HP D2D NAS Integration with HP Data Protector 6.11

Abstract

This guide provides step by step instructions on how to configure and optimize HP Data Protector 6.11 in order to back up to HP D2D Backup Systems using a CIFS backup target.



HP Part Number: EH985-90933 Published: February 2011 Edition: 1 © 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.

Contents

1 Configure the D2D CIFS server. Introduction. More about authentication modes. Configuring User authentication mode. Configuring AD Authentication Mode. To join a domain. To create shares and grant access permission.	
2 Configure Data Protector to use D2D CIFS Share Creating a new Data Protector File Library Configure drives	14
3 Configure a backup rotation scheme. To create a media pool. To create a backup job.	
About this guide. Intended audience Related documentation Document conventions and symbols HP technical support HP websites Documentation feedback.	
Index	

1 Configure the D2D CIFS server

Introduction

The first step in configuring the D2D device as a target for backups from HP Data Protector 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 click Edit.

Ø	D2D Backup Sys	stem			NUMBER OF		<u>Loqout</u> <u>Help</u>
Home	Virtual Tape Devices	NAS	Configuration	Status	Replication	Administration	
d2d-m×q0	11096w : 192.168.0.110						🚫 Statu
SI	hares CIFS Serve	er	NFS Server				
CIFS S	erver						
Auth	entication		AD 💌				
Doma	ain		mydomain.local				
						Car	ncel Update

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. Data Protector will always be able to use shares configured in this mode with no changes to either server or Data Protector 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 Data Protector media server and configuration changes to the Data Protector services. Individual users can then be assigned access to individual shares on the D2D Backup System. This authentication mode is ONLY recommended when the Data Protector 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 Data Protector Media server is a member of an AD domain.

Configuring User authentication mode

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

- Create a "local user" on the Data Protector Media server.
- Create a matching "local user" on the D2D Backup System.
- Configure Data Protector services to use the local user account.

- 1. Select or create a user on the server that will be used to administer the Data Protector media server and access the D2D Backup System, as follows:
 - Using Windows Device Manager select Users and Groups.
 - Create the user.
 - Add the user to the **Administrators** group for the local server.

■ File Action View Window Help ■	🔜 Computer Management				_ 🗆 X
Image: Second	📃 Eile Action Yiew Window He	elp			_8×
System Tools Built-in account for administering the Built-in account for guest access to Built-in account for Built-in account for Built-in access to Built-in acc	← → 主 📧 🗗 😫 😫 🗷				
Confirm password: □ User <u>m</u> ust change password at next logon □ User cannot change password □ Pass <u>w</u> ord never expires □ Account is disa <u>b</u> led	Computer Management (Local) System Tools System Tools Shared Folders Local Users and Groups Users Groups Performance Logs and Alert: Device Manager Storage Removable Storage Disk Defragmenter Disk Management Services and Applications	Name Administrator Guest New User Liser name: Eull name: Description: Password: Confirm pass User mu User cal V Passwor	Backupuser DP Backup User User configured I sword: sword: st change password at r nnot change password at r nnot change password rd rd never expires	Built-in account f Built-in account f Built-in account f for DP & D2D Backups	or guest access to

2. Set the D2D CIFS Server Authentication mode to **User**. Note that any existing backup or restore operations will fail if they are running when the authentication mode is changed.

Ø	D2D Backup Sy	stem			NEL PROPERTY		Logout Help
Home	Virtual Tape Devices	NAS	Configuration	Status	Replication	Administration	
d2d-mxq0	11096w : 192.168.0.110						🚫 Status
SI	nares CIFS Serv	er	NFS Server				
CIFS S	erver			_			
Authe	entication		User 💌				
			None User AD				Cancel Update

3. Configure a local user on the D2D Backup System with the same user name and password as the user created on the Windows Server (Backupuser in our example). Do this by selecting **NAS** — **CIFS Server** on the D2D Web Management Interface and clicking **Create User**.

Ø	D2D Backup Sy	stem	k.		No. of Concession, Name		Logout Help
Home	Virtual Tape Devices	NAS	Configuration	Status	Replication	Administration	
12d-m×q0	11096w : 192.168.0.110						🚫 Status
SI	nares CIFS Serv	er	NFS Server				
CIFS Se	erver		_		_	_	
Authe	entication		User				
							Edit
Users							
User	Name		Password		14	Password Confin	mation
Back	upuser			_			
							Cancel Update

4. In order for Data Protector to be able to authenticate with the D2D shares it must run the "Data Protector Inet" service under the new local user account that has been created on the D2D Backup System and on the Media server.

Change the logon account via the **Services** menu in Windows Computer Management. After changing the login credentials the service must be restarted for it to take effect.

B Eile Action ⊻iew Window H	elp				General Log On Recovery Depe	endencies)
• → 🖻 🖬 🖆 🗟 😫					Log on as:	
Computer Management (Local) System Tools Computer Management (Local) System Tools Computer Viewer Shared Folders Computer Sand Groups Computer Sand Groups Computer Sand Groups Computer Sand Sand Storage Computer Sand Sand Storage Computer Sand Sand Storage Computer Sand Sand Storage Computer Sand San	Name / Application Experience Lookup Service Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer 5 Computer Browser COM+ Event System COM+ Event System COM+ Event System COM+ System Application COM+ System Application Computer Browser Data Protector CRS Data Protector RDS Data Protector UIProxy DCOM Server Process Launcher Distributed Ella Suctam Extended Standard	Description Process ap Provides s Provides s Enables th Transfers f Enables Cli Supports S Maintains a Provides th (HP Data P (HP Data P (HP Data P (HP Data P Provides la Registers a Tohensher	Status Started Started Started Started Started Started Started Started Started Started Started Started Started	Startup Type ▲ Automatic Manual Manual Manual Disabled Automatic Manual Disabled Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic	Local System account Allog service to interact with This account Password: Confirm password:	

5. Now that the D2D Backup System is configured in User mode and Data Protector is configured to connect to the D2D shares with the correct credentials, it is possible to create a D2D share and apply access permissions to the Backupuser account.

