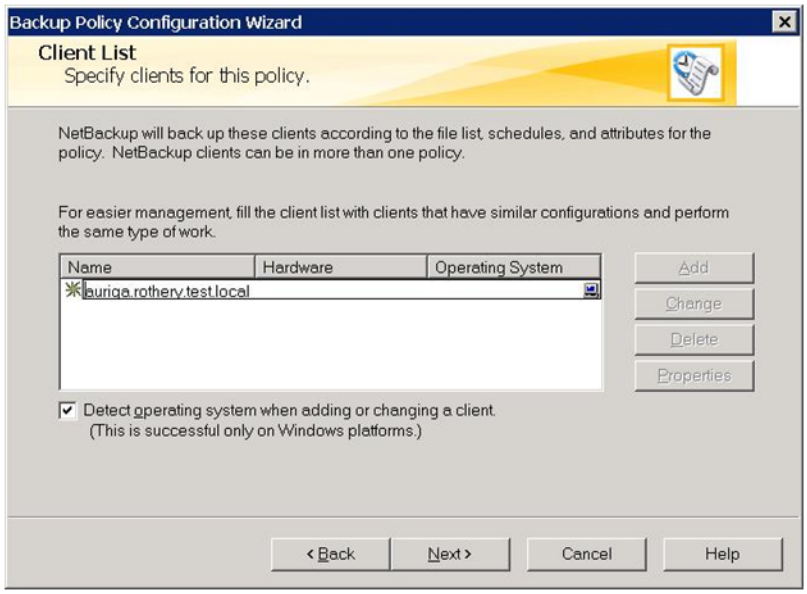
This section will describe how to create a backup policy using the storage unit created in the previous section. NetBackup 7 provides a 'wizard' for policy creation.

1. Open the NetBackup Administration console and select the **Policies** section from the left hand menu tree.
2. Select **Actions – New Policy** from the top menu, enter a policy name and tick the box to select the wizard.
3. Select the **policy type**. The policy type in this case will be MS-Windows for a Windows file system backup. For other types of backups it may be necessary to load particular agents.

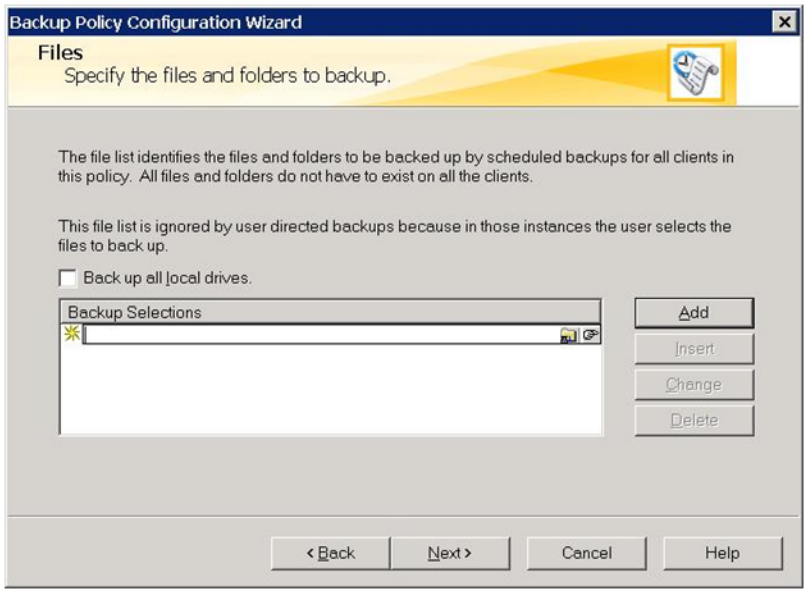


4. Click **Add** and specify the client that will be backed up. In the example shown the client is co-existing with the master server although normally it would be attached via the network.

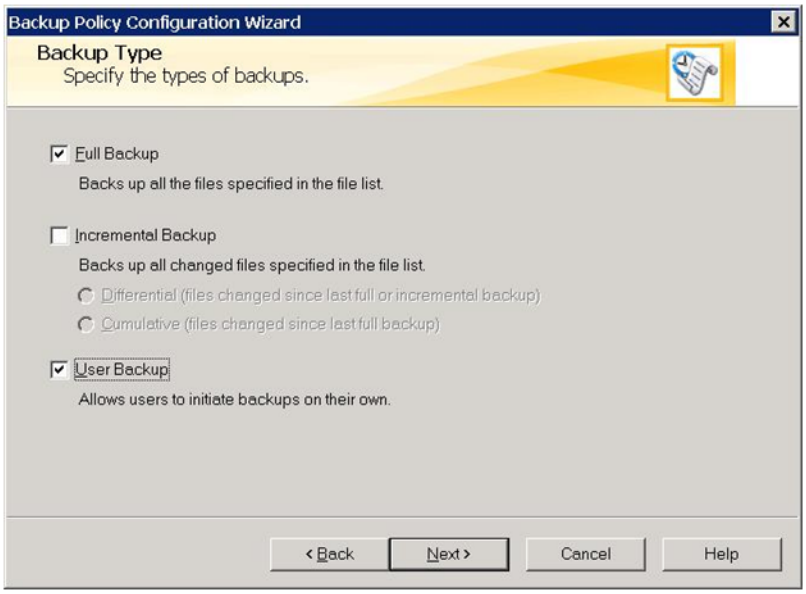
   If the desired client is not detected it may be blocked by the Windows firewall. Either turn off the firewall or open the appropriate ports. These can be specified in client properties. The client name can either be entered or selected from a list (click on small computer icon).



