

Setting Up the Dell^{TM} DR Series System as a VTL Backup Target on Microsoft[®] Data Protection Manager

Dell Engineering January 2016

Revisions

Date	Description	
February 2015	Initial release	
April 2015	Updated for current release	
January 2016	Updated content related to spanned tapes and driver and registry requirements,	

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2016 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <u>http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector</u> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell[™], the Dell logo, and PowerVault[™] are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Microsoft[®], Windows[®], Windows Server[®], Internet Explorer[®], MS-DOS[®], Windows Vista[®] and Active Directory[®] are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat[®] and Red Hat[®] Enterprise Linux[®] are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell[®] and SUSE[®] are registered trademarks of Novell Inc. in the United States and other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

1	Executive summary		
2	Insta	Illing and configuring the DR Series system	5
3	Crea	ting and configuring iSCSI target containers for Microsoft DPM	9
	3.1	Creating the iSCSI VTL container	9
	3.2	Configuring the Microsoft DPM Server – Windows	11
	3.3	Installing device drivers for the DR Series system iSCSI VTL	14
	3.4	Configuring Microsoft DPM registry settings	16
	3.4.1 Conr	. Adjusting BufferQueueSize, ConnectionNoActivityTimeout, and nectionNoActivityTimeoutForNonCCJobs registry settings	17
	3.4.2	2 Adding the TapeSize parameter	
	3.4.3	3 Adding the Storport key and BusyRetryCount parameter for each tape	19
	3.4.4	Disabling TUR	21
	3.5	Setting up Microsoft DPM to use the newly created iSCSI VTL	23
4	Perfo	orming backup and restore by using the DR Series system VTL	26
5	Resto	oring from tape	
6	Setti	ng up the DR Series system cleaner	44
7	Moni	itoring deduplication, compression, and performance	45
А	Mana	aging VTL protocol accounts and credentials	46
	A.1	Managing iSCSI account details	46
	A.2	VTL default account summary table	47
В	Mana	aging VTL media and space usage	48
	B.1	General performance guidelines for DMA configuration	48
	B.2	VTL space sizing and planning	48
	B.3	Logical VTL geometry and media sizing	49
	B.4	Media retention and grouping	50
	B.5	VTL media count guidelines	50
	B.6	Adding VTL media to a VTL container	50
	B.7	Space reclamation	52
	B.7.1	General guidelines	52
	B.7.2	Product specific guidelines	52



1 Executive summary

This document provides information about how to set up the Dell DR Series system as a backup target for Microsoft Data Protection Manager (DPM) software (Microsoft DPM 2010 and later). This document is a quick reference guide and does not include all DR Series system deployment best practices. For additional information, see the DR Series system documentation and other data management application best practices whitepapers for your specific DR Series system at:

http://support.dell.com/manuals

Note: The DR Series system and DPM screenshots used in this document may vary slightly, depending on the DR Series system firmware version and Microsoft DPM version used.



2 Installing and configuring the DR Series system

- 1. Rack and cable the DR Series system and power it on.
- 2. Initialize the DR Series system. For more information, in the *Dell DR Series System Administrator Guide*, refer to the following topics: "iDRAC Connection," "Logging in and Initializing the DR Series System," and "Accessing iDRAC6/iDRAC7 Using RACADM".
- 3. Log on to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use the user name and password of "**root/calvin**".

	TED DELL REMOTE CONTROLLER 6 - ENTER	PRISE	Support Ароня К	Logout
System Dell DR4000 root , Admin	Properties Setup System Summary St	Power Logs Alerts Console/Media stem Details System Inventory	vFlash Remote File Share	
System IDDAC Settings	System Summary		. C	2
Batteries Fans Intrusion	Server Health			
Power Supplies	Status Component		Virtual Console Preview	
Temperatures	Batteries /		Options : Settings	
Voltages	Pana Pana			
PowerMonitoring	Infrusion		and the state of t	
	Power Supp	les		
	Removable	flash Media		
	Temperature Temperature	8		
	Vutages		Relesh Launch	
	Server Information		Guick Launch Tasks	
	Power State	ON	Power Ott/ OFF	
	Oystem Model	Dell DR4000	Power Cycle System (cold boot)	
	System Revision	1	Launch Virtual Console	
	Dystem Host Name	DR4000-DKCV6S1 asglab roundrock	View System Event Log	
	Operating System	CentOS	View IDRAC Log	
	Operating System Version 2.5.1	sion 2.6.18-164 e	Update Firmware	
	Service Tag	DKCV6S1	RésetIORAC	
	Express Denice Cod	29529104401		
	BIOG Version	1.9.0		
	Firmware Version	1.80 (Build 17)		

4. Launch the virtual console.

5





5. After the virtual console is open, log on to the system with the user **administrator** and the password **St0r@ge!** (the "0" in the password is the numeral zero).



6. Set the user-defined networking preferences.



7. View the summary of preferences and confirm that it is correct.

Set Static IP A	ddress	•••••
IP Address	: 10.10.86.108	
Network Mask	: 255.255.255.128	
Default Gateway	: 10.10.86.126	
DNS Suffi×	: idmdemo.local	
Primary DNS Server	: 10.10.86.101	
Secondary DNS Server	: 143.166.216.237	
Host Name	: DR4000-5	
Are the above settings correct	(yes/mo) ? _	



8. Log on to the DR Series system administrator console using the IP address you just provided for the DR Series system, the username **administrator**, and the password **St0r@ge!** (the "0" in the password is the numeral zero).

DEAL DR4000-DKCV	/651	Help
.ogin	Piease enter your password:	ResetPassword
	Username: administrator	
	Password: St0r@gel	
	Log in	

9. Join the DR Series system to Active Directory.

Note: If you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

a. Select Active Directory from the left navigation area of the DR Series system user interface.



Copyright © 2011 - 2013 Dell Inc. All rights reserved.

b. Enter your Active Directory credentials.

	DELL DR4100 edwinz-sw	r-01 Help Log nut
	Global View	Active Directory Jeen
-	Alerta	Settings
	Events Health Usinge	The Active Directory settings have not been configured. Click on the John link to configure them.
	Statistics: Container	Active Directory Configuration
•	Statistics: Replication Storage Containers Replication	Domain Name (FGDN)*
	Compression Level Clients Schedules	Password Enter Active Directory Info
	Replication Schedule Gleaner Schedule	Cancel Join Domain
-	Networking	
-	Active Directory Local Workgroup Usera Email Adenta Admin Contact ado Pais secol Email Relay Host Date and Time Support Chapnesitos Support Chapnesitos Subware Upgrade Uconse	



3 Creating and configuring iSCSI target containers for Microsoft DPM

3.1 Creating the iSCSI VTL container

For this procedure, you need to create and export the iSCSI container as described in the following steps.

1. Select **Containers** in the navigation panel on the left navigation area, and then click the **Create** link at the top of the page.

DELL DR4000					administrator (Log	out) Help
dr9-interop-a7.ocarina.local 🔽 — — Global View	Containers			2 Create I	Edit Delete Displa	ay Statistics
 Dashboard Alerts 	Number of Containers: 2				Container Path:	/containers
Events	Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
Health	backup	0	Auto	NFS, CIFS	Not Configured	0
Container Statistics	intvm05iscsi	31	Networker	VTL iSCSI	Not Configured	0
Replication Statistics						
- Storage						
Containers						
Replication						
Clients						
Schedules						
+ System Configuration						
+ Support						
Copyright © 2011 - 2014 Dell Inc. All rights reserved.						