Navigate to the **NAS** — **Shares** page, click **Create Share**, provide a share **Name** and **Description**, and then set the **Access Protocol** to **CIFS**.

me Virtual T	ape Devices	NAS	Configuration	Status	Replication	Administration	
-mxq011096w:192	.168.0.110						🥥 s
Shares	CIFS Serv	er	NFS Server				
hares							
O No Shares Con							hey should not be used as and performance. Create Share
Share Peri	nissions D2D Backu	up Share 1		_	_		
Share Peri	nissions D2D_Backu My first bac	450 00		_	_	_	
Share Perr Name Description	D2D_Backu	450 00					
hare1 Share Perr Name Description Access Protocol Write Protection	D2D_Backu	450 00					

6. After creating the share, select the **Permissions** tab and give **Access** rights to the Backupuser account.

	Configuratio	on Status I	Replication Admin	stration	
1.110					🚫 S
IFS Server	NFS Server				
n the D2D Backup	System are in	itended to be used	as targets for backup a	pplications. They sh	ould not be used as
age or ior drag-ani	о-огор раскор	is, aunig so will res	uit in iower deduplicati	in eniciency and per	iormanice.
Role	Status	Access Protocol	User Data Stored	Created	Last Modified
Non Replicating	🚫 Online	CIFS	1. A.	15:13 2010/06/28	15:13 2010/06/28
					Create Share
					<u> </u>
ne					
ns					
ns	CIFS				
	n the D2D Backup age or for drag-an Role	in the D2D Backup System are in age or for drag-and-drop backup Role Status	in the D2D Backup System are intended to be used age or for drag-and-drop backups, doing so will res Role Status Access Protocol	in the D2D Backup System are intended to be used as targets for backup a age or for drag-and-drop backups, doing so will result in lower deduplication Role Status Access Protocol User Data Stored	in the D2D Backup System are intended to be used as targets for backup applications. They sh age or for drag-and-drop backups, doing so will result in lower deduplication efficiency and per Role Status Access Protocol User Data Stored Created

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 Data Protector services to use the correct Domain account.

To join a domain

- 1. Connect to the D2D Web Management Interface, as follows:
 - Navigate to the NAS CIFS Server page
 - Click Edit
 - Choose **AD** from the drop-down menu
 - Provide the name of the domain that you wish to join e.g. "mydomain.local"

Ø	D2D Backup Sy	stem				-	Logout Help
Home	Virtual Tape Devices	NAS	Configuration	Status	Replication	Administration	
d2d-m×q0	11096w : 192.168.0.110						🚫 Statu:
SI	nares CIFS Serve	er	NFS Server				
CIFS S	erver		_		_		
Authe	entication		AD 💌				
Doma	in		mydomain.local				
						1	Cancel Update

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**.

To register with activ administration	re deectory domain, erber domain or name and pactors and
Domain Administration	
Passing	

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 follows:

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.

🚊 dnsmgmt - [DNS\EDGWARE\Forw	ard Lookup Zo	nes\mydomain.local]		_ 🗆 🗙
🚊 Eile Action View Window H	elp			_ 8 ×
	2 🖬 🗐			
Image: Second state	mydomain.l Name Da_msdcs	ocal 12 record(s) Type Data		
			1	

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.

🚊 dnsmgmt - [DNS\EDGWARE\Reve	rse Lookup Zones\192.168.0.х S	ubnet]		
🚊 Eile Action Yiew Window He	lp			<u>_8×</u>
A DNS	192.168.0.x Subnet 6 record(s)			
EDGWARE	Name	Туре	Data	
	(same as parent folder)	Start of Authority (SOA) Name Server (NS)	[7], edgware.mydo edgware.mydomain	.local.
💮 💮 _msdcs	I 192.168.0.1	Pointer (PTR)	edgware.mydomain	.local. nydomai
e setes for	Pointer (PTR) Host IP_number: 192_168_0_110 Eully qualified domain name 110.0.168.192.in-addr.ar Host name: d2d-mxq011096w.mydom Allow any authenticate	ain.local ain.local d user to update all DNS recor les only to DNS records for a n	Browse ds with the same ew name.	iyoonan n.local.
		OK	Cancel	

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.
 - Select NAS Shares from the D2D Web Management Interface and click Create.
 - Provide a share Name and Description, then select the CIFS protocol and click Create.

ne Virtual Ta	ape Devices	NAS	Configuration	Status	Replication	Administrati	on	-1
xq011096w : 192	.168.0.110							0 s
Shares	CIFS Serve	er	NFS Server					
ares								
File shares cre general purpos	ated on the D2 se storage or fo	D Backup or drag-an	i System are inten d-drop backups, d	ded to be us oing so will i	ed as targets for esult in lower de	backup applica eduplication effi	itions. They shou ciency and perfor	ld not be used as mance.
No Shares Conf	figured							
No Shares Conf	figured							Create Share
No Shares Conf are1	figured	_						Create Share
are1	nissions							Create Share
are1		p_Share_1		_				Create Share
are1 Share Perr	nissions	157 To						Create Share
are1 Share Perr ane	nissions D2D_Backu	157 To						Create Share

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.

