

# HP D2D NAS

# Integration with Symantec™ Backup Exec™ 2010

## Abstract

This guide provides step by step instructions on how to configure and optimize Symantec Backup Exec 2010 in order to back up to HP D2D Backup Systems using a CIFS backup target.



© Copyright 2011 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

WARRANTY STATEMENT: To obtain a copy of the warranty for this product, see the warranty information website:

<http://www.hp.com/go/storagewarranty>

Linear Tape-Open, LTO, LTO Logo, Ultrium and Ultrium Logo are trademarks of Quantum Corp, HP and IBM in the US, other countries or both.

Microsoft, Windows, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation.

Symantec and Backup Exec™ are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

---

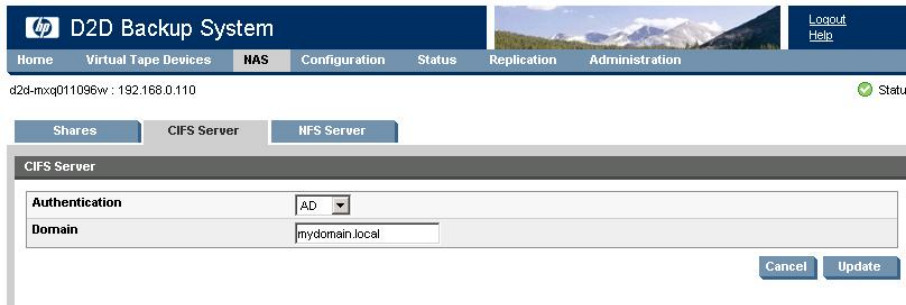
# Contents

1	Configure the D2D CIFS server.....	4
	More about authentication modes.....	4
	Configuring User Authentication mode.....	5
	Configuring AD Authentication Mode.....	6
	To join a domain.....	6
	To create shares and grant access permission.....	8
2	Configure Backup Exec to use D2D CIFS Share.....	12
	Create a D2D CIFS target for backup.....	12
	Create a Backup Exec Backup-to-disk folder.....	13
3	Configure a backup rotation scheme.....	18
	To create a media set.....	18
	To create backup policy.....	20
	Housekeeping considerations.....	24
	About this guide.....	25
	Intended audience.....	25
	Related documentation.....	25
	Document conventions and symbols.....	25
	HP technical support.....	26
	HP websites.....	26
	Documentation feedback.....	26
	Index.....	28

# 1 Configure the D2D CIFS server

The first step in configuring the D2D device as a target for backups from Symantec Backup Exec 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. Backup Exec will always be able to use shares configured in this mode with no changes to either server or Backup Exec 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 Backup Exec media server and configuration changes to the Backup Exec services. Individual users can then be assigned access to individual shares on the D2D Backup System. This authentication mode is **ONLY** recommended when the Backup Exec media server is not a member of an AD Domain.

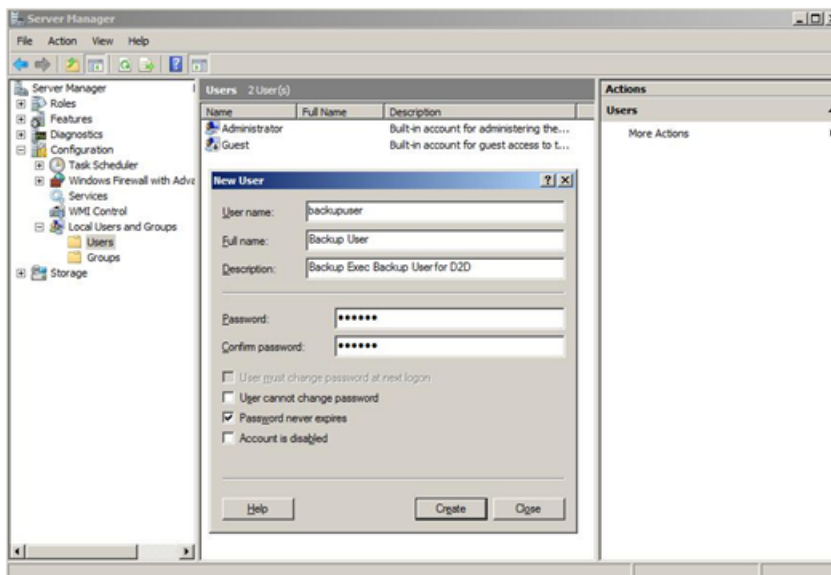
**AD:** In this mode the D2D CIFS server becomes a member of an Active Directory Domain. In order to join an AD domain the user needs to provide credentials of a user who has permission to add computers and users to the AD domain. After joining an AD Domain access to each share is controlled by Domain 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 Backup Exec Media server is a member of an AD domain.

## Configuring User Authentication mode

1. Select the **User** authentication mode on the D2D Web Management Interface and click **Update** to create a local user account on the D2D Backup System. Provide a User Name and Password for the new user.

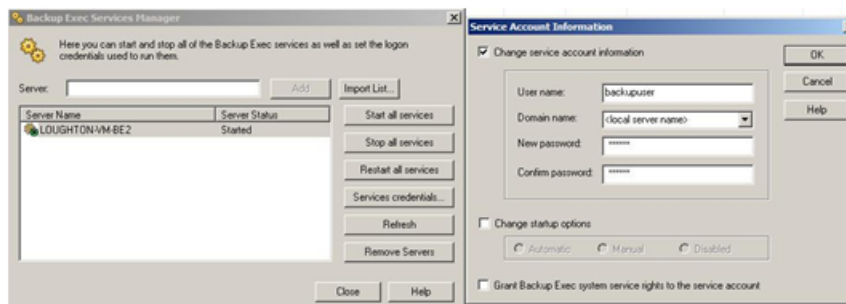


2. Use Server Manager to create a correspondingly named user on the Windows server that hosts the Backup Exec Media server.



3. It is then necessary to configure Backup Exec to use this Local user account as the credentials used to run its services. Do this from the Backup Exec interface by selecting **Tools — Backup Exec Services ....**

Then click the **Services Credentials** button and provide the new User Name, Domain name (local server name) and password.



- Restart the Backup Exec services before continuing with configuration. Note, however, that this is the **ONLY** user account that the Backup Exec Media server will be able to use to connect to remote storage that requires authentication, so this account must be the same for any other disk storage devices.

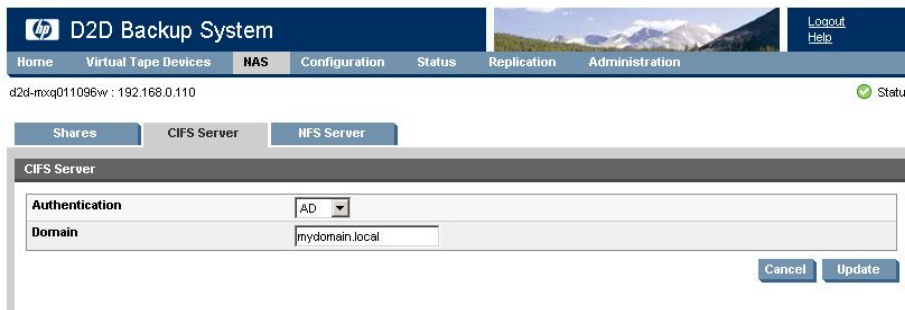
## Configuring AD Authentication Mode

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 Backup Exec services to use the correct Domain account.

### To join a domain

- 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”



The screenshot shows the D2D Backup System web interface. The top navigation bar includes 'Home', 'Virtual Tape Devices', 'NAS', 'Configuration', 'Status', 'Replication', and 'Administration'. Below the navigation bar, there are tabs for 'Shares', 'CIFS Server', and 'NFS Server'. The 'CIFS Server' tab is active, and the 'Authentication' dropdown menu is set to 'AD'. The 'Domain' field is filled with 'mydomain.local'. There are 'Cancel' and 'Update' buttons at the bottom right of the form.

- 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**.