2. Enter the container name, select Virtual Tape Library (VTL), and then click Next.

ontainer Wizard - Create N	ew Container	
Container Name		* = required fi
Container Name*:	Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter. iscsiVTL1	
/irtual Tape Library (VTL) :		
	2	
		Cancel Next >



 For the Access Protocol, select iSCSI, and then specify the Data Management Application Access Control by entering the Microsoft DPM server IP Address, IQN, or FQDN. For Microsoft DPM, you also need to specify Marker Type as Auto. Click Next.

Configure Virtual Tape Library —		* = required fie
Is OEM:	Con isc	tainer Name and Type siVTL1
Tape Size:	● 800GB ○ 400GB ○ 200GB VT	L
	○ 100GB ○ 50GB ① 10GB	
Access Protocol:	NDMP ISCSI No Access	
Access Control (initiator):	IQN, FQDN or IP	
Marker Type:	O Unix Dump O Networker O BridgeHead	
	None Auto Time Navigator	
	< Back	Cancel Next >

4. Click **Create a New Container** to create the VTL container.

Container Wizard - Create New Container		
Configuration Summary	* = required fields	
Container Name and Type	Virtual Tape Library	
Container Name: iscsiVTL1	OEM: no	
Connection Type: VTL	Tape Size: 10gb	
	Access Protocol: iSCSI	
	Access Control: iqn.1991-05.com.microsoft:2k8r2intvm05	
	Marker Type: Auto	
	< Back Cancel Create a New Container	
	hannan hanna ha	



3.2 Configuring the Microsoft DPM Server – Windows

1. Configure the iSCSI Initiator Software for Windows by providing the IP or FQDN of the DR unit in the **Target** field, and then click **Quick Connect**. The Quick Connect dialog box opens that indicates a connection was made but is set inactive as show below.

CSI Initiator Properties	X	
Targets Discovery Favorite Targets Volumes and Devices	RADIUS Configuration	
To discover and log on to a target using a basic connection, typ DN5 name of the target and then click Quick Connect.	e the IP address or	
Target:	Quick Connect	
Discovered targets	Duich Connect	
	Juick Connecc	^
I Valitë	Targets that are available for connect provided are listed below. If multiple to each target individually. Connections made here will be added to restore them will be made every tir	tion at the IP address or DNS name that you targets are available, you need to connect to the list of Favorite Targets and an attempt ne this computer restarts.
	Discovered targets	
	Name ign. 1984-05. com. dell: dr4000. 9lbp8;	Status
, To connect using advanced options, select a target and then click Connect.		
To completely disconnect a target, select the target and then click Disconnect.		
For target properties, including configuration of sessions, select the target and click Properties.	- Duranti -	
For configuration of devices associated with a target, select the target and then click Devices.	Unable to Login to the target.	
More about basic ISCSI connections and targets		
	Connect	Done
ОК		

2. Click **Done** to close the dialog box and proceed by selecting the newly discovered target. This target will have an *Inactive Status* as it requires authentication parameters to be provided for iSCSI logon. Select the Target from the list, click the **Connect** button, and then in the **Connect to Target** dialog box, click the **Advanced** button.



iSCSI Initiat	or Properties	X
Targets D	iscovery [Favorite Targets] Volumes and Dev	vices RADIUS Configuration
	nect	
To discov	er and log on to a target using a basic connection	tion, type the IP address or
DNS name	of the target and then click Quick Connect.	
	r	_
Target:		Quick Connect
Discovere	d targets	
		Refresh
Name		Status
(iqn. 1984	-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Inactive
		2
To conner	t using advanced options, select a target and t	Ithen Connect
Connect To Target	.000.	X
connect to rarget		Disconnect
Target name:		
iqn.1984-05.com.dell:dr4000.9lbp	8r1.intvm05iscsi.10	Properties
Add this connection to the list of	f Favorite Targets.	
This will make the system auton	atically attempt to restore the	Devices
connection every time this comp	outer restarts.	
Enable multi-pa		
	ov 1	
Advanced	OKCancel	
	OK	Cancel Apply

3. In the Advanced Settings dialog box, select to Enable CHAP log on and type the User Name and Target Secret / Password. Click OK. See Appendix A for more details about accounts and credentials.

anced Settings	
neral IPsec	
Connect using	
Local adapter:	Default
Initiator <u>I</u> P:	Default
<u>T</u> arget portal IP:	Default
CRC / Checksum	
🗖 Data digest	🔲 Header digest
CHAP log on inform CHAP helps ensure of an initiator. To use, specify the s initiator. The name of coefficient	nation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is 2
CHAP Lon on inform CHAP helps ensure of an initiator. To use, specify the s initiator. The name specified.	nation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is dr9-interop-a7
CHAP Lon on inform CHAP helps ensure of an initiator. To use, specify the : initiator. The name specified. Name: Target secret:	mation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is dr9-interop-a7 •••••••••
CHAP Lon on inform CHAP helps ensure of an initiator. To use, specify the t initiator. The name t specified. Name: Target gecret: Perform mutual a To use mutual CHAP RADIUS. Use RADIUS to a	matter connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is dr9-interop-a7 extension authentication , either specify an initiator secret on the Configuration page or use enerate user authentication credentials uptenticate target credentials

The iSCSI target should now show as connected, and the device discovery can now proceed.

51 Initiator Properties		
argets Discovery Favorite Targets Volumes and Device Quick Connect To discover and log on to a target using a basic connection, DNS name of the target and then click Quick Connect.	; RAE type th	DIUS Configuration
Target:		Quick Connect
Discovered targets		Refresh
Name iqn.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Conr	us nected
To connect using advanced options, select a target and the click Connect.	٦	Connect
To completely disconnect a target, select the target and then click Disconnect.		Disconnect
For target properties, including configuration of sessions,		Properties
select the target and click Properties.		
select the target and click Properties. For configuration of devices associated with a target, select the target and then click Devices.		Devices
select the target and click Properties. For configuration of devices associated with a target, select the target and then click Devices. More about basic ISCSI connections and targets		Devices



3.3 Installing device drivers for the DR Series system iSCSI VTL

After making an iSCSI connection to the VTL, the next step is to install drivers. For the DR Series system to work properly with Microsoft DPM, you need to install drivers for the medium changer and tape drives.

1. From the **cmd** prompt, type the following command to open Device Manager. **devmgmt.msc**

The DR Series system iSCSI VTL will be listed in the Device Manager as shown in the following screenshot.

Administrator: Command Prompt			
C:\Users\administrator.TESTAD>devmgmt.msc	<u>^</u>		
C:\Users\administrator.TESTAD>	=		
Device Manager		-	□ X
File Action View Help			
👂 🧫 Disk drives			^
🔈 🖳 Display adapters			
▶ 🔮 DVD/CD-ROM drives			_
▶ 🕼 Human Interface Devices			
▶ — Keyboards			
Medium Changer devices Helmaum Medium Changer			
Mice and other pointing devices			
Note and one pointing devices ▶ ■ Monitors			
Network adapters			
🔈 🖶 Print queues			
Processors			
Storage controllers			
👂 🖳 System devices			≡
🛛 📇 Tape drives			
IBM ULT3580-TD4 SCSI Sequential Device			
BM UL 13580-104 SCSI Sequential Device			
BIM UL 13380-104 SCSI Sequential Device			
IBM ULT3580-TD4 SCSI Sequential Device			
IBM ULT3580-TD4 SCSI Sequential Device			
IBM ULT3580-TD4 SCSI Sequential Device			
📕 IBM ULT3580-TD4 SCSI Sequential Device			
📇 IBM ULT3580-TD4 SCSI Sequential Device			
📇 IBM ULT3580-TD4 SCSI Sequential Device			
			Y

 To install device drivers for the Medium Changer, you need to get the device drivers at the following link: <u>http://catalog.update.microsoft.com/v7/site/Home.aspx</u>. Search for the following: "StorageTek - Storage - Sun/StorageTek Library"



TRA				pade catalog	~				
licrosoft"Update Catalog "StorageTek - Storage - Sun/StorageTek Library" Search									
Q h	elp						view basket (0) 🗳		
Se Se	arch results for ""S	StorageTek - Stora	ae - Sun/StorageT	ek Librarv""					
Jpdate	es: 1 - 2 of 2 (page 1	of 1)		5			🔶 Previous Next 🛶		
	Title	Products	Classification	Last Updated	Version	Size	Add All		
	StorageTek -	Windows Server	Drivers (Other	6/22/2009	2.3.0.0	18 KB	Add		
	Sun/StorageTek Library	Server 2008	naroware)						

.