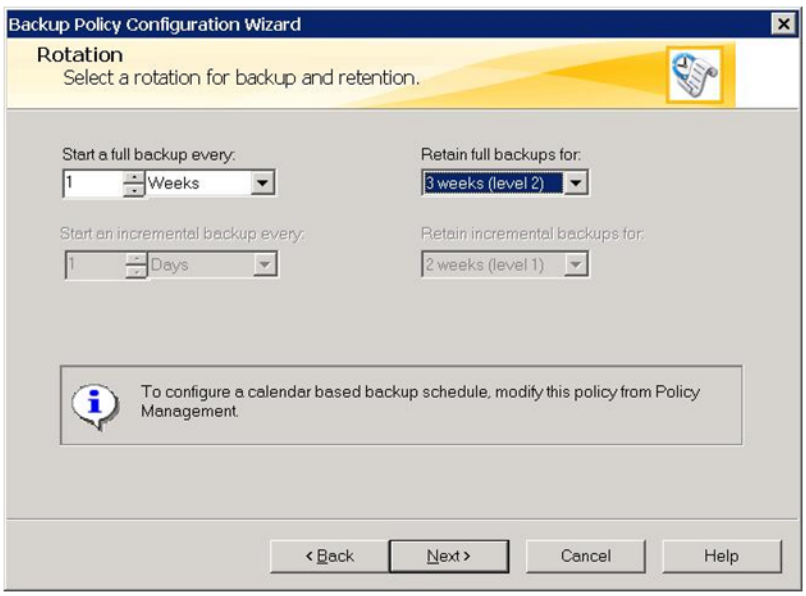
5. The next step is to specify the files for backup. Select **Add**, click on the small folder icon and select the desired directory path.



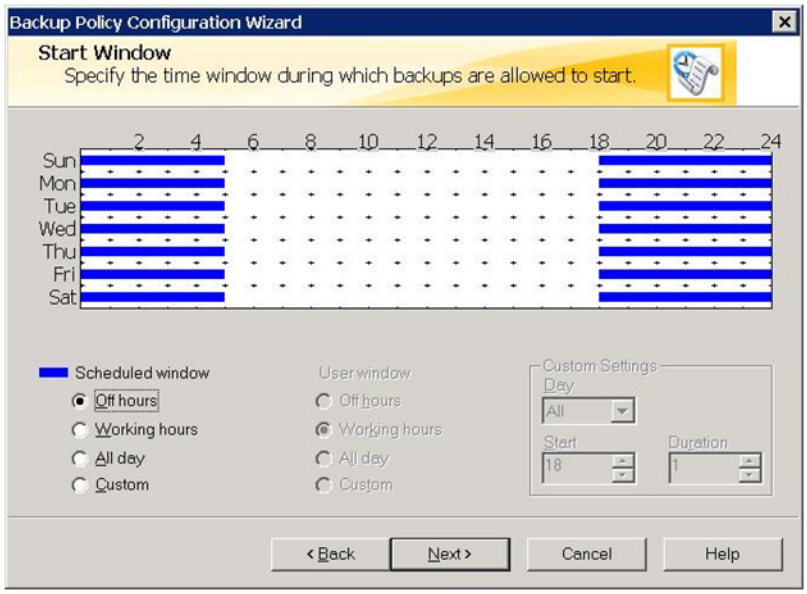
6. Click **Next>** to display the Backup Type screen. This screen is used to specify **Full Backup** or **Incremental Backup**. **User Backup** can be selected as required.



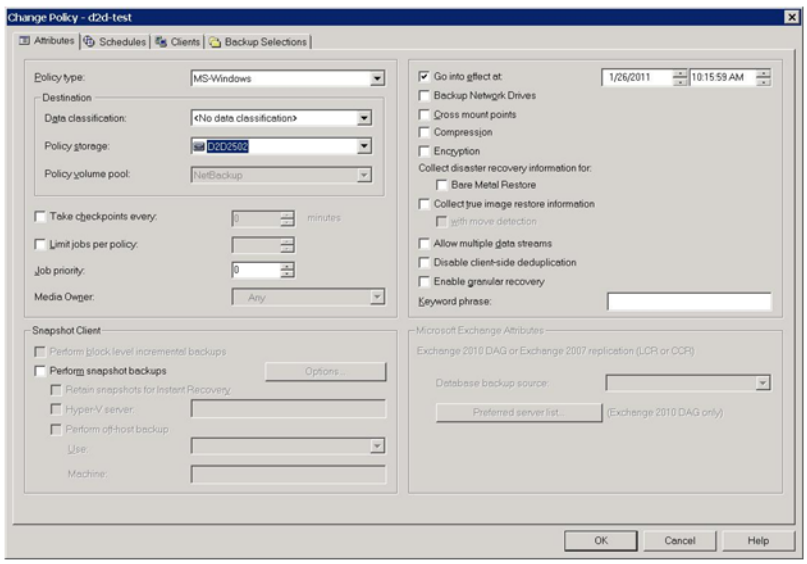
7. The next step selects the **Rotation** policy. This is how long the policy is stored before overwriting the data. As an example it would be desirable to keep the full weekly backups for a month and the full monthly backups for 6 months. Incremental may only be retained 2 weeks.