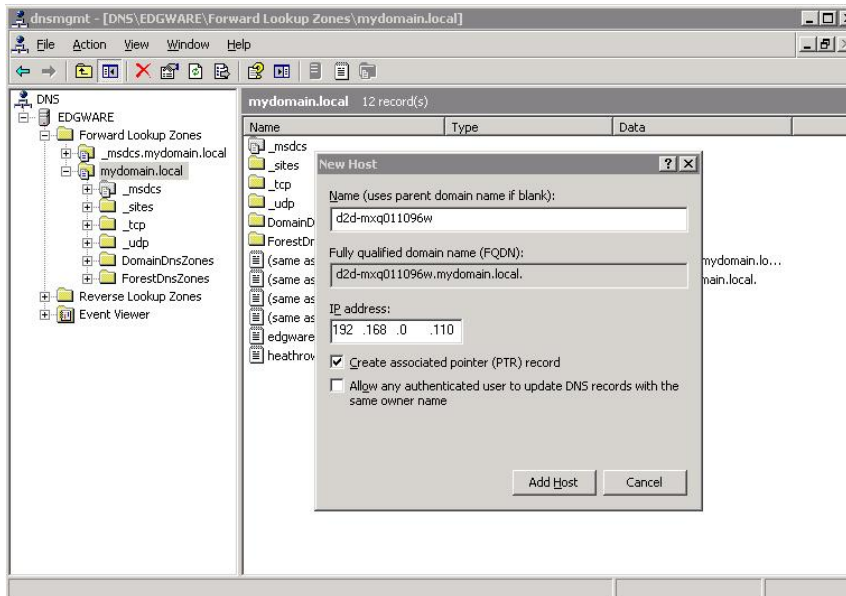
The screenshot shows a pop-up box titled 'Active Directory Registration'. It contains the following text: 'To register with active directory domain, enter domain administrator name and password'. Below this text are two input fields: 'Domain Administrator' and 'Password'. At the bottom of the box are two buttons: 'Cancel' and '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.

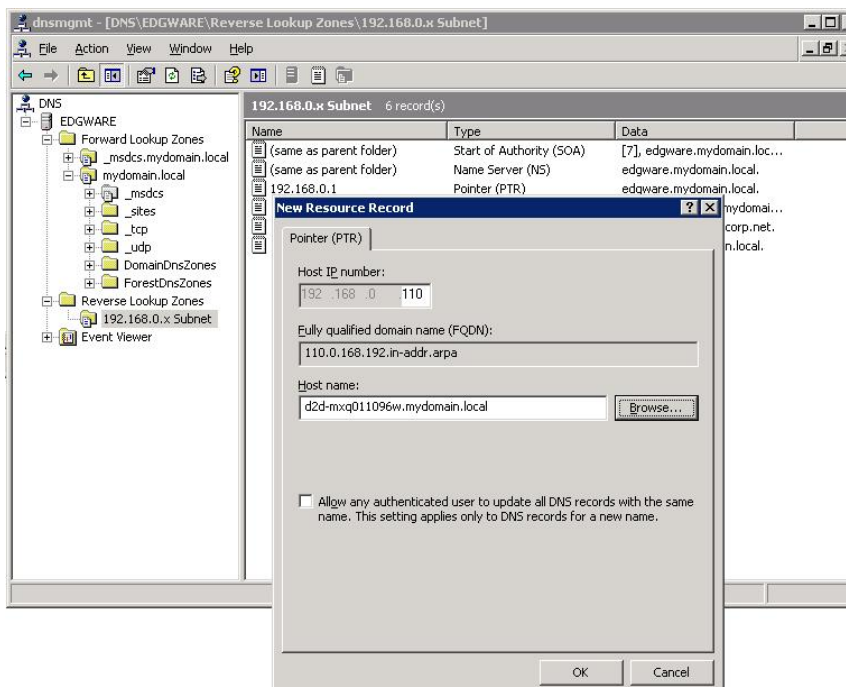
### To configure entries manually if the DNS server does not update automatically

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.

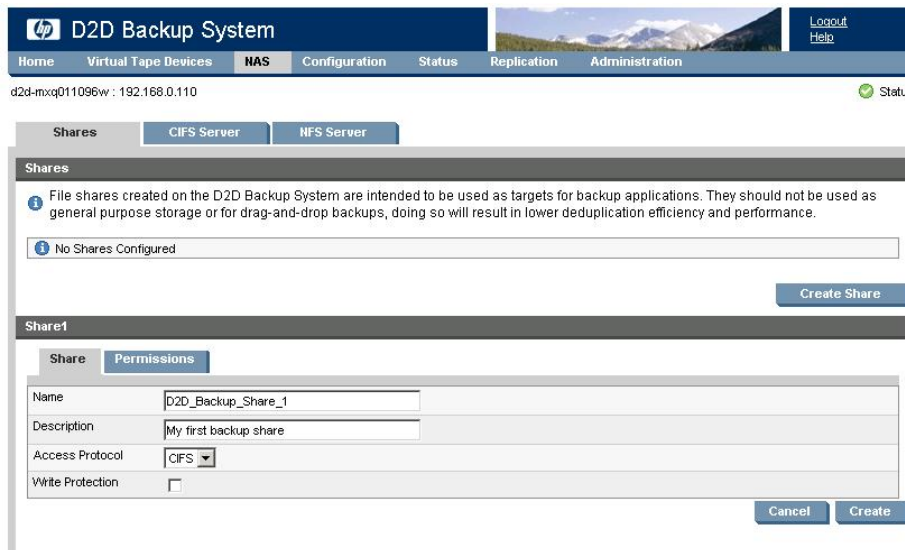


## To create shares and grant access permission

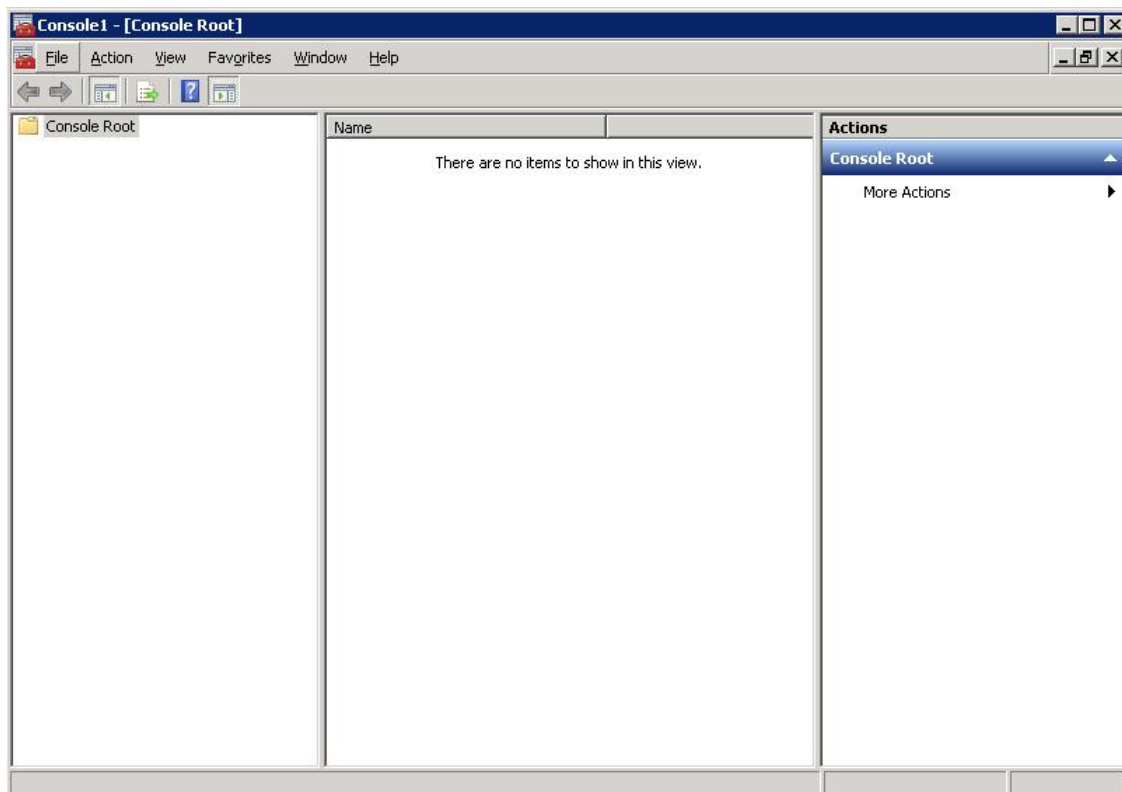
Now that the D2D Backup System is part of a domain and can be managed, it is possible to create shares and grant access permission to them for domain account users or groups.

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**.