3. Extract the package contents and install the drivers through the Device Manager. (You can refer to Microsoft online help for instructions on installing device drivers.) After installation, the library drivers will appear in the Device Manager, as shown in the following screenshot.



Dél



- 4. You need to upgrade the device drivers for the tape drive as well. Use the following drivers, which you can download from IBM as per your operating system at: <u>http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Tape%2Bdrivers%2Band%2Bsoftware&product=ibm/Storage_Tape/Tape+device+drivers&release=1.0&platform=Windows&function=all</u>
 - Windows 2008 R2 SP1 IBMTape.x64_w08_6250
 - Windows 2012 R2 IBMTape.x64_w12R2_6248_WHQL_Cert

Note: You should Install the drivers in non-exclusive mode. (Double-click the nonexclusive executable.)

5. Extract the .cab file, and then use Device Manager to install the driver by pointing to the extracted location.

3.4 Configuring Microsoft DPM registry settings

Note: Restoration of certain files that span across multiple tapes might fail if they are restored as part of a single job. When an attempt is made to restore all of the files in the same job, the recovery of the files (shown in the following graphic in pink) **might still fail**. However, with the registry setting listed below, when these files are individually restored the restores will pass.

	TAPE-1		TAPE-2		TAPE-3			TAP	°E-4		TAPE-5		TAPI	E-6	
1-file_10G	2-file_80G	3-file_20G	4-file_80G	5-file_20G	6-file_80G	7-file_20G	8-file_20G	9-file_20G	10-file_20G	11-file_20G	12-file_120G	14-file_20G 13-file_10G	15-file_20G		

For DPM to work properly with the DR Series system, you need to apply the following DPM registry settings. The following subsections describe how to adjust these settings in more detail.

Registry Setting	Value to add/edit
Set BufferQueueSize	1
Set ConnectionNoActivityTimeout and	7200
ConnectionNoActivityTimeoutForNonCCJobs	
TapeSize	Add this parameter
Storport key	Add for each tape
BusyRetryCount	Add for each tape
TUR	Disable
Service_Name	Add the AutoRun value

Note: A system reboot is required for updated registry settings to take effect.



3.4.1 Adjusting BufferQueueSize, ConnectionNoActivityTimeout, and ConnectionNoActivityTimeoutForNonCCJobs registry settings

Follow these steps:

- 1. Open a Command Prompt and type the following command to open the Registry Editor window. regedit
- 2. In the Registry Editor window, go to the following path: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent
- 3. Right-click and select New > DWORD (32 bit) Value, and then enter the value as: BufferQueueSize
- 4. Right-click **BufferQueueSize**, and select **Modify**. Select the Base value as Decimal and then enter **00000001** as the value in the text box. Click **OK**.
- 5. Right-click and select **New > DWORD (32 bit) Value**, and then enter the value as: **ConnectionNoActivityTimeout**
- 6. Right-click **ConnectionNoActivityTimeout**, and then select **Modify**. Select the Base value as Hexadecimal, and enter **00001c20** as the value in the text box. Click **OK**.
- 7. Right-click and select New > DWORD (32 bit) Value, and then enter the value as: ConnectionNoActivityTimeoutForNonCCJobs
- 8. Right-click **ConnectionNoActivityTimeoutForNonCCJobs**, and then select **Modify**. Select the Base value as Hexadecimal, and then enter **00001c20** as the value in the text box. Click **OK**.

Registry Editor						_ 6 ×
File Edit View Fa	workes Help	- A.				
	Cryptography	Name	Туре	Data		
	CTF	(Default)	REG 5Z	(value not set)		
	DataAccess	CPEstrataled	REG DWORD	0x0000001F(31)		
	DataFactory	10 BufferOueueSize	REG DWORD	0x00000001 (1)		
	DevDiv	ConnectionNedictivityTimenuk	REG DWORD	0v00001z20 (7200)		
	DFS.	Connection/InActivityTmesu#ExtMon/Clobs	REG DWORD	0x00001c20 (7200)		
· · ·	Direct3D					
	DirectDraw					
1 I I I I I I I I I I I I I I I I I I I	DirectInput					
	Direct/Say8					
	DirectPlayNATHelp					
	DirectShow	1				
	Dwectx					
	DownloadManager					
	Universigning					
10	Enternet and Enternet					
6	EuseEustan					
	E12					
10 M	Eands					
141	Function Discovery					
	Fusion					
	Help					
	HTMLHelp					
	IdentityCRL					
	IMAPI					
	DEP					
÷.	MER					
	IMETC					
æ .	InetStp					
8	Internet Account Manager					
	Internet Domains					
1 E	Internet Explorer					
8	Microsoft Data Protection Manager					
	E 1.0	-				
	1 2.0					
1	ADDER					
	Exchange files					
	tostalierteus					
1	Colocation					
	E Configuration					
	00					
	- KB					
	Setup					
•	Microsoft SDKs					
	Microsoft SQL Server					
	Microsoft SQL Server 2005 Redist					
8-3	Microsoft SQL Server 2012 Redist					
) (B)	Microsoft SQL Server Native Client 11.0					
8-	DEAC.					
	Mobile					
	Miseuald					
	MODE					
101	MONTO					
	MCE					
2	Millionsing					
	MSMO					
	MSSOLServer					
	NapServer	-				
Computer/HKEY_LOCA	A_MACHINE\SOFTWARE\Mcrosoft/Mcrosoft Data Protection	n Manageri Agent				
1 30		3				10-11 AM
Start 75	23 🔜 😎 🔍 📷 😚	• J			8	12/17/2015
and the second sec	and the second s				la construction de la constructi	ant a transfer

3.4.2 Adding the TapeSize parameter

Follow these steps:

- Open a Command Prompt and then type the following command to open the Registry Editor window: regedit
- 2. In the Registry Editor, go to the following path: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent
- 3. Right-click and select New > DWORD (32 bit) Value, and enter the value as: TapeSize
- 4. Right-click **TapeSize**, and then select **Modify**. Select the Base value as Decimal, and enter (TapeSize * 1024) as the value in the text box. Click **OK**.

Note: If you are using 800GB tapes, then the value becomes 800 * 1024 = 819200.

Note: If the TapeSize parameter is not defined, by default, it is 30GB.