8. Click **Next>** and specify the start time.



9. The policy is now fully configured and the next screen completes the process.
10. The created policy should now be displayed in the main NetBackup Administration Console under the **Policies** section. Click on the actual policy and it is possible to show some additional attributes.



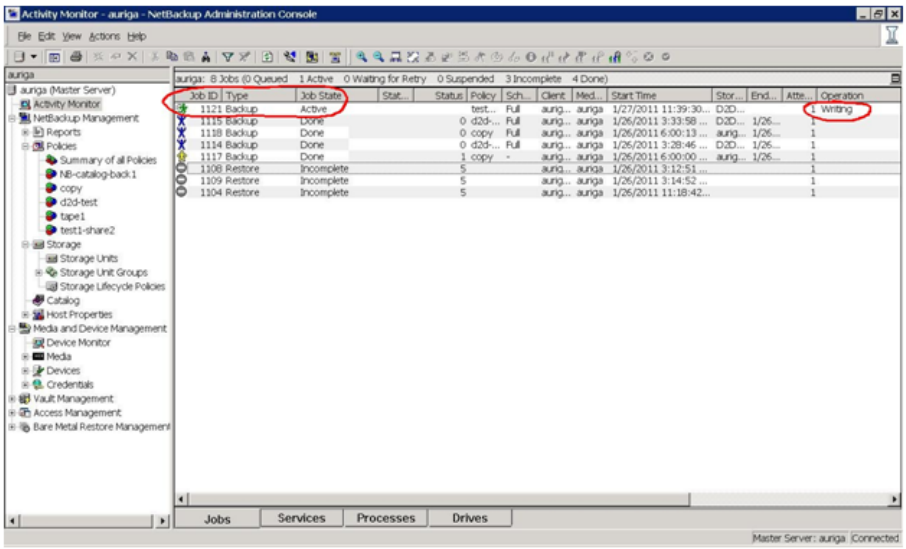
There are some important points to note in this screen.

- **Data classification** allows administrators to classify data on relative importance as part of storage lifecycle management. It is not supported with basic disk. (It requires the Advanced Disk option.)
- The **Encryption** option should be un-ticked because encryption effectively randomizes data and this will result in no deduplication.
- The **Bare Metal Restore** option is only required if this feature is used.

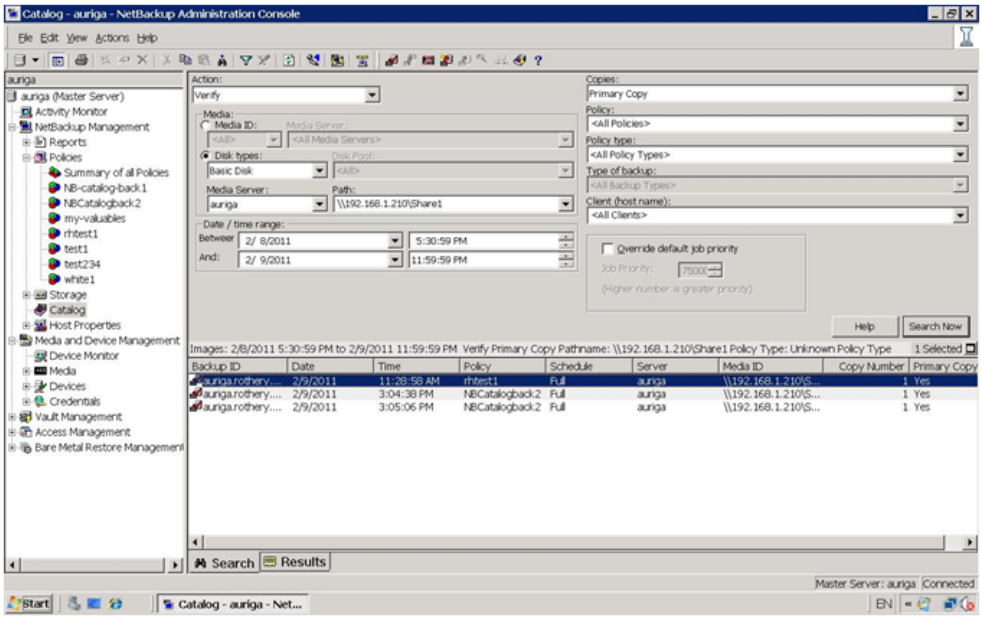
11. This completes the policy settings.