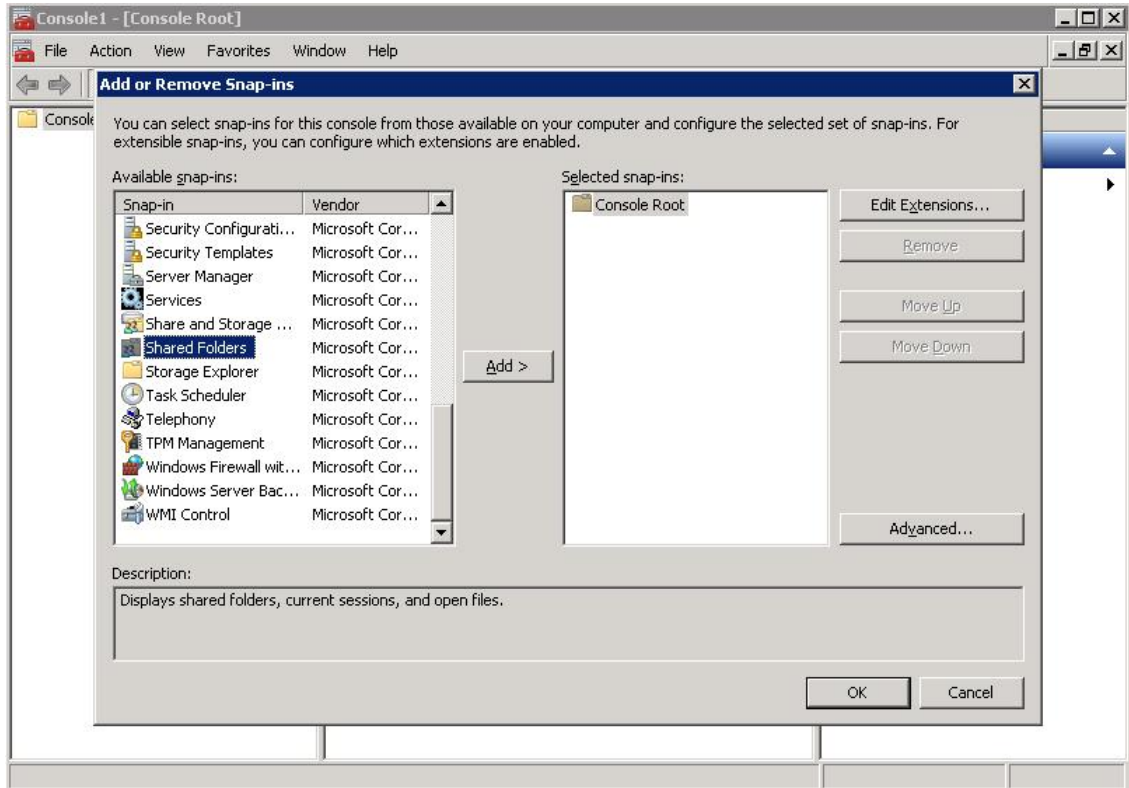


2. Now that the D2D Backup System is a member of the domain its shares can be managed from any computer on the domain by configuring a customized Microsoft Management Console (MMC) with the Shared Folders snap-in. To do this first open a new MMC window by typing `mmc` at the command prompt or from the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

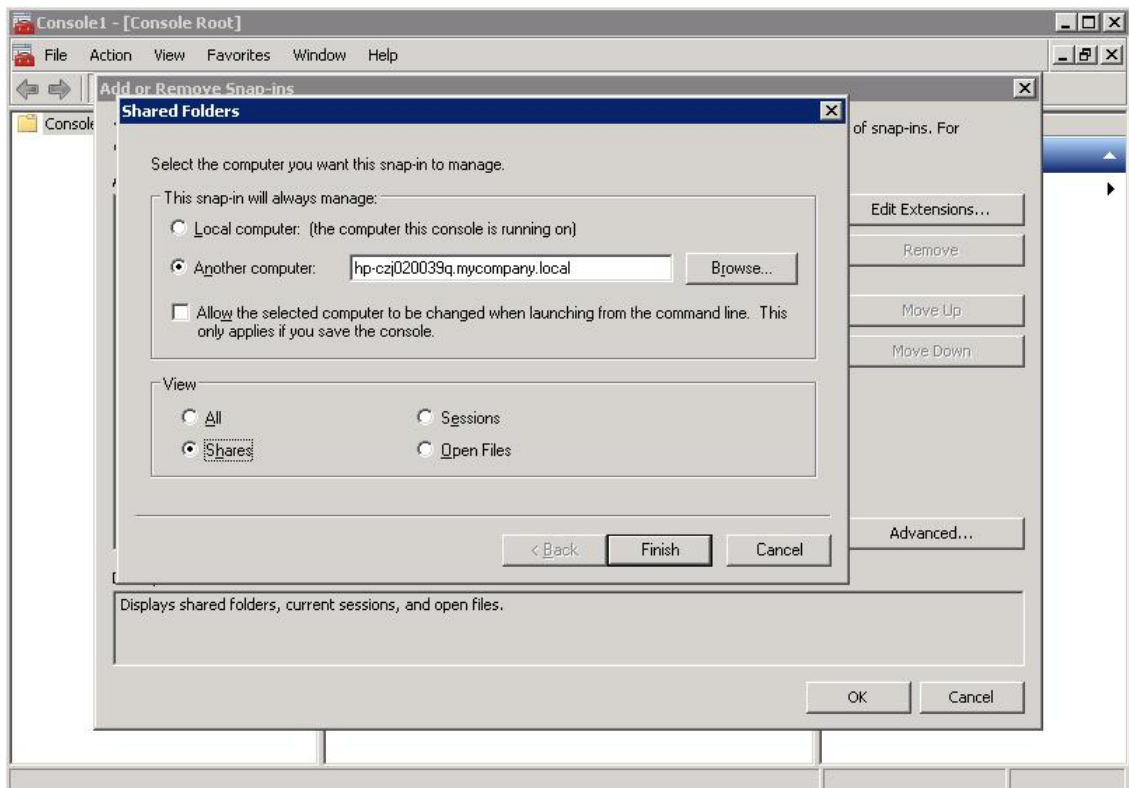




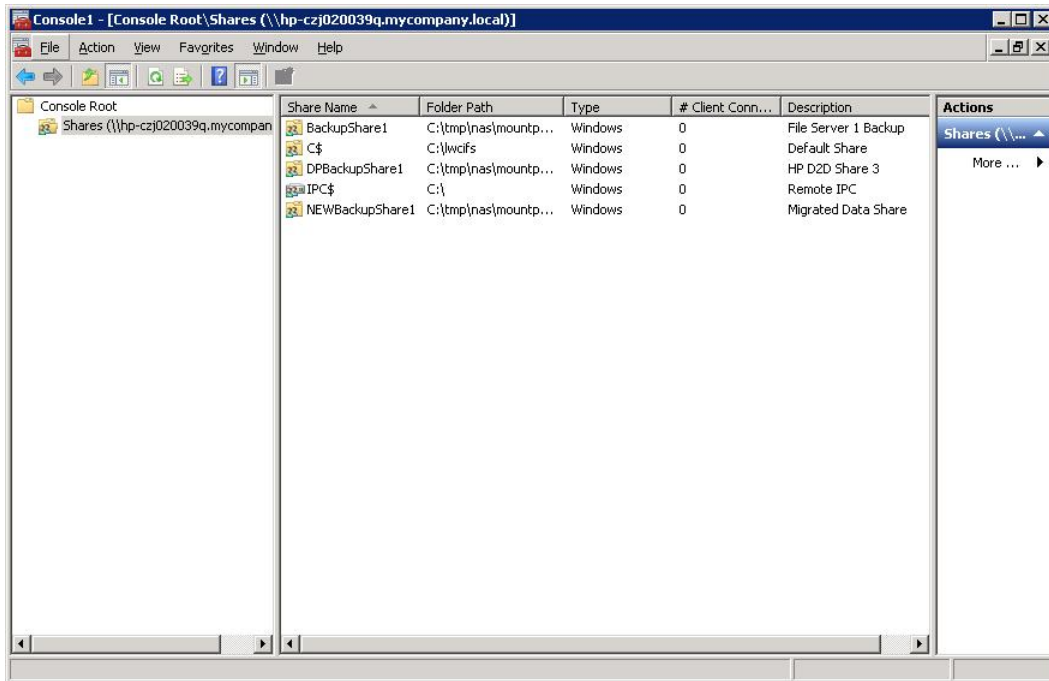
- To this empty MMC window add the Shared Folders snap-in. Select **File — Add/Remove Snap-in ...**, then select **Shared Folders** from the left-hand pane.