😰 Registry E	Editor	a new second				_ 8 ×
File Edit Vie	ew Fa	avorites Help				
	B-1	Cryptography 🚊	Nome	Туре	Data	
	.8-	CTF	(Default)	REG_52	(value not set)	
		DataAccess	20 QFEsinstalled	REG_DWORD	0x0000001f (31)	
	•	DataFactory	#BufferQueueSize	REG_DWORD	0x00000001 (1)	
		DevDiv	20 ConnectionNoActivityTimeout	REG_DWORD	0x00001c20 (7200)	
	1	DPS	202 ConnectionNoActivityTimeoutForNonCCJobs	REG_DWORD	0x00001c20 (7200)	
	1	DirectaD	W TapeSze	REG_DWORD	Gx000c8000 (019200)	
	1	DrectDraw				
	10	Directinput				
	1	DirectPlays				
	(B) (Direconaynwirrep				
	10	Directoriow Directoriow				
	10	President Manager				
		Driver Siming				
		DXP				
	in l	ExtentriseCertificates				
	é.	EventSystem				
	÷-	F12				
	1-0	Feeds				
		Function Discovery				
	10	Fusion				
	10	Help				
		HTMLHelp				
	1-1	IdentityCRL				
	1.1-1	IMARI				
	18-1	DME3P				
		IMEXR				
		IMETC				
	8-	InetStp				
		Internet Account Manager				
	•	Internet Domains				
		Internet Explorer				
	8	Microsoft Data Protection Manager				
		E 🔒 1.0				
	1.5	2.0				
		- ADMK				
		2.0 Fundada differen				
		LicoudedHies				
	1.5	a instanting				
	1	Configuration				
	111	Compation (
		KB.				
		Setup				
	10-1	Microsoft SDKs				
	10	Microsoft SQL Server				
	÷.	Microsoft SQL Server 2005 Redist				
		Microsoft SQL Server 2012 Redist				
		Microsoft SQL Server Native Client 11.0				
		MMC				
		Mobile				
		MSBuild				
		MSDE				
	11	MSDLS1				
		MSDTC				
		NGP				
		MSLicensing				
	1	MSMQ .				
		ManServer w				
Computer() #EY	LOCA	AL_MACHINE\SOFTWAREIMicrosoft(Microsoft Data Protection /	Manager\Agent			
Start	澳					* D- 00 (n. 10:16 AM
	100		1			12/17/2015

3.4.3 Adding the Storport key and BusyRetryCount parameter for each tape

Follow these steps.

- To get a list of all the tape devices in your DPM Server to which you need to add the registry key, run the following command from an administrative command prompt.
 wmic tapedrive list brief

This command returns a list of tape drives **Scsi\DeviceID\Instance** that you can use to make the above change.

3. Right-click **DeviceParameters**, select **New > Key**, and change NewKey as **Storport**.



- To add BusyRetryCount value for Storport key, right-click and select New > DWORD (32 bit) Value. Enter the value as BusyRetryCount
- 5. Right-click **BusyRetryCount** and select **Modify**. Select the Base value as Decimal, and enter **250** as the value in the text box. Click **OK**.

Déd

6. Ensure the Storport and BusyRetryCount settings are configured for all tape drives



3.4.4 Disabling TUR

Follow these steps.

To disable TUR, you need to find the service name used by the tapes. To find the service name, go to the following path:
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI\<DEVICEID>\<INSTANCE
 </pre>

Déd



If you click INSTANCE, you can see the Service parameter.

- If DPM installed on Win 2012R2, Service name will be "ibmtp2k12".
- If DPM installed on Win 2008R2 SP1, Service name will be "ibmtp2k8".
- 2. Go to the following location, and select the appropriate service. \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service_Name
- 3. Right-click and select New > DWORD (32 bit) Value. Enter the value as: AutoRun
- 4. Right-click **AutoRun** and select **Modify**. Select the Base value as Decimal and enter Zero as the value in the text box. Click **OK**.
- 5. Reboot system for the registry setting to take effect



🚮 Registr	y Editor					_ 8 ×
File Edit	View Favori	tes Help				
	ϥ	defragsvc 🔺	Name	Туре	Data	
	÷.	DfsC	ab (Default)	REG_SZ	(value not set)	
	. E-	Dhcp	AutoRun	REG_DWORD	0×00000000 (0)	
	. E-	DiagTrack	200 ErrorControl	REG_DWORD	0×00000001 (1)	
	- E-	discache	B ExclusiveAccess	REG_DWORD	0×00000000 (0)	
	- P-	Disk	88 FailoverDriver	REG_DWORD	0×00000001 (1)	
		dmvsc	ab ImagePath	REG_EXPAND_SZ	system32\DRIVERS\ibmtp2k8.sys	
		Discache	100 ReserveType	REG_DWORD	0×00000000 (0)	
		dot3svc	118 Start	REG_DWORD	0×00000003 (3)	
		DPMAC	ab SystemDrive	REG SZ	Cil	
		Dem CPU harage Can Jac	110 Type	REG DWORD	0x00000001 (1)	
		DemElter				
		Down o				
		DEMEA				
		Dom/mmHelperService				
		Domikiriter				
		DPS				
		DXGKml				
		EapHost				
	T	ebdry				
		EPS				
		elxstor				
		ErrDev				
		ESENT				
		eventlog				
		EventSystem				
		exfat				
	-	fastfat				
	÷	FCRegSvc				
		fdc				
		fdPHost				
		FDResPub				
	E .	FileInfo				
		Prietrace				
		Elther				
		Fight State				
	-	FortCache3.0.0.0				
	i i i i i i i i i i i i i i i i i i i	Es Rec				
	E E	EsDenends				
	i iii	gagp30kx				
	i iii	apsyc				
	T	HDAudBus				
		HidBatt				
		hidserv				
		HidUsb				
	÷-	hkmsvc				
	⊕	HpSAMD				
	÷	HTTP				
	÷-	hwpolicy				
		i8042prt				
	L 1	laStorV				
	1	tom Cugnus Content Database				
		ibilityuszko				
		hmtph://w				
		IBMToFt2k8				
		IBMWASZ0Service - V2.1 TIPProfile Port 16310				
Computers		ACHINE/SVSTEM/Current/Control/Set/cervicer/ibmtn2k9	1			
-comparer (H	Inter Liveral Jr					(10 ····
Start		2 🚞 🙋 🥒 巈 💣				* P 1:49 AM 12/17/2015

3.5 Setting up Microsoft DPM to use the newly created iSCSI VTL

1. Within the Microsoft DPM Administration interface, access the **Libraries** submenu item and select to **Rescan for Devices**.



File Action View Help					
Rescan Refresh Optimize Ubrarjas Ontin	Options About Help DPM Help				^
Total capacity: Select to Rescan f	for devices 3			• ۹	Search in details also (Slow)
	Name / Status	Tape Label Barcode	Offsite Ready	Data Written	Protection Group
Online Registration status: Unknowr Azure backup agent version: - Used space: - Libraries: - Total libraries: 10 Total drives: 0 Tapes ready for offsite: 0 Expired tapes: 0	Microsoft System Center 2012 82 Data Protection The resean contain checks for new libraies att state of currently attached libraies. Do you want to proceed with rescan? ID: 31101 Select the Libraries Sub-Menu	A Manager A data ached to the DFM server and refreshes the Yes No 2	Confirm the resc	an 4	
	Details:				
_					
🔮 Monitoring					
Protection					
📷 Recovery					
Reporting Management	From the Management Menu	0			

2. Once the iSCSI library has been detected by the Microsoft DPM application, then proceed to **Enable** the library for use. Right-click the newly discovered library and select to enable it.