To run the backup policy

1. To run the policy manually click on the policy, select **Actions** from the top menu and run manually. To monitor the progress click on the **Activity Monitor**. A sample screen is shown below.



2. When completed the backup details can be seen by searching the catalog. Click on **Catalog** and search the catalog for particular storage units.



You will see in the above example that the disk types selected is Basic Disk and the media server is 'auriga'. The example shows three backups listed for the storage unit.

In this screen it is possible to expire backups that are no longer required; expired backups are removed by device cleanup. Normally the files are left to expire at the time determined by the policy.

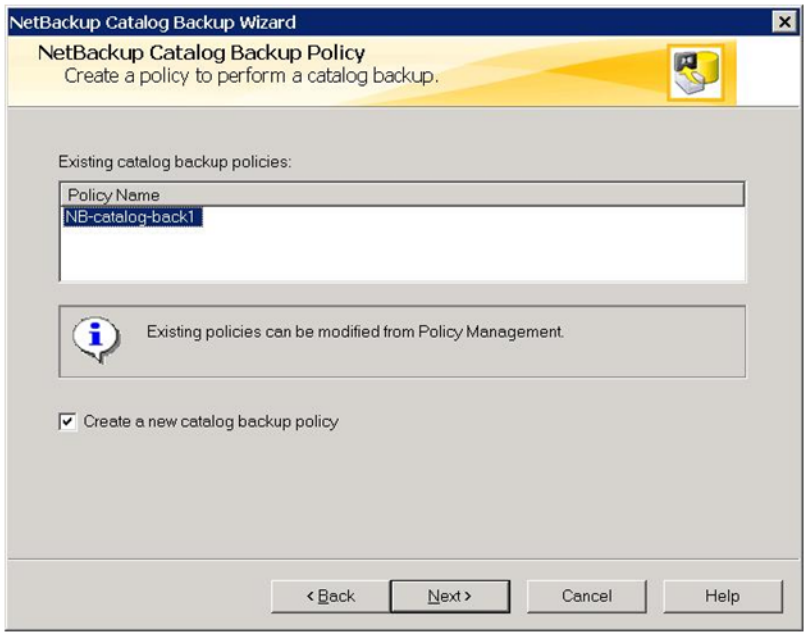
Selecting the active job will give more information on progress. (Also note that the **Services** tab is included on this screen. This is useful in checking that the correct services are running. You may see that Device Manager service is not running. This is correct if no tape library is configured.)

Catalog backup

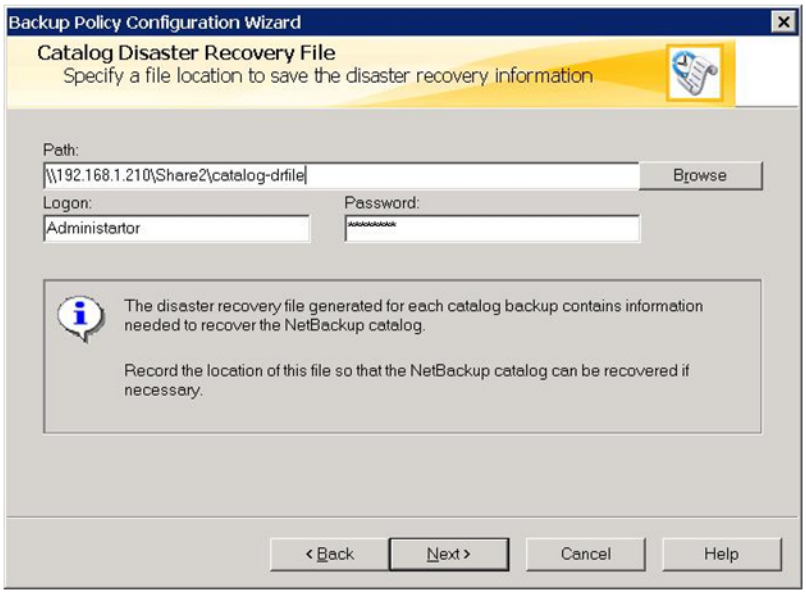
The information about the backup is stored in a database held on the Master Server; this is known as the catalog and must be regularly backed up to ensure recovery. Netbackup 7 introduced the ability to perform 'hot' catalog backups. This means that the database can be backed up in an open state which effectively permits backup any time. (Note that 'cold' catalog backups are not permitted under NetBackup 7)

Catalog backups are configured using a wizard.

1. Click on the icon labeled **Configure the catalog backup** from the NetBackup Administration Console. The first screen will request a name for the catalog backup policy as shown below.



2. Click **Next** and the catalog backup policy screen is displayed. This screen is used to specify full or incremental backup. (Remember catalog backup can be large in enterprise class configurations.)
3. The next two screens specify the rotation policy and backup window exactly as in a normal file backup.
4. The next screen is very important and is used to specify the location of the catalog disaster recovery file that is vital for catalog recovery. This file can be stored on the D2D or another disk media attached to the media server but it needs to be stored offsite along with the catalog backup. (Note: both DR File **AND** Catalog backup are required for recovery).