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

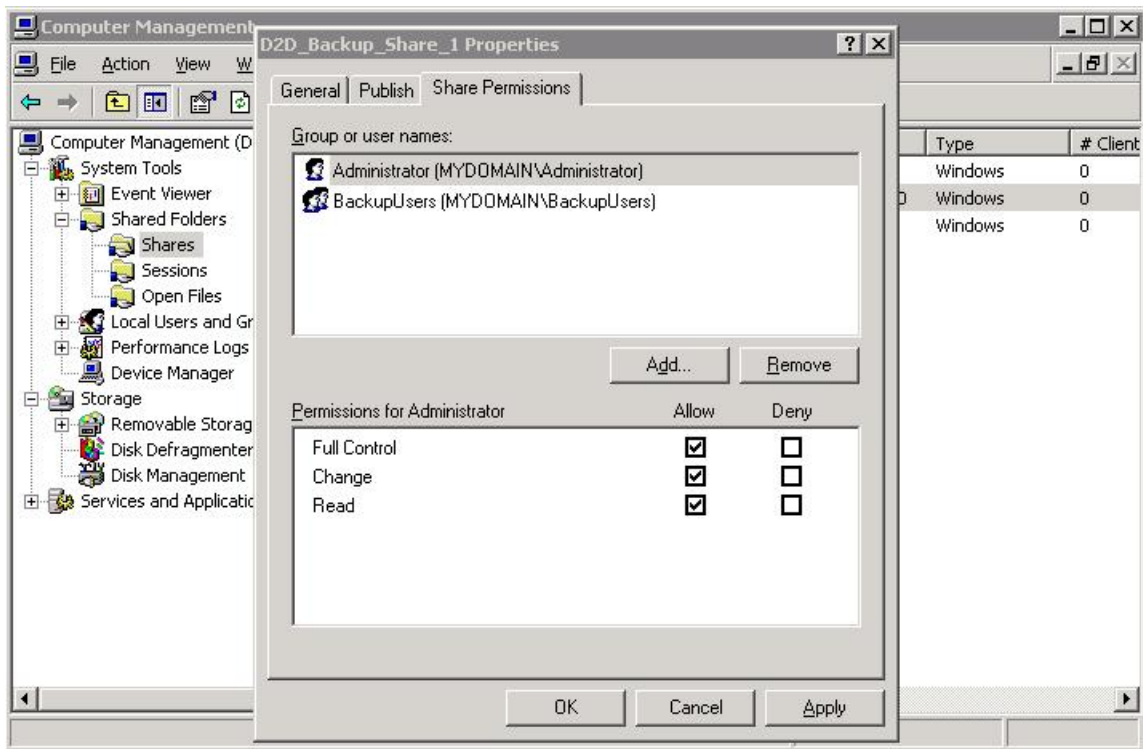


- Click **Finish** and **OK** to complete the snap-in set up.



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.

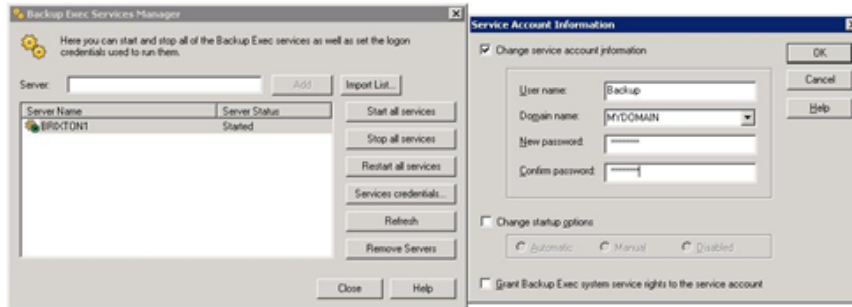
---

**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.

---

9. It may also be necessary to configure Backup Exec to use this AD Domain user account as the credentials used to run its services. Do this from the Backup Exec interface by selecting **Tools — Backup Exec Services ....**

Select the **Services Credentials** button and provide the new User Name, Domain name and password.



10. Restart the Backup Exec services before continuing with configuration. Note, however, that this is the **ONLY** user account that the Backup Exec Media server will be able to use to connect to remote storage that requires authentication, so this account must be the same for any other disk storage devices.

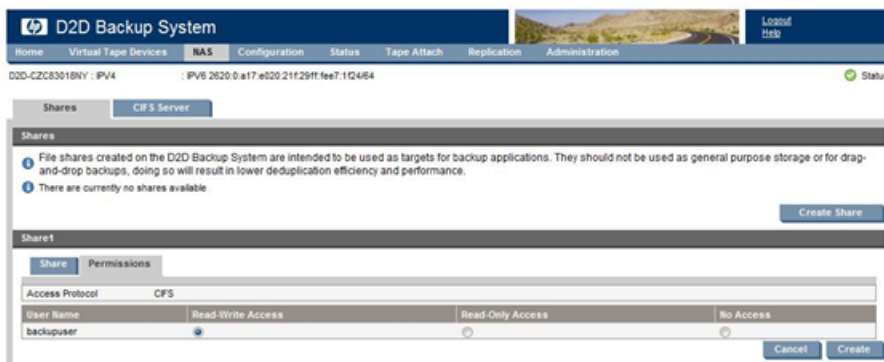
## 2 Configure Backup Exec to use D2D CIFS Share

### Create a D2D CIFS target for backup

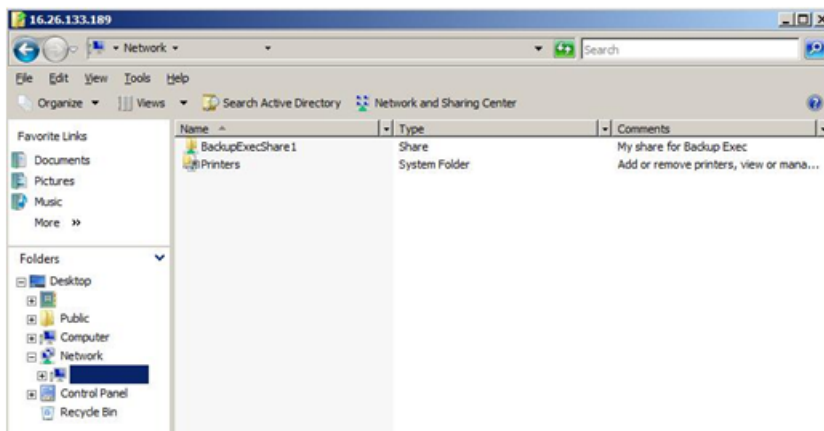
If a new D2D CIFS share has not already been created as part of the authentication configuration process in the previous section, it is now necessary to create a new CIFS NAS share.

The available options for share creation are:

- **Name** – This is the name of the CIFS share to be created
  - **Description** – A “friendly” description of the share and its use, this will be presented to the Windows host for easy identification.
  - **Access Protocol** – CIFS is the only option provided
  - **Network Path** – This is a non-configurable field which shows the share name appended to the IP address upon creation of the share
  - **Write Protection** – Global write protect for the share, to be used if no further writing is to be permitted to the share.
1. Click **Create**, the share is configured and starts after a few seconds.



2. After the share has started it will report as “Online”. If required, configure **User** or **AD** authentication mode, as already described, so that the share is accessible to the appropriate users. After that it is possible to access the share from the Windows server, for example by clicking the **Network Path** link from the Shares page which will open a Windows Explorer window.



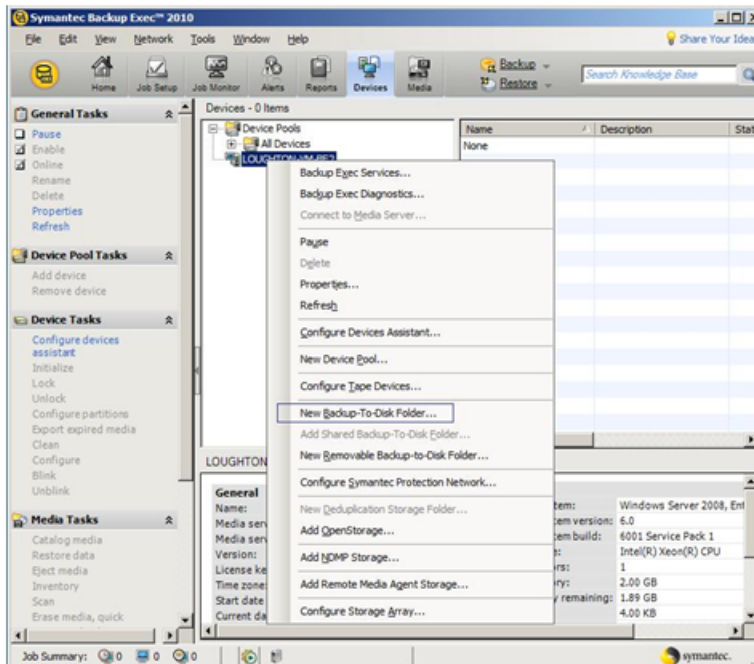
## Create a Backup Exec Backup-to-disk folder

Backup Exec refers to NAS backup targets as “Backup-To-Disk” folders, which may be one of three types of folder:

- Backup-To-Disk folder – This is used for CIFS shares or local disk devices
- Removable Backup-To-Disk folder – Used for removable media devices, such as HP RDX
- Shared Backup-To-Disk folder – Used with the CASO or SAN Shared Storage options to share a NAS backup target across multiple Backup Exec Media servers.