Image: Search ist below Image: Search ist below Image: Search ist below Image: Search ist below <th>File Action View Help</th> <th></th> <th></th> <th></th>	File Action View Help			
Total capacity: 0 KB	Rescan Refresh Optimize Uibraries Option	Options Help DPM Help Help		
Status Tape Label parcode Online Registration status: Unknowr Azure backup agentversion: - Used space: - Ubbraries 10 disbled Total libraries: 1 (d isabled) Total libraries: 0 Free tapes: 0 Online 0	Total capacity: 0 KB	Search list below		Search in details also (Slo
Expired faces'	Online Registration status: Unknown Azure backup agentiversion: - Used space: - Libranies Total libraries: 1 (1 disabled) Total drives: 10 Free tape: 0 Tapes ready for offsite: 0	Name > Slatus ■ Library: Sun/StorageTek Library (Disabled) ■ Drives (In use: 0 Idle: 10) ■ Slots (Tape available: 30 Empty: 0) Micro	Acknowledge the confirmation of the rescan completion	Protection Group

3. Once the library has been enabled to use, it must now be inventoried to identify the media available for further configuration. Select and confirm to **Inventory** the newly added library.



🐯 System Center 2012 R2 DPM Administrator	r Console				_ @ ×
Elle Action View Help					
Rescan Refresh Unlock Re Liventory Libraries	ename Optimize Disable Add updat Tape	k Options Help			
Number of disks: 0 Select to Invent	ory the Virtual Tape Library			، و	🗆 Search in details also (Slow)
Total capacity: 0 KB	Name / Status	Tape Label Bar	code Offsite F	Ready Data Written	Protection Group
	🗏 📓 Library: Sun/StorageTek Library				
Online	🗷 🌳 Drives (In use: 0 Idle: 10)		Inventory Li	10 S MI	
Registration status: Unknown	🗉 🗊 Slots (Tape available: 10 Empty: (Select the Virtual Tape Li	brary 🕗 Choose the h	ne of inventory you want to perform	
Azure backup agent version: -			c. East inve	ntory	
Used space: -			Only the I	barcode of each tape is read.	
	4 Confin	m Detailed Inventory	C Detailed i Each tap	nventory e is mounted on a drive and read.	
Libraries					
Total libraries: 1				Start Cancel Help	2
Total drives: 10	From within the Libraries Manag	ement Facility			
Free tapes: 0	Details: Sup/StorageTek Library				
Tapes ready for offsite: U	Details. Guidotoragerek cloraly				-
	Status:	Enabled			
S Monitoring	Computer:	2K8R2INTVM22.interopdev.lab			
Protection	Number of drives:	10			
	Number of slots:	10			
Recovery	Number of L/E Ports:	4			
Reporting	Door:	Locked			_
	Barcode reader:	Available			
Management	Autoloader:	Available			.
🎊 🚮 🗿					* 🕞 🐑 🐌 🚯 8:34 PM

4. Once the inventory is complete, the media can now be placed into production as needed.

File Action View Help							
Rescan Refresh Optimize Libraries	Options About Help	• 1	Inventory progress	→ Eibrary: ■ Cibrary: ■ Drive ■ Slots	Sun/StorageTek Library (s (In use: O Idle: 10) (Tape available: 10 Empt	Inventory in progress) y: 0)	
E Accents	Search list below					ا 🔽 🤇	 Search in details also (Slow)
Bestevited 0	Name /	Status	Tape Label	Barcode	Offsite Ready	Data Written	Protection Group
Unprotected: 0	E Library: Sun/Stor	ageTek Library					
Upgrade available: 0	🗉 🧼 Drives (In use	: 0 ldle: 10)					
	🗉 🥩 Slots (Tape av	ailable: 10 Empty: 0)					
📼 <u>Disks</u>	Slot 1	Tape available	Free	UBWDPC001		-	
Number of disks: 0	Slot 2	Tape available	Free	UBWDPC002			
Total capacity: 0 KB	Slot 3	Tape available	Free	UBWDPC003		-	
	Slot 4	Tape available	Free	UBWDPC004		-	
	Slot 5	Tape available	Free	UBWDPC005		-	
la <u>Online</u>	Slot 6	Tape available	Free	UBWDPC006		•	
Registration status: Unknown	Slot 7	Tape available	Free	UBWDPC007		· J	
Azure backup agent version: - Used space: - Monitoring Protection Recovery Recovery Management	Details:				Inventory is Complete ready for use	and 2	

5. You should reboot the system for registry settings to take effect.



4 Performing backup and restore by using the DR Series system VTL

This section describes how to perform file-based backup and restore.

 Install/push the DPM agent on the client that contains the files to be protected. After a successful installation on the DPM agent, the client is listed under Agents > Protected. The DPM installation shows 1 protected agent and 1 library.

0			System Center 2012
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> e	elp		
Install Check Op updates Agents Options	ptions About DPM Hel	P	
E Agents	`	Search list below	
Protected: 1		Computer Name	Cluster Name
Unprotected:		Protected computers with	protection agent: (1 Computer)
Upgrade available: 0		SATYAN-W2K8R2-0	-
		Unprotected computers w	rith protection agent: (1 Computer)
📼 <u>Disks</u>		SATYAN-W2K8-02	-
Number of disks: 0 Total capacity: 0 KB			
interest and the second			
Registration status: Azure backup agent ver Used space:	Unknown sion: - -		
Libraries Total libraries: Total drives: Free tapes: Tapes ready for offsite: Expired tapes:	1 10 9 0 0		



2. Click Protection > New to open the Create New Protection Group Wizard, and then click Next.





3. Select server options, and then click **Next**.

0		Create New Protection Group	x
Ē	Select Protecti Select what kind of c	ion Group Type computers you would like to setup protection for.	
Sta	eps: Welcome Select protection group type Select group members Select data protection method Select short-term goals Choose consistency check options Summary Status	You can create two kinds of protection groups. Select one of them below Image: Servers Start this, you for backing up file servers and application servers. Before selecting this option, ensure the DPM protection agent is already installed on the target server. These computers must be online at the ine of configuring protection. You will need to select the specific resources you want to backup. Image: Clients Belot this option for backing up data from laptops and desktops. You can install the DPM protection agent recompleting the configuration on the DPM server. Image: Clients Ima	e that gent vate o Syst



4. Select the folder that needs to be protected, and click **OK** for the system state selection. Click **Next**.

0	Create New Protection Grou	qu	x
Select Group	Members. you want to protect.		
Steps: Welcome Select protection group type Select group members Select data protection method Select short-term goals Choose consistency check options Summary Status	To choose the data to protect, select the check boxes is expand the directory structure, and clear the check box If you do not see the data source you want to protect in unsupported configurations Available members Available members Berger All Volumes Berger All Volume	n the Available members of the folder. the tree below, click the Selected members C:\Users C:\Users	section. To exclude a folder, following link for a list of Computer WIN-T16N70KQII4.t Remove
	< <u>B</u> ack	Excluded file types:	0 Exclude Files./a to Go to Sys Cancel Helpidows.



5. Enter a name for the protection group, and select **Tape** for short term protection. Select the option, **I want long-term protection using tape**, and click **Next**.