Available <u>s</u> nap-ins: Snap-in	Vendor		Selected snap-ins:	Edit Extensions
Security Configurati				Remove
Security Templates	Microsoft Cor Microsoft Cor			
Services	Microsoft Cor			Move Up
Share and Storage	Microsoft Cor			
Shared Folders	Microsoft Cor	Add :	<u></u>	Move <u>D</u> own
Storage Explorer	Microsoft Cor Microsoft Cor	<u></u>		
	Microsoft Cor			
TPM Management	Microsoft Cor			
Windows Firewall wit	. Microsoft Cor			
Windows Server Bac				
WMI Control	Microsoft Cor	-		Advanced
Description:	urrent sessions, an			

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

File Action View Favorites Window Help		
Add or Remove Snap-ins	×	
Console	of snap-ins. For	
Select the computer you want this snap-in to manage.		
This snap-in will always manage:	Edit Extensions	
C Local computer: (the computer this console is running on)		
Another computer: hp-czj020039q.mycompany.local Browse	Remove	
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	Move Up	
	Move Down	
_ View		
C All C Sessions		
< <u>Back</u> Finish Cancel	Advanced	
Displays shared folders, current sessions, and open files.		
1		
	OK Cancel	

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

File Action View Favorites Wind	∖ hp-czj020039q.mycc dow <u>H</u> elp					_ 8
🔿 🖄 📅 🖪 🖬 🚺						
Console Root	Share Name 🔺	Folder Path	Туре	# Client Conn	Description	Actions
📸 Shares (\\hp-czj020039q.mycompan	🕺 BackupShare1	C:\tmp\nas\mountp	Windows	0	File Server 1 Backup	Shares (\\
	2 C\$	C:\lwcifs	Windows	0	Default Share	0.012 (201
	🕺 DPBackupShare1	C:\tmp\nas\mountp	Windows	0	HP D2D Share 3	More
	IPC\$	C:\	Windows	0	Remote IPC	
	🕺 NEWBackupShare1	C:\tmp\nas\mountp	Windows	0	Migrated Data Share	
•	4				•	

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**.

File Action Window Help Console Root Shares (\\h-cz)020039q.mycompant Security Beneral Permissions Security Beneral Provide Root Shares (\\h-cz)020039q.mycompant Stares (\\h-cz)020039q.mycompant	📅 Console1 - [Console Root\Shares (hp-czj020039q.n	nycompany.local)]				
Console Root Shares (\\hp-cz]020039q.mycompan Shares (\\hp-cz]020039q.mycompan Soup or user names: Group or user names: Administrator (MYCOMPANY\Administrator) More > Permissions for Administrator Allow Deny Full Control Change Read Learn about access control and permissions	📸 File Action View Favorites Wi	ow Help					_8×
Shares (\\hp-cz)020039q.mycompan General Publish Share Permissions Security Eroup or user names: Administrator (MYCOM PANY VAdministrator) Permissions for Administrator Allow Dery Full Control Change Read Dery Eul Control Learn about access control and permissions OK Cancel	🗢 🔿 🙍 🖬 🖬 🖉					<u></u>	
General Publish Share Permissions Security Broup or user names: PD 2D Share 3 Administrator (MYCOMPANYVAdministrator) HP 2D Share 3 Remote IPC NEWBacktur Add Bernove Permissions for Administrator Allow Dery Full Control Change D Read D Learn about access control and permissions DK Cancel		and provide a local division of the local di	hare1 Properties		×		Actions
Administrator (MYCOMPANY/Administrator) Add Add Add Add Add Bemove Permissions for Administrator Allow Deny Full Control Change Read Learn about access control and permissions OK Cancel Apply NewBackut More Networe	Shares (\\hp-czj020039q.mycompai	🦉 🗍 General 🛛 Pi	ublish Share Permissions	Security			Shares (\\ 🔺
Administrator (MYCOMPANY/Administrator) Administrator (MYCOMPANY/Administrator) Agd Agd Agd Agd Bemove Agd Bemove Agd Bemove Agd Bemove Permissions for Administrator Allow Dery Full Control Change Read Learn about access control and permissions OK Cancel Apply Remote JPC More More		34. Group or u	ser names:			1 - 1 1 2 3 3 3 1 1 1 1 1 1 2 3 1 2 3 3 3 3	More 🕨
Add Bernove Permissions for Administrator Allow Derny Full Control Change □ Read □ Learn about access control and permissions OK Cancel			istrator (MYCOMPANY\A	dministrator)			NEWBacku 🔺
Agd Bernove Permissions for Administrator Allow Permissions for Administrator Allow Full Control Image Change Image Read Image Learn about access control and permissions OK Cancel		33				Migrated Data Share	More
Permissions for Administrator Allow Deny Full Control Image Image Change Image Image Read Image Image Learn about access control and permissions Image Image Image Image I							
Permissions for Administrator Allow Deny Full Control Image Image Change Image Image Read Image Image Learn about access control and permissions Image Image Image Image I							
Permissions for Administrator Allow Deny Full Control Image Image Change Image Image Read Image Image Learn about access control and permissions Image Image Image Image I		1					
Full Control Image Change Image Read Image Learn about access control and permissions Image Image Image Image <td></td> <td></td> <td></td> <td><u>Add</u></td> <td><u>R</u>emove</td> <td></td> <td></td>				<u>Add</u>	<u>R</u> emove		
Change Read Learn about access control and permissions OK Cancel		Permission	s for Administrator	Allow	Deny		
Learn about access control and permissions DK Cancel Apply		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	trol				
Learn about access control and permissions OK Cancel Apply		5.2 S.C.					
OK Cancel Apply		neau					
DK. Cancel Apply							
DK. Cancel Apply							
DK. Cancel Apply							
		Learn abou	ut access control and perr	<u>hissions</u>			
				K Cancel	Acoly		
		•					<u> </u>