5. It is also possible to e-mail the DR file to an E-mail address in the next screen. This then completes the policy wizard for the catalog backup.

D2D NAS open file limits best practice

Each D2D Model has different limits for the number of open files it can support – see Appendix A. Event logging on the D2D will inform the user if any of these limits have been exceeded, so it is a best practice to regularly check the Event logs because backups may pause when the number of open file limits is exceeded.

There are separate Open file limits for files that are less than 24 MB (generally dynamic control files being accessed all the time during the backup and those that are greater than 24 MB such as the fragment sizes we set previously in the Storage unit parameters.

Some specific backup policy types such as Exchange are known to open up many control files (less than 24 MB) during a Storage Group backup and these can be monitored on the D2D NAS share using Windows Explorer. Having checked the limits in Appendix A it may be necessary to reduce the number of Exchange backups going to the D2D NAS share simultaneously to prevent exceeding the open file limits.

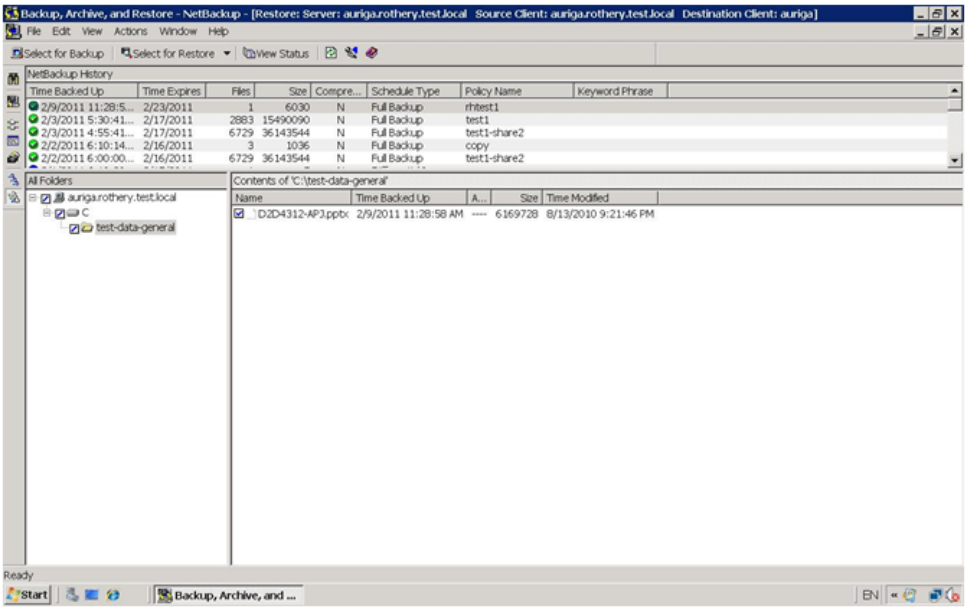
These limits exist because the D2D NAS is not a simple NAS filer but a deduplication appliance allowing the customer to store more backups on the same physical disk capacity than simple NAS filers. In order to do this it is necessary for a memory allocation to be applied which in turn limits the number of open files possible.

Restoring files from the backup

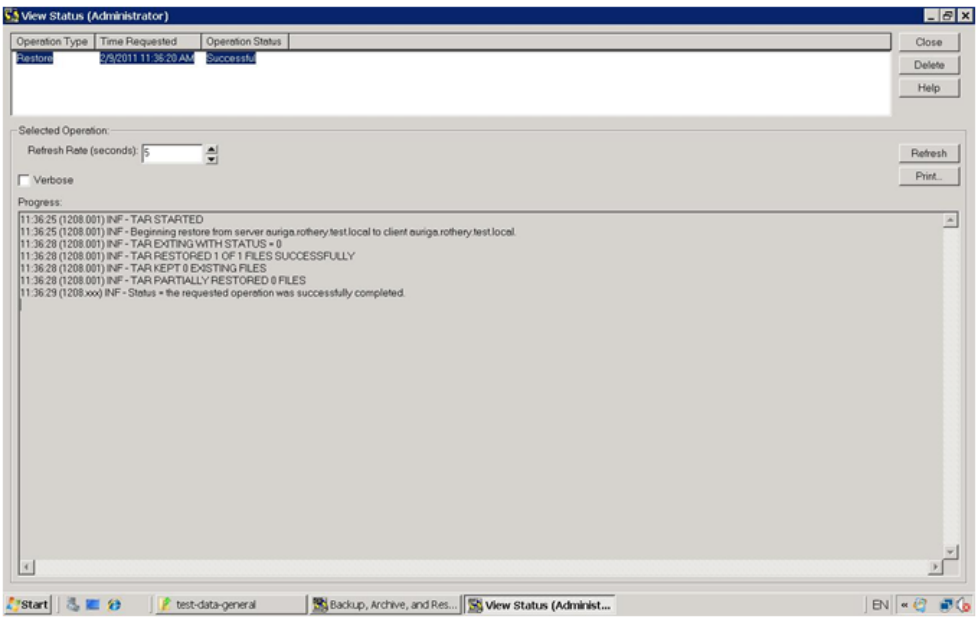
Restoring files is performed using the NetBackup Backup, Archive and Restore client. This can be run from the master server or a client. Clients can have the ability to restore their own files if necessary.