]	Create New Protection Group									
r	Select Data Pr DPM can help provide	otection Method e disk, online and tape based data protection.								
	Steps: • Welcome • Select protection group type • Select group members • Select data protection method • Select short-term goals • Choose consistency check options • Summary • Status	Protection group name: FileProtection Protection method Select your protection method. Image: Ima								



6. Specify the short-term recovery goals and click Next.

3	Create New Protection Group	x
Specify Short- Specify your short-terr	Ferm Protection n recovery goals, which DPM will use to generate your protection plan.	
Steps: Velcome Select protection group type Select group members Select data protection method Specify short-term goals Specify long-term goals Select library and tape details Summary Status	Specify your protection goal on tape. Retention range: 1 • weeks Frequency of backup: Daily Backup mode: Daily Backup schedule: Specify your backup day and time. Full backup time: 11:00 PM • Full backup day: Saturday Incremental backup time: 11:00 PM • Incremental backup day: Saturday Incremental backup day: Sunday • Tuesday • Wednesday • Thursday • Friday • Saturday • Incremental backup of full backups	
	< Back Next > Cancel Help	



7. Specify the long-term protection goals. Customize these settings if required, and click **Next**.

0	Create New Protection Group
Select Long-T	erm Goals otection plan using your long-term recovery goals.
Steps: Velcome Select protection group type Select group members Select data protection method Specify short-term goals Specify long-term goals Select library and tape details Summary Statue	Specify your long-term recovery goals for tape-based protection. All long-term tape-based protection uses full backups. Recovery goals The retention range and backup frequency that you select will determine the recovery point schedule. (i) Click Customize to modify the recovery point schedule or the default tape labels. Retention range: 3 Months Frequency of backup: Weekly Recovery points: 1 recovery point every 1 week(s) for the last 4 week(s) 1 recovery point every 1 month(s) for the last 3 month(s) Restore Defaults Customize
• Jidus	Backup schedule Based on the specified backup frequency, the tape library will perform a full backup to the tapes according to the following schedule Image: Click the Modify button to choose the backup days in case of daily tape backups. Weekly: Sat 11:00 PM Monthly: Day 1 , 11:00 PM Monthly: Day 1 , 11:00 PM Keekly: Cancel



	Customize F	Recovery Goal	x
You can customize the long recovery goals, specify the increment of backup to be	g-term recovery goals for daily, w backup frequency, retention rar applied to this protection group.	eekly, monthly, or yearly backups. To customize the ige, number of backup copies, and tape label for each	
👔 To modify the tape lab	el, click the label text to select it,	, and then click the label text again to edit it.	
Recovery goal 1			
Back up every:	1 🗘 Weeks 🗸	Tape Label	
Retention range:	4 🗘 Weeks	FileProtection-LT-1Weeks-Copy0	
Number of backup copy:	1		
Recovery goal 2			
Back up every:	1 🗘 Months 🗸	Tape Label	
Retention range:	3 🗘 Months	FileProtection-LT-1Months-Copy0	
Number of backup copy:	1		
Recovery goal 3			
Back up every:	1 🗘 Years 🗸	Tape Label	
Betention range:		FileProtection-LT-1Years-Copy0	
Number of backup copy:	· ·		
Option Specify the action DPM s O Run backup for all (igr Run backup only for the second s	hould take when the backup job nore overlap of days) ne 'Recovery goal 2'	s for different recovery goals occur on the same day.	ctiva
		OK Cancel Help ^C	ndow

- 8. Under Library and Tape Detail, do the following:
 - a. Select the **Library** for primary backup and **Copy Library** for additional copy of the backup.
 - b. You can also select Check backup for data integrity.
 - c. Select **Do not compress or encrypt data** for both short-term and long-term backup,
 - d. Click Next.

Note: The DR Series system has built-in compression and encryption features; therefore, enabling these features on DPM might affect savings.

0	Create	New Protection Group
Select Library a	ind Tape Details ape and the library that you v	vould like to use for backup.
Steps: • Welcome • Select protection group type • Select group members • Select data protection method • Specify short-term goals • Select library and tape details • Summary • Status	Specify details about the I Library details Library: Drives allocated: Copy library: Check backup for d Tape options for short-te Compress data Encrypt data A valid DPM encryp Do not compress or Tape options for long-ter Compress data Encrypt data A valid DPM encryp Do not compress or	ibrary and tape that you want to use for tape backups. swsys-49-satyavtl 1 swsys-49-satyavtl swsys-49-satyavtl



9. Review the protection group summary and click **Create group**.

0	Create New Prote	ction Group	x
Summary	te the FileProtection protection group.		
Steps:	Review the settings, and then click Create	Group to create the FileProtection protection group.	
Welcome	Protection group members:		
Select protection group type	D:\Savingtest		
 Select group members 			
 Select data protection method 			
Specify short-term goals	Protection group settings:		
Specify long-term goals	Setting	Details	
 Select library and tape details 	Short-term retention range Synchronization	1 Week(s) Daily Models Sci 11 00 DM	
🕘 Summary	Short-term backup schedule	Weekty:Sat T1:00 PM Daily:11:00 PM exception:Sat	
 Status 	Long-term (tape) retention range	3 month(s)	
:	Long-term (tape) backup schedule	Weekly Weekly Sat 11:00 PM	
	Long term (tape) backup schedule	Monthlin David 11:00 PM	
	You can <u>optimize performance</u> of the performance of the performanc	is protection group now or you can do it later from the acti	ons pane
		Eack Create Group Cancel He	lp



10. Make sure that the protection group is created successfully. Click **Close**.

3	Create New Protection Group	x
- Final Status		
Steps:	Tasks	
Welcome	Task Results	
Select protection group type	Create protection group: FileProtection Success	
Select group members		
i Select data protection method		
🔹 🧶 Specify short-term goals		
Specify long-term goals		
e Select library and tape details		
Summary	() DPM does not protect reparse points found in file systems, except for deduplication reparse	points,
 Status 	which are protected. If you have selected volumes or folders in this protection group, all data protected except for the unprotected reparse points. Read <u>"Select Group Members"</u> page of DPM 2012 Help for more details on unsupported data	is a.
		Close

11. To start an offline backup, expand the protection group, and select the data entry. Click **Recovery Point** to start a full backup. Click **OK**.

0						System Cente	er 2012 R2	DPM Administ	rator Con	sole		
File A	ction View H	Help										
1	-		₽	2	<mark>ي (</mark>		•	.	i.	;	i	?
New	Recovery point	Remove	Disk	Online	Tape	Selfservice Ta recovery	ape catalog retention	Recovery point status	Check updates	Options	About DPM	Help
Protecti.		urce op	Re	sume backu	ps	Manar	ne Cra	Benorte este recoven i n	oint	lone	х	Help
	Source Health		<	Group by:	Pro		- Ch	cate recovery p	onne			
8	Critical (0)			Search lis	tbelow	Selected:		D:V				Q
O	ок <mark>(2)</mark>			Protection	Group M	Member type:		Volume				Status
<u> </u>	Warning <mark>(0)</mark>			🗆 ங 🕜 P	rotection	Create recovery	point for:	Short term	i tape protect	ion	<u> </u>	
					omputer	Recovery poin	t creation optio	ns				
▲ All Pr	otection Groups											
	FileProtection			F 60 p	rotootion	á full backup	will be created	for the protected me	mber The late	est data on th	e	
	Protection Group	01			rotection	protected con configured in	nputer will be b the protection	acked up to tape. Th group settings.	e library to be	used can be		
						Library to be u	used:	swsys-49-saty	avtl			
				Details:	D:\\$	Available free	tapes:	9				
				Statue					-			
🔁 N	Ionitorina			Latest r	ecoverv			ОК	Cancel	He	b	
3 1	lonitoning			Oldest							-	
🔥 P	rotection			Total re	COVERV D	ointe:	0					-
PR P	Recoverv			Diekall	corery p	onna.						
-9 .				DISK di	ocadon.		-				A	ctivate W
_ El p	Renarting										<u>_</u>	n to Custom

12. You can view the progress of the backup job from the Monitoring tab.



5 Restoring from tape

1. Click **Recovery** and select your protected volume. On the right, select the recovery point that you want to restore and right-click the recoverable item that you want to restore. The Restore Wizard opens.