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. In order for Data Protector to be able to authenticate with the D2D shares it must run the "Data Protector Inet" service under the new local user account that has been created on the D2D Backup System and on the Media server.

Change the logon account via the Services menu in Windows Computer Management. After changing the login credentials the service must be restarted for it to take effect. In this case a user Backup is created and is a member of the BackupUsers group.

Computer Management				_ 🗆 🗙	Data Protector Inet Pro	operties (Local Computer)	?
및 Eile Action Yiew Window H	elp			_8×	General Log On Reco	overy Dependencies	
⊨ → 🖻 🖬 💣 🖻 🗟 😫					Log on as:		
IJ Computer Management (Local) ∃- 擬 System Tools	Name A Application Experience Lookup Ser	Description Process ap	Status Started	Startup Type	C Local System accou		
	Application Layer Gateway Service	Provides s Processes i	Started	Manual Manual	Allo <u>w</u> service to		
Local Users and Groups	ASP.NET State Service	Provides s Enables th	Started	Manual Automatic	Ihis account	Backup@mydomain.local	Browse
Groups	Background Intelligent Transfer 5	Transfers f	Dearted	Manual Disabled	Password: Confirm password:	·····	-
	COM+ Event System	Supports S Manages t	Started	Automatic Manual	You can anable or dival) ble this service for the hardware	profiles listed below.
	Computer Browser	Maintains a		Automatic	Hardware Profile	de uns service for une flatoware	Service
Disk Management	Cryptographic Services	Provides th [HP Data P		Automatic Automatic	Profile 1		Enabled
Telephony Services	Data Protector Inet	[HP Data P [HP Data P	Started Started	Automatic Automatic			
	Data Protector UIProxy	[HP Data P	Started	Automatic			
Indexing Service Indexing and Remote Access	DCOM Server Process Launcher	Provides la Registers a		Automatic Automatic		Enable	Disable
	Distributed File System	Integrates Enables cli	Started	Automatic Manual		Filance	
<u> </u>	Extended Standard			<u> </u>		OK Car	ncel Apply

2 Configure Data Protector to use D2D CIFS Share

Before configuring Data Protector it is good practice to check that the user authentication settings to be used by Data Protector are working.

To do this:

- Use Windows Explorer to navigate to the D2D CIFS share that is to be used for backup.
- Log in with the previously configured username and password to make sure that the share is accessible.
- Create an empty file on the share to ensure that it is writable.

NOTE: D2D shares should not be used for Drag-and-Drop storage; this check process is purely intended to prove that authentication configuration is correctly set up.

Creating a new Data Protector File Library

The first step in using Data Protector to back up to a D2D CIFS share is to create a File Library device.

1. Launch the Data Protector Manager and select the **Devices & Media** option from the context box.

Right click the **Devices** folder and select **Add Device** ...



2. A Wizard will now step through the process of creating a new device.

Provide a new **Device Name** and **Description**; it is useful if these provide information about the logical location of the CIFS share.

Then select File Library as the Device Type and click Next.

💶 Add Device - HP Data Protector M	anager		
Eile Edit View Actions Help			
Devices & Media		?]	
Environment Automated Operations	Specify the device name, t Optionally, add a description	he client system where the device is connected, and the device type. .n.	_
Devices Image: The second s	Device Na <u>m</u> e	D2D_Backup_Share_1	
€ 🚔 Extended Copy € 🚔 Media	Description	D2D - D2D-MXQ011096W	
	MultiPath device		
	☐ ⊻irtual tape library - TB based lin	pensing	
	Device <u>T</u> ype	File Library	
	Interface Type		
	Client	heathrow.mydomain.local	•
	N <u>D</u> MP Server		¥
	Management Console URL		
			-
		< <u>B</u> ack <u>N</u> ext > Finish <u>I</u>	 Cancel
🕼 Objects	N 4 D N Add Device 🛏		
		🔂 heathrow.mydomaii	n.local

3. The next step of the Wizard provide the path for where the file library is to be stored. This may be the path to the root level of the D2D CIFS share or it could be a directory within that share. The **Browse** button only works for storage that is local on the media server so cannot be used to locate the D2D CIFS share.

After adding the directory path, click **Properties** in order to specify the following parameters:

- **Maximum size of file depot:** This is the size of each individual backup file. The default is 5 GB; this should be set to a value larger than the expected maximum size of the backup jobs that are being sent to this file library. Doing so prevents the creation of lots of small files and the overhead of doing so.
- Minimum free disk space to create new file depot: The default is 2 MB which is OK.
- Amount of disk space that should stay free on disk: Leave this at the default of 0 MB as it makes little sense on a deduplicating file store.
- **Even if free disk space drops below** %: Leave this set at 10%. Although this has little relevance on a deduplicating filestore it still acts as a useful early warning.