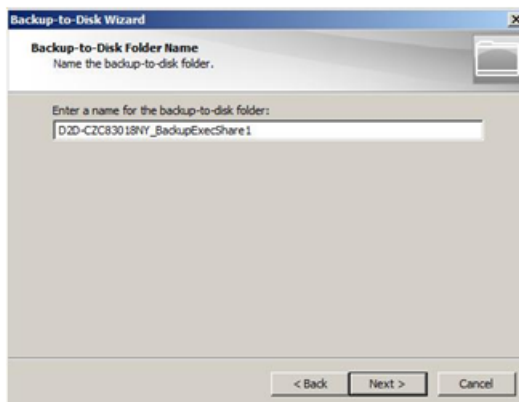
When using an HP D2D CIFS share the “Backup-To-Disk” folder type should be used.

1. From the Backup Exec, Devices page select the Media server and right click, then select **New Backup-To-Disk Folder...**

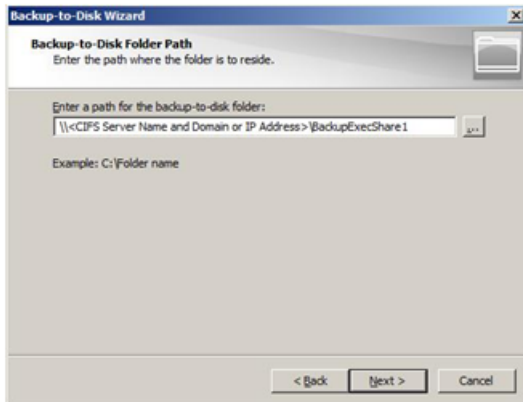


2. This will launch a Backup-To-Disk Wizard to step through the creation and configuration of a Backup-To-Disk folder.

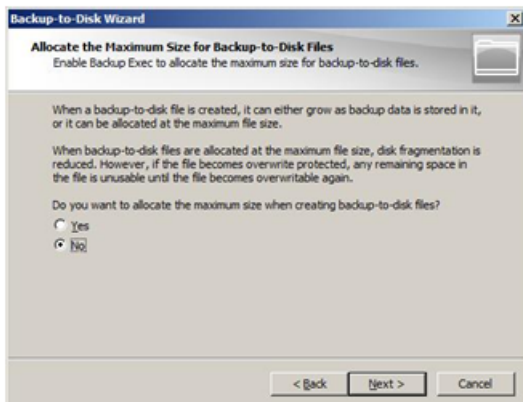
Enter a name for this folder that Backup Exec will use to identify it. A best practice is to use the name of the D2D Backup System and share name in order to easily identify where this backup-to-disk folder resides.



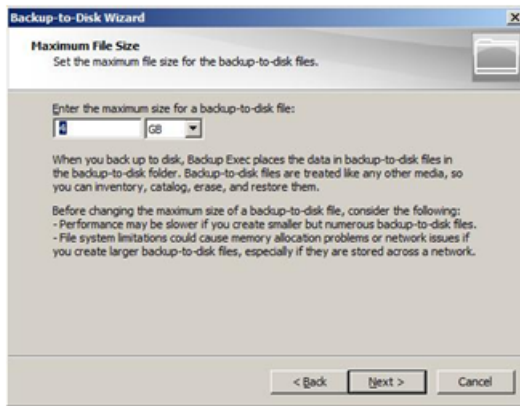
- The next step is to provide the path to the backup-to-disk folder, this is the path to the CIFS share on the D2D Backup System. There is no need to mount the D2D CIFS share as a Windows drive letter because the full path including domain extension or IP address with share name will allow direct access to the D2D share.



- If more than one Backup-To-Disk folder is required per D2D CIFS share, it is necessary to create multiple folders within the D2D NAS share because each Backup-to-disk folder must be in a different folder on disk.  
Use Windows Explorer to create a new folder on the D2D CIFS share.
- The next step in the wizard provides the user with the option to pre-allocate the maximum size of each Backup-To-Disk file as it is created, this option **MUST** be set to "No".  
Pre-allocating disk space for each backup to disk file will result in incorrectly reported deduplication ratio, and also poor performance or failures because the D2D Backup System will need to "pad" the data file when created.

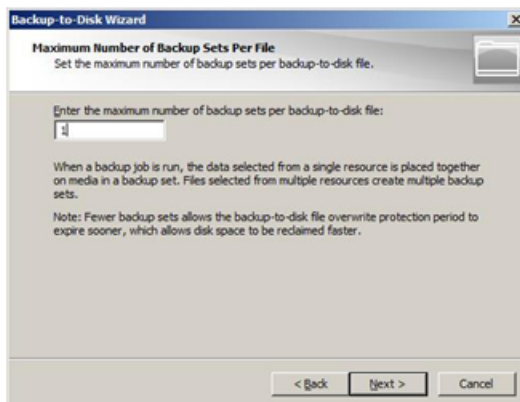


- Configure the maximum size that each Backup-To-Disk file may reach before spanning to a new file.  
The default size is 4GB; however this should be set to a larger size in order to improve performance. It is suggested that this maximum file size is set to at least the size of the full backup with enough headroom for future data growth. (If in doubt about the amount of growth expected, setting this to the maximum value of 4TB (4096GB) will have no detrimental effect.) This means a single file can hold the entire backup and prevents the housekeeping process, which starts whenever a file is closed, from interfering with the remainder of the backup job.



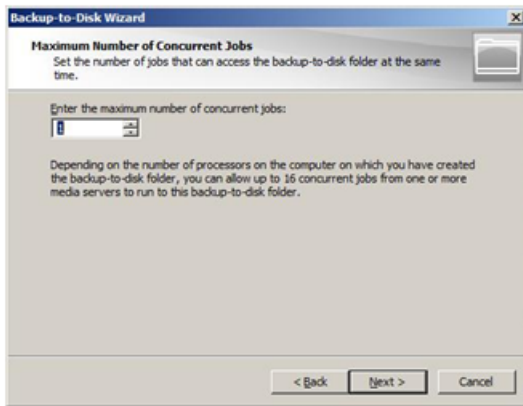
An exception to this rule is when D2D replication is being used when it may be beneficial to use a smaller file size in order to start replicating backup files before the whole backup completes. However this may reduce backup performance, if the D2D Backup System is heavily loaded with other backups or housekeeping processes.

7. Configure the **Maximum number of backup sets** that can be held in each backup to disk file. This setting should be set to 1; this prevents backups from appending to backup-to-disk files. No space is lost in this configuration because no space is allocated per file. Appending of backups to Backup-to-disk files is undesirable because it prevents that file being overwritten until all sets have expired. It also causes additional D2D replication overhead because replicating an appended file requires the replication target file to be “cloned” before new data can be added to it, which reduces performance.



An exception is if a large Backup-to-disk file size is configured but backups are quite small. These backups could be appended to the Backup-to-disk file (if appending is enabled in the backup job) and, in this case, the maximum number of backups per file can be configured

8. Configure the **Maximum Number of Concurrent jobs**. This is an important selection for D2D due to the limitation on the number of concurrently open files that are permitted. The default setting for this variable is 1, which means that only one backup job is permitted to that Backup-To-Disk file at any one time.



When Backup Exec is backing up flat file data (rather than database or any other media agent) it will have four files open concurrently during the backup. One is the backup data file (B2DXXXXXX.bkf) which is deduplicated; the other three files are smaller than the 24KB pre-deduplication limit and consist of a file lock (B2DXXXXXX.lck), a changer configuration file (Changer.cfg) and a Backup-To-Disk folder configuration file (Folder.cfg).

However, it is possible that a second backup file may be temporarily open on the D2D Backup System during transitional periods when the backup spans to a new \*.bkf file. This is because the Windows operating system will report that the previous file is closed before the D2D Backup System actually closes the file.

It is recommended that no more than four backup jobs run concurrently to a D2D share - the maximum number of concurrent jobs setting is used to prevent more than four concurrently open files. Depending on the number of Backup-To-Disk folders configured within a single NAS share this value should be set in the range between 1 and 4.