0	System Center 2012 R2 DPM Administrator Console	x
File Action View Help		
Recover Show all Verify data Recovery Configure	Check Options updates Options Help	^
< Browse	Recovery points for: C:\	Π
Filter servers Image: Comparison of Compar	Available recovery points are indicated in bold on the calendar. Select the date from the calendar and the time from the drop down list for the recovery points that you want. Click recover in the Actions pane to op the Recovery Wizard. February • 2015 • Recovery date: February 08 2015 Recovery time: 11:00 FM • Recovery time: 11:00 FM • Sun Mon Tue Wed Thu Fri Sat 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28	ən
 Search Recovery Points 		
Files and folders Files and folders Fixehange mailboxes	Path: All Protected Volumes	P
sharePoint	Search list below P V Search in details also (Slor	N)
Monitoring Protection Recovery Reporting Management	CA Coveragie term Size CA Coveragie term Cast modified Coveragie term Cast modified Cast mo	



2. Review the recovery selection and click **Next**.

0		Recovery Wizard		x
Review Recov Review the information	ery Selection on for the items that you ch	ose to recover.		
Steps:	Review your recovery s	elections.		
Review recovery selection	Recovery point:	2/4/2015 3:52:03 AM		
Select recovery type	Recover from:	Таре		
 Specify recovery options 	Tape set for recovery:	Tape set 1 🗸 🗸	Tape set details	
 Summary 	Item details			
 Recovery status 	Recovery items:	Name	Size /	
		📼 C:\	1.13 MB	
	Total size:	1.13 MB		
	Recovery source:	C:\ on WIN-T16N70KQII4.testad.ocarina	.local	
		/ Back	A G	ctivat o to Sys
		< Back N	lext > Cancel Hel	P



3. Make the appropriate selection for the recovery type and click **Next**.

0	Recovery Wizard	x
Select Recove Select the type of rec	ry Type covery you want to perform.	
Steps: Review recovery selection Select recovery type Specify recovery options Summary Recovery status	 Recover to the original location Driginal location: C:\ on WIN-T16N70KQII4.testad.ocarina.local Recover to an alternate location Alternate location: Copy to tape This option copies the volume that contains the selected data to tape in a DPM library. Note that the volume might also contain data that was not selected for recovery. 	Browse
	< <u>B</u> ack <u>N</u> ext > Cancel	Activat Go to Sys



4. Specify the recovery options and click **Next**.

0	Recovery Wizard
Specify Recov	very Options o apply to the recovery.
Steps: Review recovery selection Select recovery type Specify recovery options Summary Recovery status	Recovery library All the tapes needed for recovery needs to be present in this library. Library name: satyan-sw-01-VTL-Test Existing version recovery behavior • Create copy Skip D verwrite Restore security • Apply security settings of the destination computer Apply security settings of the recovery point version Network bandwidth usage throttling Status: Disabled Modify SAN Recovery Enable SAN based recovery using hardware snapshots Click on Help to learn about the prerequisite steps Notification Send an e-mail when this recovery completes Recipients: Separate e-mail addresses with comma. Example: Kim@Contoso.com, Terry@Adventure-works.com Activation Separate e-mail addresses with comma.



5. Review the summary and click **Recovery**.

0	Recovery Wizard	x
Summary Review your recover	y settings.	
Steps: • Review recovery selection • Select recovery type • Specify recovery options • Summary • Recovery status	Recovery point: 2/4/2015 3:52:03 AM Recovery media: Tape set 1 Tape set details Source: C:\ on WIN-T16N70KQII4.testad.ocarina.local Destination: C:\ on WIN-T16N70KQII4.testad.ocarina.local Notification: No Recovery items Size / Details: Size / Recovery Items Size / C:\ 1.13 MB	
	Any synchronization job for the selected recovery server will be cancelled while the recovery is in progress.	tivat to Sys



6. To monitor the restore job, click **Monitor > All jobs in progress**.

0	System	n Center 20)12 R2 DPM Ad	dministrator C	onsole			x
File Action View Help								
								~
Alerts	Group by: 🔿	Protection g	roup 🔿 Comp	uter O Status	🖲 Туре			
Show inactive alerts	Search list belo	w			₽ ▾ 🗆	Search in d	details also (S	low)
✓ All Alerts	Status	Source	Computer	Protectio	Start Time 💎	Time	Data T	^
🔇 Critical (173)	🗉 🚰 Detailed	inventory (Total jobs: 311)					
\Lambda Warning (6)	🗉 🐨 Tape ver	ification (To	otal jobs: 9)					=
(J) Information (3)	🗄 🙋 Tape ba	ckup (Total	jobs: 23)					
Jobs	∃® Tape rec	:overy (Total	jobs: 18)					
✓ Default Filters	📢 İn prog	C:\	win-t16n70kqii	-	2/7/2015 9:47:22	00:00:11	0 MB	
🍸 All jobs 📃 🗏	🜏 Compl	CA	win-t16n70kqii	-	2/6/2015 5:48:00	00:00:37	0.81 MB	
🍸 All jobs in progress	😵 Failed	C:A	win-t16n70kqii	-	2/6/2015 5:41:02	00:00:40	0.44 MB	_
📅 Falled jobs for yesterd 🗸	Compl	C4	win-t16n70kaii	-	2/4/2015 3:53:54	00.00.37	0.81 MR	
	Details:							
S Monitoring								
A Protection								
🕂 Recovery								
Reporting								
							Activate	vvin
Management							GO TO Syste Windows	m in i



Setting up the DR Series system cleaner

6

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication.

The cleaner runs during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner to force it to run during a scheduled time.

If necessary, you can perform the procedure shown in the following screenshot to force the cleaner to run. After all of the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place, and generally after a backup job has completed.

l	DE DR4000 DR4000-D	KCV6S1			Help Log out
	Dashboard Alerts Events Health	Cleaner Sched	ule entral, Mon Jan 23 15:18:49 2012	Schedule Cleaner	Schedule
	Usage Statistics: Container	Day	Start Time	Stop Time	
	Statistics: Replication	Sun	-	-	
	Storage	Mon		-	
	Replication	Tue		-	
	Compression	Wed		-	
-	Schedule	Thu		-	
	Replication	Fri	-	-	
0	Cleaner	Sat	-	-	
	System Configuration Networking Active Directory Email Alerts Date & Time Support Diagnostics Software Upgrade	Note: When no schedule	e is set, the cleaner will run as needed.		



Monitoring deduplication, compression, and performance

7

After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits of the DR Series system.

Note: Deduplication ratios increase over time. It is not uncommon to see a 2-4x reduction (25-50% total savings) on the initial backup. As additional full backup jobs are completed, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio, in most cases.





A Managing VTL protocol accounts and credentials

A.1 Managing iSCSI account details

By default, the iSCSI username is the **hostname** of the DR Series system and can be confirmed by reviewing the output of the iscsi –account --user CLI command. For example:

```
>iscsi --show --user
user : dr9-interop-a7
```

The default iSCSI password is **St0r@ge!iscsi**. You can modify this password in the iSCSI tab of the **Clients** page. Click **Edit CHAP Password** and enter a new password as needed.