Add Device - HP Data Protector M	fanager	
Devices & Media	월 ⊘ 🖬 🖣 🗉 😭 ? ♂ ♂ ● 📽 💐 🖄 ⋧ & 0	
Environment Environment Environment Devices Devices Devices Devices Devices Devices Devices Media	Specify a list of directories for the library. Add N192 168.0.110\D2D_Backup_Share_1\DFBackup1 Brgware Properties Dejete < Back Next > Epoteb	Properties General General Specify the maximum size of file depot, the minimum size to create new file depot, the amount of disk space which should stay free on the disk for the our entry selected disc correctings of file deficit, space at which an event will be fired if it drops below this value. Maximum size of file depot (GB) 200 (0.1 - 2000) Minimum fired disk size to create new file depot 2 (2 - 1000) Minimum fired disk space which should stay free on 0 (0 - 100000) Event if the free disk space dops below (%) 10 (0 - 100) QK Qencel Help
R Objects	H 4 F H Add Device	

4. In the next step of the Wizard specify the **Media Type**the **Standard** media type should be set to **File**, which is the default, and the **Distributed Media Format** should not be selected.

Distributed media format allows the creation of virtual full backups, however, this format is very inefficient when used with deduplication devices due to the creation of a large number of small files and the way in which these files are accessed in a random access fashion. If Distributed Media Format is selected, there will be a significant performance impact and possibility of backup failure.

BD Add Device - HP Data Protector Ma File Edit View Actions Help	anager	_ 🗆 ×
Devices & Media	≝⊘ E ≠ E E ? ≠ ≠ ≠ ≤ ≤ ≥ 5 €	
Environment Environment Device Policies Devices by host Extended Copy Media	Specify the type of media used in the library. Media Type Standard type of media used by the physical device. File Distributed file media format Using distributed file media format enables the file library for virtual full backup. Use distributed file media format	
		Cancel
R Objects		n.local

5. The final step of the Wizard provides a summary of the configuration, and also shows information about the disk space available on the D2D Backup System. If these values are 0, this is an indication that the Data Protector Inet service is not properly configured with the correct authentication settings and backups will fail.

BD Add Device - HP Data Protector M	anager				_ 🗆 ×
<u>Eile Edit View Actions Help</u>					
Devices & Media] 🚇 ⊗ 📷 🛥 📰 ?] 🛎 ♂ 💣 🕯	. 💰 2	, B	<u>n</u>	
Environment Environment Environment Environment Device Policies Environment Device Policies Devices	Summary All storage sizes are in GB				
🕀 👩 Devices by host	Directory Name	Total Size	Used	Max. Avail. for Backup	Max. File Dep
n ∰	T \\192.168.0.110\D2D_Backup_Share_1\DPBackup1	4131.330	0.113	4131.215	200.00
	< Back	1	lext >	Finish	
R Objects					
				heathrow.mydo	main.local

6. After completing the Wizard, the Devices and Media Environment folders will show information about the structure of the newly created file library. The **Devices** folder shows the **Directories** to be used and the **Drives** used to write to those directories.



7. The final step in configuring the File Library for use is to add more drives and modify their configuration, as described in the next section.

Configure drives

A single drive within the File Library will be automatically created, this allows for a single stream backup to the File Library. If multiple backup streams to the File Library are required, additional drives can be created. See *D2D Best Practices for VTL, NAS and Replication implementations* for more information on the maximum numbers of concurrent streams and recommendations on how many streams should be used for the different D2D Backup System products.

There are several settings for each drive that must be correctly configured in order to provide good D2D performance. Highlight each drive and select **Properties**. Go to the **Settings** Tab and click **Advanced**.

Advanced menu — Settings tab

On the Settings Tab of the Advanced menu is an option for **Concurrency**, this indicates how many parallel streams can write to that drive simultaneously, the default is three. Concurrency is a Data Protector term for Multiplexing, so the backup streams would be interleaved within the backup file, this is bad for deduplication so Concurrency should be set to 1 in order to prevent multiplexing.

ud I I I I I	Sizes Other Specify concurrency and options for device.
Concur	
)ptions	¢
D	Eject media after session
\sim	CRC Check
	☐ <u>R</u> escan
	📕 Detect dirty drive
	Drive-based encryption

Advanced menu — Sizes tab

On the Sizes tab the following settings are defined

- Block Size: this should be set to 512 KB for best performance
- **Segment Size:** this is how often a catalog section is written; it can be left at the default of 10 GB
- **Disk Agent Buffers:** this setting can be tuned to improve performance for slow client systems or media servers, the default of 8 is generally acceptable

lock size (kB)	512	 (8 · 1024)
egment size (MB)	10000	(10 or more)
isk agent buffers	8	(1 - 32)

Advanced menu — Policies tab

Lastly in the Policies tab of the drive properties enable the device for restore and as a source for object copies if required.



3 Configure a backup rotation scheme

When backing up to CIFS shares on the D2D Backup System it is recommended that a retention and rotation scheme similar 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 Backup Schedule created in Data Protector will define how long media will be retained before overwriting and, therefore, how many files will be created.