1. Click on the icon which is normally on the desktop of the master server and clients.

2. Select a backup policy from the list to display the relevant directory tree. This information is obtained from the catalog. Tick the box of the required file and use the **Actions** menu to initiate the restore.



3. View status will show progress, as illustrated below. It is also possible to restore files to different locations and other servers.

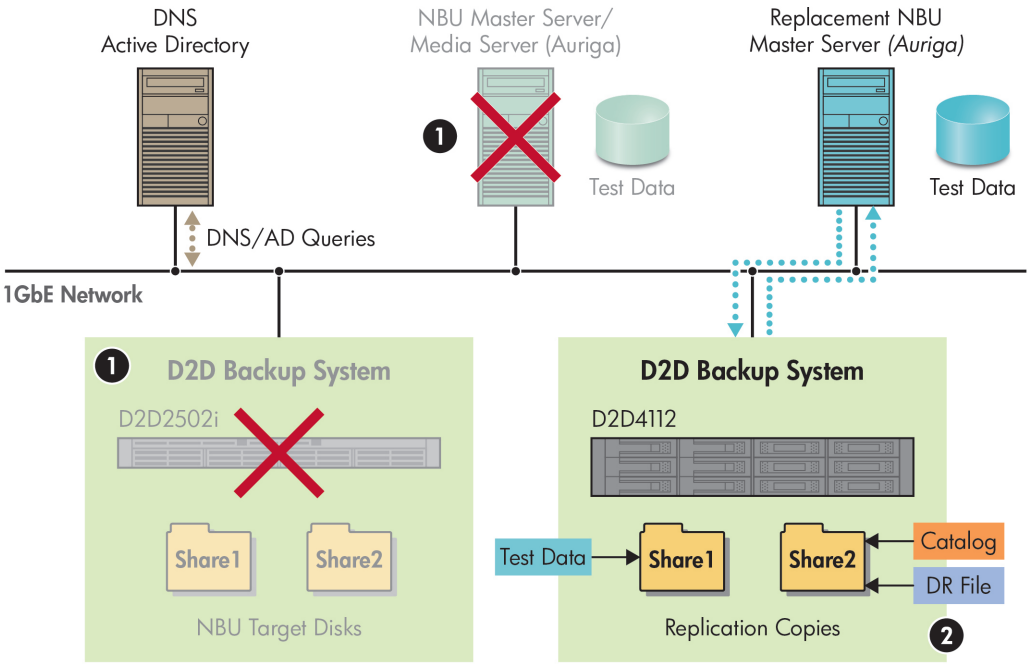


5 Recovering from a disaster situation

This section will describe how to recover files from the D2D Backup System assuming that the master server and other components are lost. In the test example used to illustrate this guide the NAS shares are set up to replicate between D2D Backup Systems. In a real life scenario the units would be located on different sites and connected via a WAN link. It is also quite likely that the master server would stay at a central location with several D2D Backup Systems connected to remote media servers, using replication to move data from the remote offices.

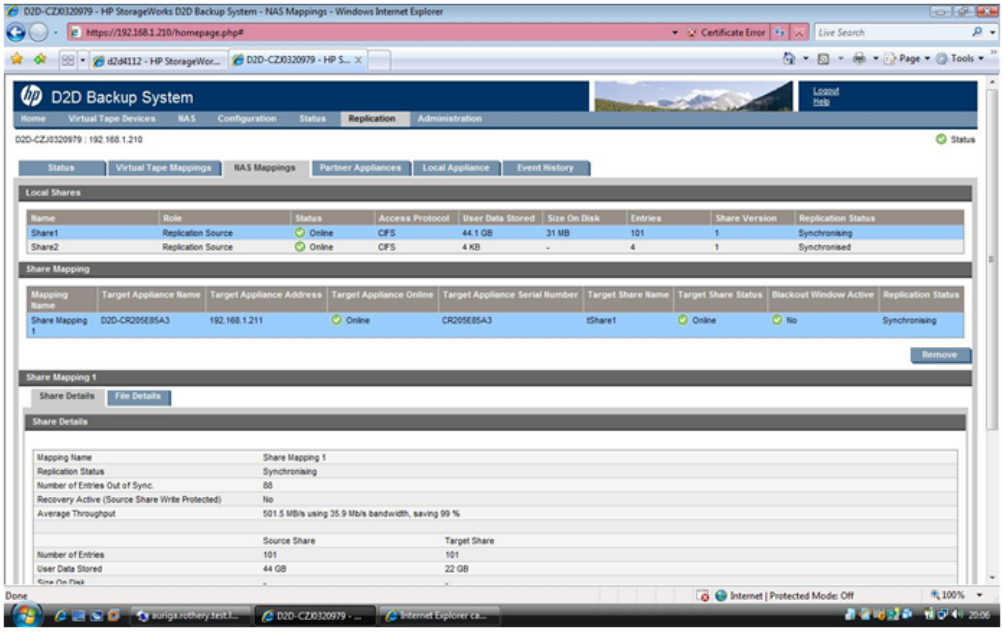
Figure 5 illustrates the recovery test scenario used for this guide.