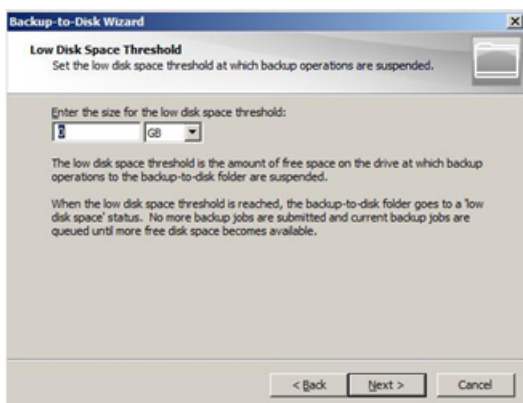
When Backup Exec is using media agents to back up other types of data, e.g. Exchange or Oracle Database, it is possible that a much larger number of small (pre-deduplication) files are held open concurrently. Thus it is recommended that only a single job runs to a D2D NAS share when backing up these data types.

See the *D2D Best Practices for VTL, NAS and Replication implementations* for more information on the maximum number of concurrently open deduplicated and pre-deduplicated files per D2D Share and per D2D Backup System appliance for different D2D Backup System models.

9. Configure the **Low Disk Space Threshold** setting.

This is a number of GB of remaining disk space at which point backups to the Backup-To-Disk folder are suspended. The default for this setting is 0GB, i.e. there is no low space threshold set, and it is the recommended setting.

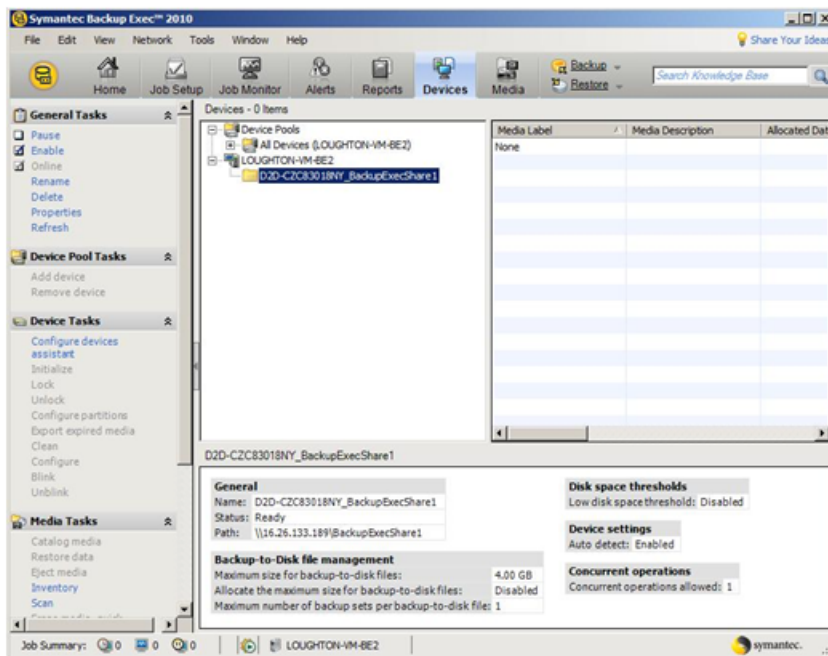
With deduplication a physical disk space remaining figure is meaningless, because a backup may use a fraction of the physical disk space compared to the amount of data backed up.





10. Finally Backup Exec will present a summary of the Backup-To-Disk folder configuration before creating the folder.

Once complete the Backup-To-Disk device will be created and presented on the **Devices** page in Backup Exec. At creation time two small configuration files will be created on the D2D CIFS share (Changer.cfg and Folder.cfg).



## 3 Configure a backup rotation scheme

When backing up to CIFS shares on the D2D Backup System it is recommended that a similar retention and rotation scheme to that of virtual tape is used. There is some simplification over virtual tape in that no account needs to be taken of the number of cartridges within the virtual library, only the total number of files that can be supported on a D2D CIFS share (25000), which should be more than adequate.

It is, however, important to ensure that the amount of data in the share does not grow in an uncontrolled fashion due to keeping all backups forever. The default media set in Backup Exec is the **Keep Data Indefinitely** set, this should not be used for CIFS backups.

The following is an example of a “Best Practice” backup rotation and retention scheme configuration with Backup Exec. This scheme observes the following best practices:

- Backup-To-Disk files are never appended to; appended backups reduce replication performance, prevent files from being overwritten until all sessions have expired and have no disk space benefit for NAS targets.
- Different media pools are used to set retention periods for different types of backup (Daily, Weekly, Monthly).
- Only one type of data is backed up in this Backup-To-Disk folder, in this case it is flat file data, other types would be Exchange, SQL, Oracle etc.
- This backup will create only one concurrent backup stream; up to three other flat file backups (of other client servers perhaps) could use the same Backup-To-Disk folder concurrently.
- Most backups will not include a Verify pass because this impacts overall performance.
- Software compression is disabled because this will slow the backup job and result in a worse deduplication ratio.

The rotation and retention scheme for this backup rotation scheme employs GFS as follows:

1. Daily (Monday – Friday) Incremental backups, overwritten every week.
2. Weekly (Saturday) Full backups, overwritten every 4 weeks.
3. Monthly (1st Day Month) Full backups, overwritten every 12 months.
4. Yearly (Jan 1st) Full backups, never overwritten.

Monthly full backups will replace the last weekly full backup.

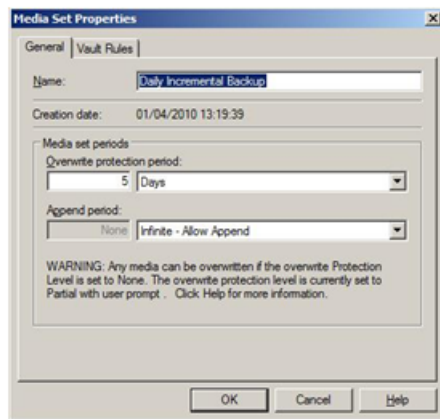
### To create a media set

The first step in creating this scheme is to create new Backup Exec Media sets that employ the correct protection. Once this protection period expires media (in this case Backup-To-Disk Files) will be overwritten by the next backup job that uses the media set.

In this example we need four new media sets as follows:

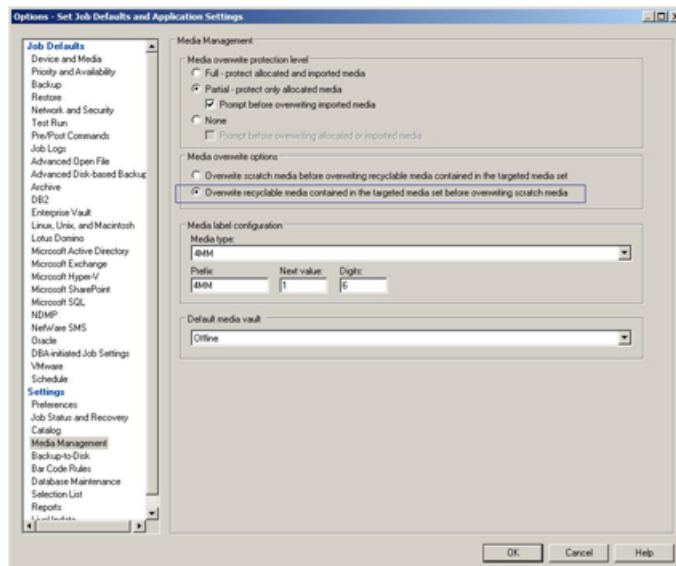
Media Set Name	Overwrite Protection Period	Append Period
Daily Incremental Backup	5 Days	Infinite (though not used)
Weekly Full Backup	4 Weeks	Infinite (though not used)
Monthly Full Backup	1 Year	Infinite (though not used)
Yearly Full Backup	Infinite – Do not overwrite	Infinite (though not used)

1. To create these media sets, go to the **Media** page of the Backup Exec interface and select **New Media Set** from the **Tasks** panel. An example of a media set configuration for the Daily Incremental Backup is shown.