The following is an example of a best-practice backup rotation and retention scheme configuration with Data Protector. This scheme observes the following best practices:

- File Library 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.
- Only one "type" of data is backed up in this File Library 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; more "flat file" backups (of other client servers perhaps) could use the same File Library folder concurrently.
- 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.

To create a media pool

The first step in creating the new backup rotation scheme is to create a media pool. It is sensible to ensure that a backup has its own media pool as this prevents expired data from other backups being overwritten which would create a large amount of unrelated housekeeping.

NOTE: Ideally, separate media pools would be created for incremental and full backups from the same backup job, however Data Protector does not allow this configuration.

 Select the Devices & Media context, and expand the Media — Pools branch. There will be default pool entry for use with the new File Library but we will create a new one. Right click on the Pools folder and select Add Media Pool.

📴 Add Media Pool - HP Data Protector Manager	×0.
Eile Edit View Actions Help	
Devices & Media	→ → * * * * * * *
	Type a name for the media pool. Optionally, add a description. Pool Name Description Media Type Standard media type used by the physical device, drive, or library. Att
	< <u>B</u> ack. <u>N</u> ext > Finish <u>C</u> ancel
🗱 Objects	N 4 D M Properties for D2D_Backup_Share_1_Writer0
Add new media pool	, Carl Carl Carl Carl Carl Carl Carl Carl

Provide a Pool Name and Description, set the Media Type to File and click Next.

ices & Media 🗾 🔛 😒 📖 🛶 📖	ĨĨ ! ?] ♂ ♂ ● ≒ ▲ み <i>あ</i> ♡
Automated Operations Device Policies	Type a name for the media pool. Optionally, add a description.
Gimer Contraction Gimer Contraction Gimer Contraction Gimer Contraction Gimer Contraction	Pool Name D2D Local Server Backup Media
⊕	up1 Description Local Backup Media Pool
Gill Devices by host Gill Extended Copy	∼ Media Iype
☐ (marconic marconi	Standard media type used by the physical device, drive, or library.
D2D_Backup_Share_1_MediaPool Pofault AIT	
- Pefault DDS - Pefault DLT - Pefault DTF	
Default Exabyte	
🛨 🔐 Default LTO-Ultrium	
Default Optical	
Pefault QIC Pefault SAIT Pefault SD-3 Pefault SD-3 Pefault SD-3	

2. On the next step of the wizard set the allocation policy, by changing the **Usage** to **Non Appendable**. This ensures that all backups start a new backup file rather than appending to a backup file from a previous backup. In turn, this prevents a large housekeeping overhead when the appended file is overwritten.

Leave **Allocation** set to **Loose**; this will enable the use of any suitable media rather than requiring a specific media file, which often results in backup failure.

Do not select Allocate unformatted media first or Use Free Pool.

Click Next.

📴 Add Media Pool - HP Data Protector Manager			_ 🗆 🗙
Eile Edit View Actions Help			
Devices & Media] - - - - - -	-@	
	Select allocation policies Allocation Policies Allocation Allocation Allocation Allocate unformatt Use free pool Move free medi	for the new media pool and specify whether you want magazing the new media from the specify whether you want magazing the specify whether you want	Eancel
Dijects	N 4 🕨 🛛 Add Media Pool 🛶		
		🔂 heathrow.myd	omain.local //,

 Lastly you have the option to specify Media Condition Factors. This has little relevance to file media but will result in media files being marked as "Poor" once their "Valid for" and "Maximum Overwrite" thresholds are exceeded. So, these should be set to their maximum values of 828 Months and 9999 Overwrites. Click Finish and the new media pool will be created.

pu Add Media Pool - HP Data Protector Manager	<
Eile Edit View Actions Help	
Devices & Media	
Control Contro Control Control Control Control Control Control Control Control Co	Specify free pool options. These will be inherited by all media pools (of this media type) using the Media Condition Factors Media Condition Factors When these factors are exceeded, the medium is marked as poor and not used for backup. Vajid for (Monthe) 223 Magimum overwrites 3335 Set to Default < Back Media 200 Finish Cancel
💯 Objects	N 4 D N Add Media Pool -
	🔓 heathrow.mydomain.local

To create a backup job

Now a backup job can be created. In this example a simple "Filesystem" backup is going to be created to back up the local Cell Manager server.

1. Select the **Backup** context and expand the Backup Specifications folder. Right click **Filesystem** and select **Add Backup** ...to create a new Filesystem backup.

If other types of backup agents are to be used, e.g. VMWare backups then this Backup Specification should be selected instead.

B Backup - HP Data Protector Manager			
Eile Edit View Actions Help			
Backup 🗾 🔡 😵 🛅 🗰 🖻	1 ? BB 0 & x	1	
Raduel	Name	Description	
Backup Specifications Flexystem Resystem Re		Description Used for creation and modification of backup specifications. Used for creation and modification of backup templates.	
😰 Objects 📲 Tasks	N 4 D H Backup		
Add new backup specification		🚱 heathr	row.mydomain.local

2. The **Create New Backup Wizard** will now start, the first step is to choose from a default backup template or create a "Blank" template to configure manually. In this case we will select the "**Blank Filesystem Backup**" and click**OK**.