Figure 5 Recovering the catalog and data after a disaster has removed the NBU Master Server and the remote office D2D system



1. X = unit lost in disaster
2. Delete replication mappings to promote and configure as Storage Unit for replacement master server

Setting up D2D replication is well covered in the *D2D Backup System User Guide* and has a wizard driven configuration system. Once configured the mapping for the NAS shares can be viewed from the D2D Web Management Interface. The test setup shown above has the following D2D mapping screen.



The target D2D Backup System will keep exact copies of the NAS shares from the target D2D Backup System.

In the previous chapter the NetBackup catalog wizard was used to make a catalog backup and drfile. The drfile is located on 'Share2 '; the catalog backup is located on Share1. (Although both could be in the same location.)

It is now assumed that the remote office is lost and so is the primary data on the D2D Backup System. However the copies of the share are intact on the target D2D Backup System.

The next step would be to 'promote' the target D2D Backup System by deleting the mapping to the source appliance. The shares are normally accessible in read-only mode but, with the mappings removed, they are normal write/read shares.

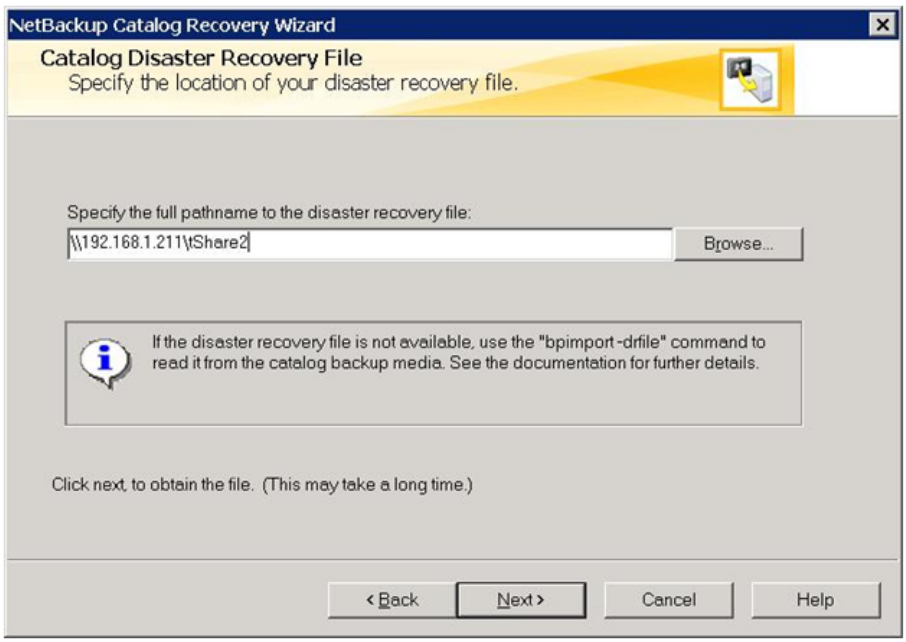
If the master server is lost

Should the master server be lost it will be necessary to recovery the catalog using the catalog recovery wizard. In this case any new master server must have the same hostname. The NetBackup software is installed specifying the Install Master Server option. The catalog is recovered using the Catalog Recovery Wizard once the NetBackup software installation is complete. It will be necessary to locate the disaster recovery file for the recovery wizard.

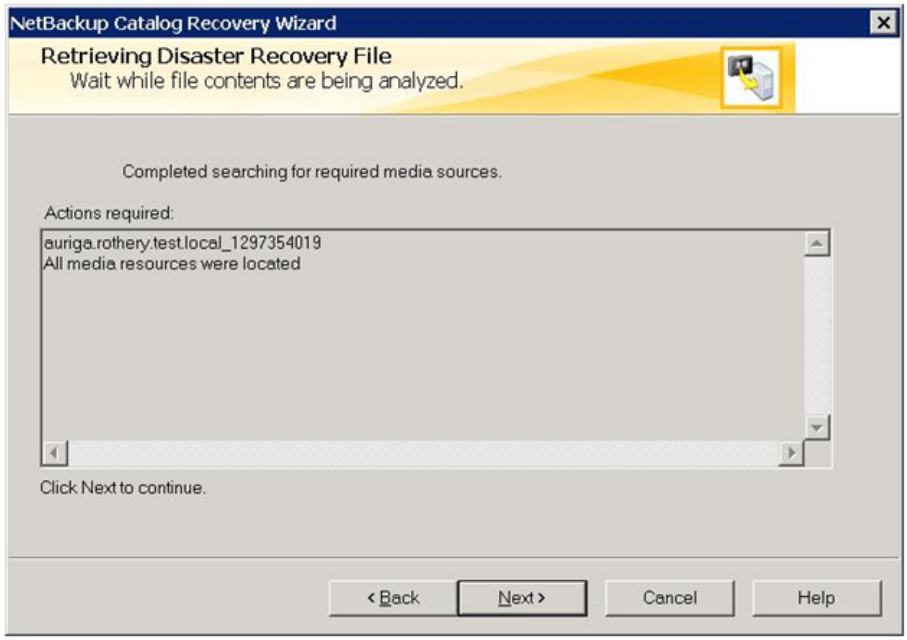
To recover the catalog:

1. Run the Catalog Recovery Wizard from the NetBackup Administration console.

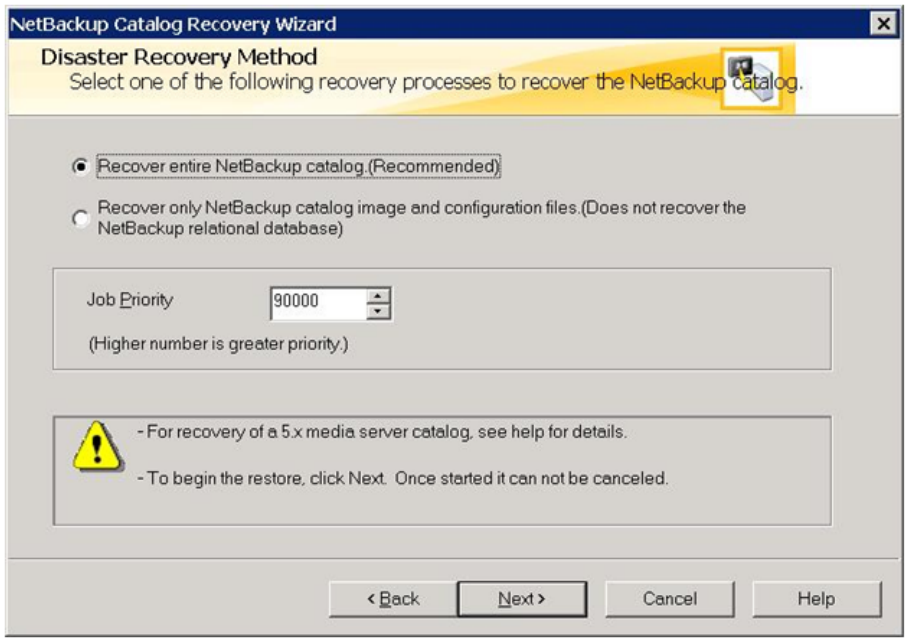
2. Enter the full pathname to the disaster recovery file. If the file is located on a D2D share it can be mapped to a drive letter and then the browse button can be used to locate it.



3. The system will then indicate that it is retrieving the disaster recovery file. On completion it will show the available disaster recovery files at that location. Click **Next**.



4. The next screen will restore the catalog. (There is an option not to recover the relational database.) Click **Next**.



5. The catalog recovery will proceed and advise of success.
6. Click next and

On successful completion of catalog recovery the NetBackup server should be restarted and then the restore client can be used (as we did previously in the restore section) to recover files as required.

A 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

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 NetBackup 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.

For example: An HP 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 information about:

- Installing the HP StoreOnce D2D Backup System
- Using the HP StoreOnce D2D Backup System
- Troubleshooting the HP StoreOnce D2D Backup System

Intended audience

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

Related documentation

In addition to this guide, the following document provides related information:

'Start here' poster for an overview of the installation information in this guide (available in English, French, German and Japanese)

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 33)	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
`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

Customer self repair

HP customer self repair (CSR) programs allow you to repair your StoreOnce product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

http://www.hp.com/go/selfrepair

Registering your HP D2D Backup System

Once you have installed and tested your HP D2D Backup System please take a few minutes to register your product. You can register via the web (http://www.register.hp.com).

To ensure your registration is complete, there are a number of questions on the electronic form that are mandatory. Other questions are optional. However, the more you feel able to complete, the better HP can meet your needs.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, software updates, and other product resources.

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.

Glossary

C

Catalog This is an internal SQL database which contains information about the backups and the NBU configuration. NetBackup requires catalog information for client restores. It is vital that the catalog is regularly backed up. By default the catalog is stored on the master server.

Client A server or workstation running NBU client software which enables it to backup and recover it's own datasets via the media server.

M

Master server The primary server in an NetBackup(NBU) environment which controls and tracks backups, manages tape media. Maintains the NBU catalog. Can also act as a media server if required.

Media server This servers manages the movement of data between clients and the storage device (tape or disk based).

Policy Details what data should be backed up, to which storage unit (or media manager in the case of tape) and when the backup should run. Often referred to as a backup job in other data protection software products.

Storage unit A device which acts as a repository for backups. This can be a tape device or directly attached disk. In certain circumstances can be a pool of disks. The storage unit really provides the logical link between a media server and the backup device.

Index

T

W