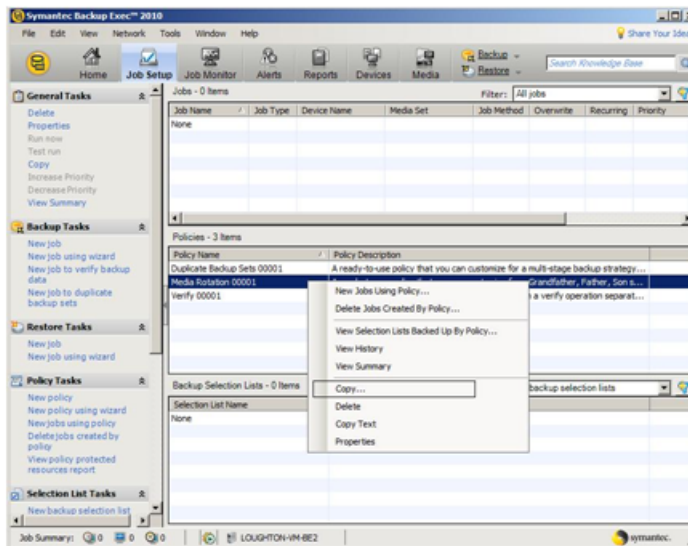
2. It is also useful to change the Media overwrite options.

From the **Tools — Options** menu select **Media Management** and change the Media overwrite option to **Overwrite recyclable media contained in the targeted media set before overwriting scratch media**. This will ensure that the retention period of the media is not exceeded by creating new Backup-To-Disk files rather than overwriting expired ones.

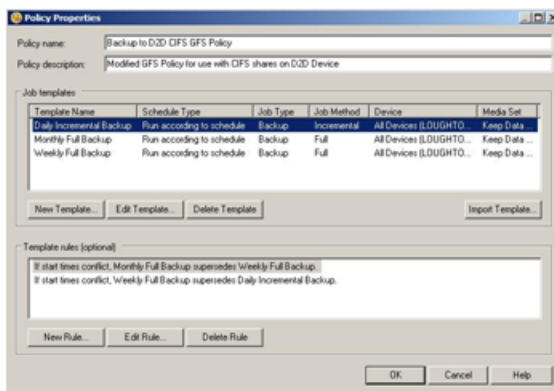


## To create backup policy

1. Once media sets have been created, a new backup policy can be created from the **Job Setup** page on the Backup Exec User interface. There is a default backup policy that is similar to the required scheme in this example, so copying this provides a start point for modification.



2. Once copied the new template can be renamed and edited to match the rotation scheme in the example, the policy already consists of three individual job templates for Daily, Weekly and Monthly backups.



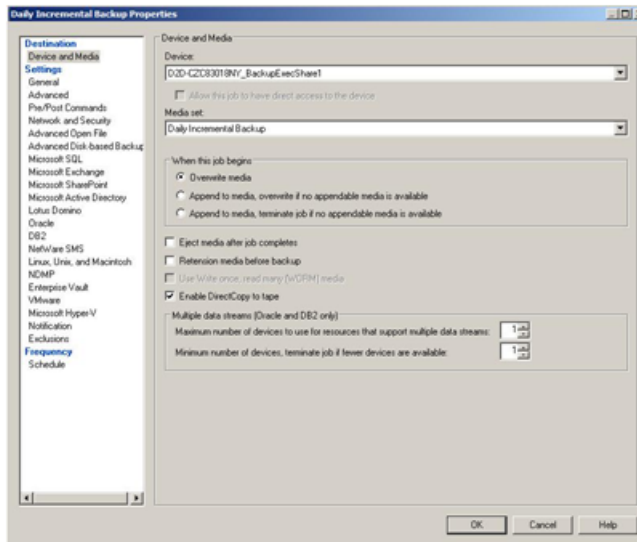
Note that the individual Job templates for Daily, Weekly and Monthly backups need to be modified.

### Device and Media

Firstly adjust the Device and Media options to:

- Select the new Backup-To-Disk folder
- Change the media set to the newly created sets
- Set the job to always overwrite

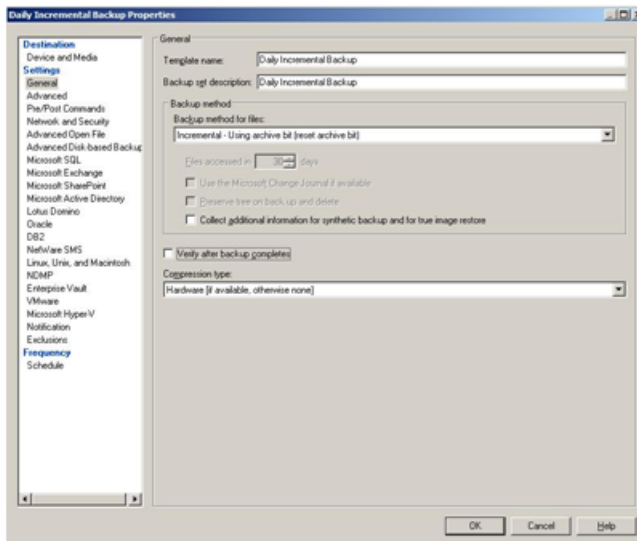
The daily incremental backup template changes are shown here



## General settings

Then change the General settings to:

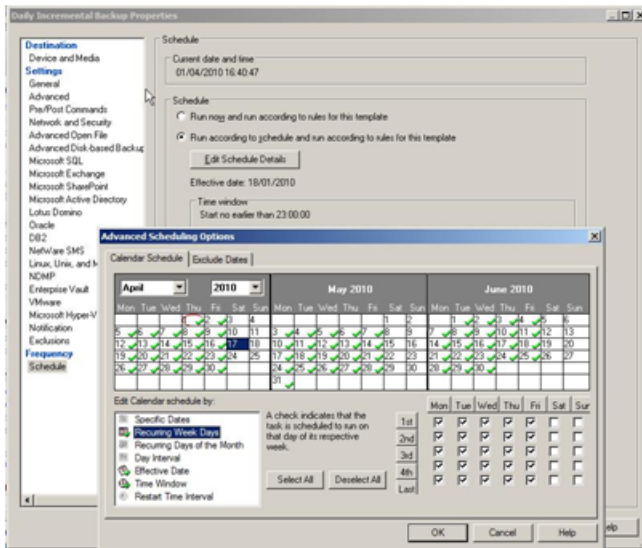
- Rename and re-describe the template
- Select the backup method (Incremental, full, etc)
- Disable verify
- Set compression to either **Hardware if available** or **None**. (The D2D Backup System will always deduplicate and compress the data; enabling software compression will slow the backup job and result in a worse deduplication ratio so should NOT be selected.)



3. Lastly modify the schedule to meet the requirements of the template type.

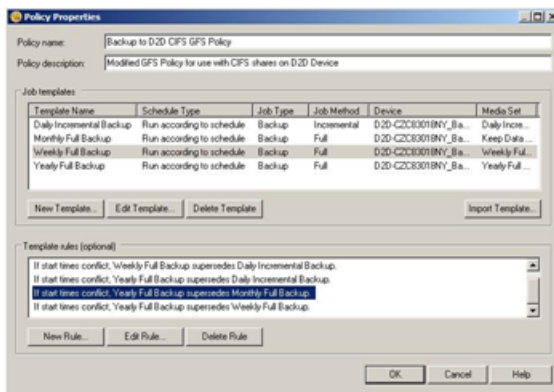
For example, for the daily incremental backups disable the **“Day Interval”** setting and enable the **Recurring Week Days** setting, then select the days of the week to run the job.

Also set the **Time** interval to meet the backup window requirements.



- Once the three existing templates have been modified, a new Yearly template needs to be created using the same principles.

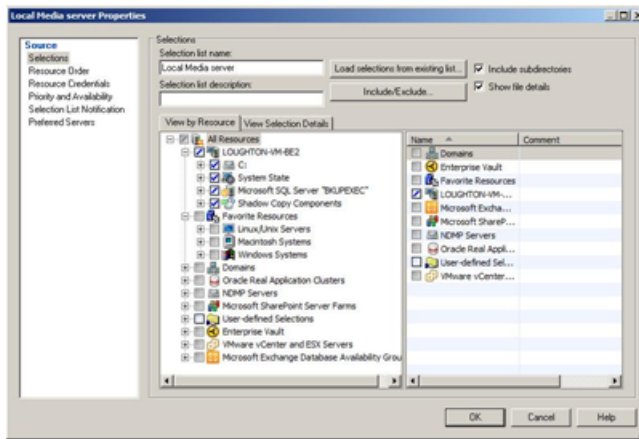
The default template rules ensure that Weekly backups supersede Daily Backups and Monthly backups supersede Weekly backups, if start times conflict, and can remain. Three further rules can be created to ensure that Yearly backups supersede the other three backup types.