j Filesystem - HP Data Protect File Edit View Actions Help Backup ⊟- → Backup	 	
Backup Specifications Filesystem Mware Templates	Create New Backup Select a template to apply to the new backup. Use the Blank template to create a specification with n settings.	io default
	Filesystem Name Group Blank Filesystem Backup Default Person Daily_Intensive Default Daily_Intensive Default Dily_Intensive Default Dily_Intensive Default Dily_Intensive Default Dily_Intensive Default Dily_Intensive Default Dirix_INIM_template Default Weekly_Full_Catalog Default Weekly_Full_Catalog Default Weekly_Full_Og_Dire Default Weekly_Full_Catalog Default Weekly_Full_Catalog_Line Default Weekly_Full_Catalog_Line Default Weekly_Full_Catalog_Line Default Weekly_Full_Catalog_Line Default Weekly_Full_Catalog_Line Default Weekly_Full_Catalog_Line Default	
	Backup options Backup type Local or network backup Local or network backup Local or network backup Local or network backup Local or network backup	V
Objects	<u>ΩK</u> <u>Cancel</u>	

3. The next step is to select the items to be backed up, in this case just the local cell manager server. Then click **Next**.

Eile Edit View Actions Help						
Backup		- E S				
Backup Backup Specifications Filesystem More		Select the items that you	ı want to back up.			
Templates	Sho <u>w</u> :	All	•	Filesystem Bac	kup	1
		🗊 Internal Database 🖳 heathrow.mydomain.loc	-1		Mag Network Sha	re
		CONFIGURATION			Disconnect <u>S</u> hai	re
	±				<u>A</u> dd/Remove	
😰 Objects 📲 Tasks			< <u>B</u> ack	<u>N</u> ext >	Finish	<u>C</u> ancel
	1.00000	Backup - New1 🛶				

4. Now select the backup device, this is our newly created file library and writer device within it. If the Backup Specification were backing more than one object (i.e. filesystem or mount point) and had more than one writer device in the file library then it would be necessary to specify each writer to use for the backup and the load balancing configuration.

🕫 Backup - New1 - HP Data Prote	ector Manager		
Eile Edit View Actions Help			
Backup			
Backup Backup Specifications Generations Generation Generation Generation Generation Generation Generation	Select the devices or drives to be used for the backup.		
🕀 📺 Templates	Backup		Add Mirror
	C Show selected C Show all		Remo <u>v</u> e Mirror
	□ □ □ □ □ D2D_Backup_Share_1 □ □ □ □ □ D2D_Backup_Share_1_Writer0	Properties	Move Mirror <
		☑ Load balancing	Mov <u>e</u> Mirror >
		Min: 1 💌	
		Ma <u>x</u> 5 💌	
		< <u>B</u> ack <u>N</u> ext>	Finish Cancel
📳 Objects 📲 Tasks	H 4 D M Backup-New1 -		
			heathrow.mydomain.local

5. Select the **Properties.**.box in order to specify some additional options. In this case set the **Media pool** to the newly created pool to be used for this backup. **Concurrency** will already be set to 1 as this was previously configured for the writer device.

💼 Backup - New1 - HP Data Protector Man	lager	_ 🗆 ×
Eile Edit View Actions Help	Device Properties [D2D_Backup_Share_1_Writer0]	
Backup	General	
Backup Backup Specifications Filesystem Mware		
Templates		Add Mirror
c	<u>H</u> escan	Remo <u>v</u> e Mirror
		Move Mirror <
	Media pool	
	D2D Local Server Backup Media	Mov <u>e</u> Mirror >
	AddDelete	
	<u>DK</u> <u>Cancel</u> <u>Help</u> <u>voice</u>	Finish Cancel
📲 Objects 📲 Tasks 🛛 🕅 4 🕨		
		G heathrow.mydomain.local

6. The next page of the wizard provides options for specifying other backup options, in this case there are no changes required. The protection period options will be overridden by the schedule options that will be configured in the next step.

🔂 Backup - New1 - HP Data Prote	ector Manager	×
Eile Edit View Actions Help		
Backup		
Backup Specifications	Select the backup options for all objects in this backup specification. Backup Specification Options Adjust general backup specification options.	1
	Description Advanced	
	Filesystem Options Select the default protection period for all backed up files and directories. Protection: Permanent Advanced	
	☐ Disk Image Options	
	Select the default protection period for all backed up disk images. Piotection: Permanent Advanced	
	<back next=""> Eprinth Cancel</back>	
🕼 Objects 📲 Tasks	Кодаск <u>теки / прими далсен</u>	
	R R P R Backup - New T - M	- //

7. The last step is to create our backup schedule for Full and Incremental Backups. On the Schedules page click **Add...** to create an item in the schedule.

skup 🗾]] 🖳 🤇					?	相關		Z M	9					
Backup Backup Specifications Filesystem Kommen Templates Templates	7	Spec run o	ify the c n holida	lates ar iys.	nd time	is that y	ou want	backup	s perfo	ormed. C	iheck ti	ne Holi	day box	to indicate that you do not want scheduled	backups to
			21	010 J	ul						lugus	.+			
			2	510 5	ui					-	sugue	<u>.</u>		<u><u>R</u>eset</u> Predefined	
	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	
				1	2	3	4							1 🗖 Holida <u>y</u> s	
	5	6	7	8	9	10	11	2	3	4	5	6	7	8 🗖 Disable schedule	
	12	13	14	15	16	17	18	9	10	11	12	13	14	15 Legend	
	19	20	21	22	23	24	25	16	17	18	19	20	21	22 Full Incremental	
	26	27	28	29	30	31		23	24	25	26	27	28	29 Full + Incr	
								30	31					Holidays	
	i ⊢ 07 Jul	2010													
)ptions		r						[Add.		
	Tim		/pe u	ptions		2			_		_		A <u>a</u> a. Delete		
													Dejete		

For the schedule that we are creating there will be some "conflicts" where for example monthly backups occur on the same day and time as some daily backups. In order to ensure that these higher priority backups overrule schedules for those lower down the priority list, configure backups in the following priority order: 1. Yearly, 2. Monthly, 3. Weekly, 4. Daily.