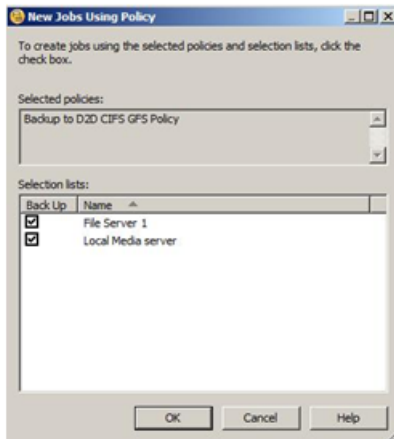
- The last configuration step before actually creating the backup jobs is to create a Backup **Selection** list; this is the list of resources to be backed up.

In this example the Selection list is just going to contain the local media server backup.

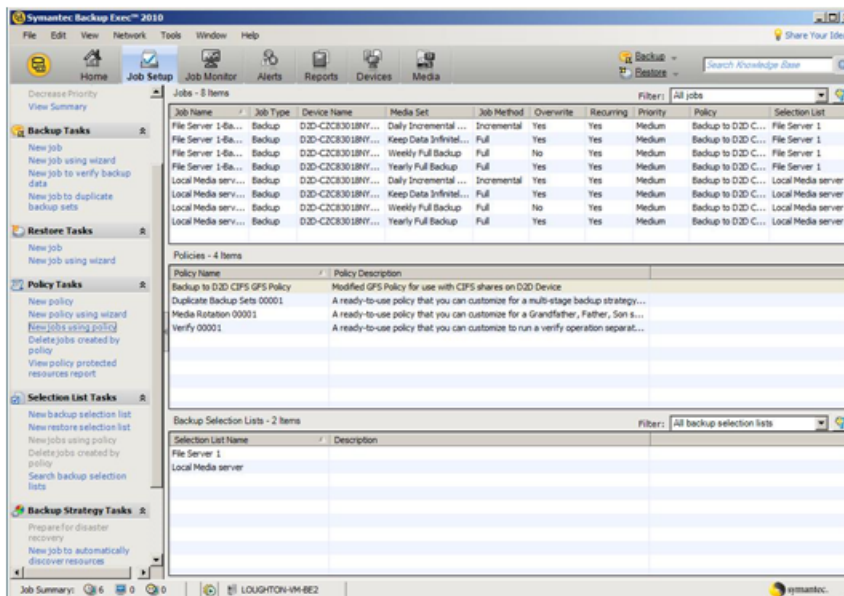
If multiple servers are configured for backup, they will be queued to run sequentially in the backup job. In order to ensure that multiple backup streams run concurrently to the Backup-To-Disk folder (assuming the concurrency value for the folder is greater than 1) more backup selection lists can be created



- The last step in the process is to create backup jobs based on the Policy and Selection Lists. Select the **New Jobs Using this policy** option from the tasks panel, then select the **Selection lists** for which jobs will be generated.



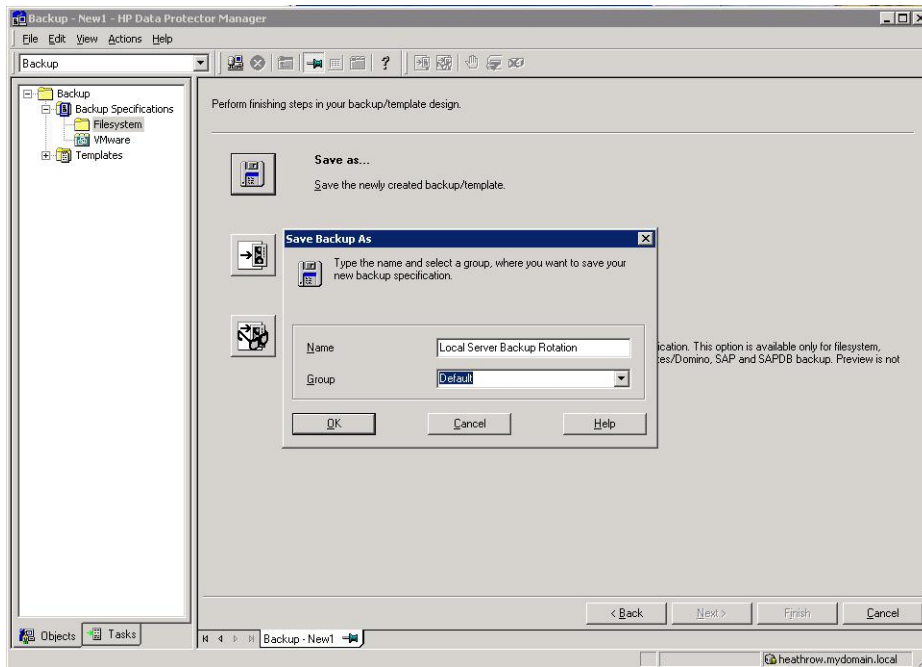
- The jobs will be created and will run according to the schedule and rotation scheme defined.



## Housekeeping considerations

For the initial backups new Backup-To-Disk files will be created for every new backup, however, as soon as sessions reach their protection expiration, Backup Exec will overwrite each file in turn as a new job starts.

Because the backups are configured to use one Backup-To-Disk file per backup the housekeeping process will not start until the new backup has completed and thus will not interfere with the backup. However, if multiple jobs are running concurrently but do not finish at the same time there will be some housekeeping interaction with the other backups. In order to avoid this, some tuning of the backup start times can be made in order to better align the backup finish times. This, however, means that a new policy with different templates is needed for each backup job.



The backups will now run according to the new schedule, for initial backups new backup files will be created. When backup protection expires, e.g. after 1 week of incremental backups, the previous backup files will be overwritten. Overwriting of the backup files will result in Housekeeping work being generated; this will run in parallel with the backup process and could cause a slight reduction in performance. During the backup, Backup Exec creates two files, one is the backup data file depot which grows throughout the backup, the other is a temporary file of 15MB which is removed when the backup completes.



# About this guide

This guide provides information about:

- Provides step by step instructions on configuring a D2D NAS CIFS device on Symantec Backup Exec 2010
- Describes the Symantec Backup Exec 2010 backup folder 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 Symantec Backup Exec 2010

## Intended audience

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

This guide assumes a basic working knowledge of Symantec Backup Exec 2010 and that it has been installed correctly by loading the appropriate Media Agents and licences.

## Related documentation

In addition to this guide, the following document provides 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 1 Document conventions**

Convention	Element
Blue text: <a href="#">Table 1 (page 25)</a>	Cross-reference links and e-mail addresses
Blue, underlined text: <a href="http://www.hp.com">http://www.hp.com</a>	website addresses
<b>Bold</b> text	<ul style="list-style-type: none"><li>• Keys that are pressed</li><li>• Text typed into a GUI element, such as a box</li><li>• GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes</li></ul>
<i>Italic</i> text	Text emphasis

**Table 1 Document conventions** *(continued)*

Convention	Element
Monospace text	<ul style="list-style-type: none"><li>• File and directory names</li><li>• System output</li><li>• Code</li><li>• Commands, their arguments, and argument values</li></ul>
<i>Monospace, italic</i> text	<ul style="list-style-type: none"><li>• Code variables</li><li>• Command variables</li></ul>
<b>Monospace, bold</b> 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/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](mailto:storagedocs.feedback@hp.com). All submissions become the property of HP.

---

# Index

## A

- access permissions, 8
- AD authentication, 4
  - configuring, 6
- audience, 25
- authentication modes, 4

## B

- backup policy, 20
- backup rotation scheme
  - best practices, 18
- backup-to-disk folder, 13
- best practice, 13, 18

## C

- check
  - share accessible, 12
- CIFS server, 4
- CIFS target, 12
- configure
  - AD authentication, 6
  - backup policy, 20
  - backup rotation scheme, 18
  - CIFS server, 4
  - media set, 18
  - user authentication, 5
- conventions
  - document, 25
  - text symbols, 26
- create
  - backup-to-disk folder, 13
  - CIFS target, 12
- create shares, 8

## D

- document
  - conventions, 25
  - related documentation, 25
- documentation
  - HP website, 25
  - providing feedback, 26
- domain, 6

## H

- help
  - obtaining, 26
- host(A) record, 7
- housekeeping, 24
- HP
  - technical support, 26

## J

- join domain, 6

## M

- media set, 18

## P

- Pointer(PTR) record, 7

## R

- related documentation, 25

## S

- services, 6, 11
- share
  - check accessible, 12
- symbols in text, 26

## T

- technical support
  - HP, 26
  - service locator website, 26
- text symbols, 26

## U

- user authentication, 4
  - configuring, 5

## W

- websites
  - HP, 26
  - product manuals, 25