8. Firstly we will create an annual full backup to run on the 1st January at 21:00, the protection period for this backup is set to **Permanent** to ensure that it is never overwritten.

Recurring	Time options
	Time: 21:00
C Daily	
C Wee <u>kl</u> y	✓ Use starting
 Weekiy Monthly 	01/01/2011
Session options	
Session options Backup type	Full
	Full 💌

Configure monthly full backups to be overwritten every 12 months (52 weeks).

Recurring Non <u>e</u> Daily Wee <u>k</u> ly Monthly	Time options Time: 21:00 ★ Use starting 07/07/2010 ▼	
ecurring options	1 * of every 1 * month	
ession options		
iession options Backup type	Full	
	Full High O Medium O Low	

Configure weekly full backups to run at 21:00, which are overwritten every 4 weeks.

Recurring	Time options
⊂ Non <u>e</u>	Time: 21:00 *
O Dajly	Use starting
Weekly	
C Mo <u>n</u> thly	07/07/2010
Becurring options Every ⊂Sun ┌─ Mon	1 ★ week(s) on Tue ■ Wed ■ Thu ■ Fri ♥ Sat
Every Sun Mon Gession options	Tue ■ Wed ■ Thu ■ Fri ♥ Sat
Every ⊂ Sun ┌─ Mon	
Every Sun Mon Session options Backup type	Tue ■ Wed ■ Thu ■ Fri ♥ Sat

Lastly create a daily incremental backup to be overwritten every week.

łecurring ONon <u>e</u> ODajly ▼Weeklu	Time options Time: 21:00
- wee <u>⊾</u> iy D Mo <u>n</u> thly	07/07/2010
Every Sun I⊽ Mon	1 🛃 week(s) on I Tue I Wed I Thu I Fri I Sat
Sun 🔽 Mon	I Tue I Wed I Thu I Fri □ Sat

9. After creating all of the schedule entries, proceed to the Summary page and select **Save As** ... from the finishing steps page.

🔂 Backup - New1 - HP Data Prote	ctor ManagerX
Eile Edit View Actions Help	
Backup	ਤ,월⊘ 首,—■ = = ? 5 ፼ - € Ø
Backup Backup Specifications Filesystem	Perform finishing steps in your backup/template design.
ि WMware स्रि ि Templates	Save as Save the newly created backup/template.
	Save Backup As X Type the name and select a group, where you want to save your new backup specification. Image: Comparison of the save your new backup specification.
	Name Local Server Backup Rotation ication. This option is available only for filesystem, es/Domino, SAP and SAPDB backup. Preview is not Group Default Image: Common Section Common
	QK <u>C</u> ancel <u>H</u> elp
	<back next=""> Finish Cancel</back>
🙀 Objects 📲 Tasks	N 4 ▷ Ø Backup - New1 - ₩ Backup - № Backup - New1 - ₩ Backup - № Bac

The backups will now run according to the new schedule and, 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 Data Protector creates two files; one is the backup data file depot which grows throughout the backup, the other is a temporary file of 15 MB which is removed when the backup completes.

About this guide

This guide:

- Provides step by step instructions on configuring a D2D NAS CIFS device on HP Data Protector 6.11
- Describes the HP Data Protector 6.11 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 HP Data Protector 6.11.

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 HP Data Protector 6.11 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 1 Document conventions

Convention	Element
Blue text: Table 1 (page 31)	Cross-reference links and e-mail addresses
Blue, underlined text: <u>http://www.hp.com</u>	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 1 Document conventions (continued)

Convention	Element
Monospace text	 File and directory names System output Code Commands, their arguments, and argument values
<i>Monospace, italic</i> text	Code variablesCommand variables
Monospace, bold text	Emphasized monospace text

Marning! Indicates that failure to follow directions could result in bodily harm or death.

- Δ 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:

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

Documentation feedback

HP welcomes your feedback.

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

Index

A

access permissions, 10 AD authentication, 4 configuring, 7 audience, 31 authentication modes, 4

В

backup job, 23 backup rotation scheme best practices, 20 backup schedule, 27

С

check share accessible, 14 CIFS server, 4 concurrency, 18 configure AD authentication, 7 backup job, 23 backup rotation scheme, 20 CIFS server, 4 drives, 18 media pool, 20 user authentication, 4 conventions document, 31 text symbols, 32 create file library, 14 create shares, 10

D

Data Protector Inet service, 13 document conventions, 31 related documentation, 31 documentation HP website, 31 providing feedback, 32 domain, 8 drives configuring, 18

F

file library, 14

Н

help obtaining, 32 host(A) record, 9 HP technical support, 32 J

join domain, 8

Μ

media pool, 20

Ρ

performance, 18 Pointer(PTR) record, 9

R

related documentation, 31

S

schedule, 27 service , 17 share check accessible, 14 symbols in text, 32

Т

technical support HP, 32 service locator website, 32 text symbols, 32

U

user authentication, 4 configuring, 4

W

websites HP , 32 product manuals, 31