IMPORTANT NOTE: iSCSI CHAP passwords must be between 12 and 16 characters long

1313-03-000	rina.local 🔻	Clients	5				Update Client Ed	dit Password Edit C	HAP Password Dolete	DR2000
Global V Dashbor Alerts	ew rd	Total Num	ber of Cli	ents: 1				_	2	
Events		NFS	CIFS	RDA	NDMP	ISCSI	DR2000v			
Usage Containe Replicat	r Statistics on Statistics	Number of ISCSI Cur Containe	of Current rent Sess	t ISC SI Se ions Stati	ssions acti stics	ve: 1				3
Containe	rs .	Name	co	Edi	t CHAP Ac	count		and a second second second		
Replicat	on	Test-VII		WA WA	RNING: All	existing iS	CSI sessions will be te	irminated upon subr	nission.	
Constantio	n	1				User: dr	1-interop-a7.dsgdev.lab		"At fields	are require
Clients										

Alternatively, you can also use the *iscsi--setpassword* CLI command to change the iSCSI CHAP password as shown in the following example:

> iscsi --setpassword

A.2 VTL default account summary table

Service	Account	Default Credentials	CLI Modifier
iSCSI	iscsi_user	St0r@ge!iscsi	iscsisetpassword



B Managing VTL media and space usage

B.1 General performance guidelines for DMA configuration

- The DR Series system (version 3.2 and later) provides inline VTL deduplication, compression, and encryption at rest functionality. Backup applications (such as Dell NetVault, Symantec BackupExec, Symantec NetBackup, and so on) should be configured so that any multiplexing, pre-compression, software-side deduplication, or encryption is disabled. Enabling any of these features may adversely affect the space savings and ingest performance of the DR Series system VTL feature.
- Slots and media should be configured so as to accommodate the environment backup requirements. Initially, the logical capacity of a VTL should be no more than twice the physical size of the DR Series system. If the initial VTL setup is over-subscribed at higher than a 2-1 ratio without proper planning the DR Series system could fill up prematurely and cause unexpected system outage. It is highly advisable to configure the DR Series system VTL feature such that the media count be made to accommodate your initial data protection requirements. and then media be added as the deduplication statistics become available to ascertain growth, media, and space requirements.
- Media Type selection will depend on a number of factors including the DMA used, the backup cycles, data sources, and more. As a general rule, using smaller tapes is better than using larger tapes so as to allow for a higher level of control over space usage by backup operations. This also allows for easier handling in the event of a system running out of physical space as well as the normal data cleanup procedures.
- Adding media to an existing DR Series system VTL is painless and should be leveraged to incrementally add media as needed. Although this may require a higher level of involvement in managing the media usage, it will result in better performance and avoid unplanned outages.

B.2 VTL space sizing and planning

Various factors such as total data footprint, change rate, backup frequency and data lifecycle policies will dictate how much physical space will be needed to accommodate the Virtual Tape Libraries within a DR Series environment. In addition, if other container types are hosted these two must be factored into space requirement calculations. As a general rule the following can be used as a reference architecture to determine the basic capacity needed for a given virtual tape library container:

- 1. Determine Existing Data Set
- 2. Determine the change rate (Differential)
- 3. Determine the retention period
- 4. Calculate the data footprint during the retention period for existing data sets based on a 10-1 deduplication ratio



- 5. Calculate the data footprint during the retention period for change rate data sets based on a 10-1 deduplication ratio
- 6. Calculate the ratios within the retention period for each of the data sets
- 7. Determine the lowest ratio data set to be retired within the retention period and create media of size that closest matches this data footprint so that when a retention period is met the most amount of media is recycled to invoke data reclamation alignment and optimizing media consumption.

IMPORTANT NOTE: If other containers are being configured to host CIFS, NFS, RDA, or OST, these must also be factored into the planning and management of space.

Note: For complete details, see the Dell DR Series Capacity Sizing Guide: A Dell Technical White Paper or contact a support or sales specialist for assistance.

B.3 Logical VTL geometry and media sizing

The logical size of the VTL, including media size and media count should be made so as to accommodate the existing data footprint targeted for protection. The calculation for such should include the initial footprint, change rate and retention period. It should also take into account the size of both full and incremental data sets. Using the smallest iteration of the data sets to dictate the logical size of the VTL media affords users the ability to retire media in smaller increments which results in high levels of use. It also provides users the ability to conduct operations across smaller objects, which results in higher levels of flexibility, such as when a restore is needed during backup operations.

We can review a typical full weekly plus incremental daily example to demonstrate one method of conducting this calculation. In our example the total logical foot print for the customer environment is 20TB and with a 10% change within a weekly recovery point objective period for a complete weeks' worth of protection we calculate that we will require 22TB of total logical media to retain the data footprint for the given environment for one week. In order to allow for disparities we also include a 10% increase to allow for flexibility in the deployment and use of the VTL which results in a 24.2TB total virtual media requirement for a single weekly retention period.

IMPORTANT NOTE: Media can always be added as needed. Media cannot however be deleted; therefore, care must be taken to avoid creating too many media items.

In the previous example at the end of the 5-week cycle, the 1st week retires and frees up media to be reused or recycled which once processed will allow the DR to reclaim the physical space associated with the virtual media. Since the smallest data set footprint resulting from the change rate is 2TB in each incremental iteration, we create our media at 800GB increments and add as we grow. For this example the initial VTL would be created with **152** (*121TB divided by 800GB*) pieces of media at **800GB** for each piece media.

		Pre-Dedup	olication
Week	Logical Size	Logical Full Metrics	10% Change Rate Logical Incremental Metrics
1	24.2TB	20TB	2TB
2	24.2TB	20TB	2TB
3	24.2TB	20TB	2TB
4	24.2TB	20TB	2TB
5	24.2TB	20TB	2TB
Total	121TB		

20TB Total initial footprint with a 10% change rate

NOTE: For complete details please refer to the Dell DR Disk Backup Appliance Capacity Sizing Guide: A Dell Technical White Paper or contact a support or sales specialist for assistance.

B.4 Media retention and grouping

Due to the nature of VTLs, media must be managed to ensure that physical capacity is reclaimed in an orderly fashion to avoid running out of space and disrupting operations. Media must be grouped within the data management application, in a way that full data sets are targeted to separate media as incremental data and they in turn are grouped by data sets that expire within the same period or that share the same recovery point objective. This ensures that media can be reused effectively so that when full, all incremental data expire, the logical space can be reconciled thus enabling the physical space to be reclaimed.

B.5 VTL media count guidelines

Туре	Capacity	Max number of Tapes supported
LTO-4	800GiB	2000

B.6 Adding VTL media to a VTL container

Follow these steps.

1. To add media to an existing VTL container, select **Containers** in the left navigation area of the DR Series system user interface.



- 2. Select and edit the target VTL container.
- 3. In the field **Add More Tape (no of Tape)**, enter the number of tapes to add to the VTL container.

Global View	Containers			Create	Edit Delete Displa	ay Statistic
Dashboard Nerts	Number of Containers: 5				Container Path:	/container
ivents	Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
lealth	backup	0	Auto	NFS, CIFS	Not Configured	0
Jsage Containor Statistics	intvm05_ndmp	31	Unix Dump	VTL NDMP	Not Configured	0
Renlication Statistics	intvm05iscsi	31	Networker	VTL iSCSI	Not Configured	0
torage	intvm05iscsi2	31	Networker	VTL iSCSI	Not Configured	0
Containers	TEST VILLALA	31	None	VTL NDMP	Not Configured	
system Configuration	IS OF M				Container Name and Ty	/pe
ystem Configuration letworking Active Directory Local Workgroup Users Email Alerts	is OEM: Tape Size:	 800GB 100GB 	 400GB 50GB 	200GB	Container Name and Ty TEST_VTL_LALA VTL	/pe
letworking letworking ccal Workgroup Users Email Alerts vdmin Contact Info assword Email Relay Host	Is OEM: Tape Size: Access Protocol:	 800GB 100GB NDMP 	 400GB 50GB iSCSI 	O 200GB O 10GB No Access	Container Name and Ty TEST_VTL_LALA VTL	γpe
ystem computation letworking ocal Workgroup Users imail Alerts udmin Contact Info assword imail Relay Host ale and Time	Is OEM: Tape Size: Access Protocol: Access Control:	 800GB 100GB NDMP FQDN or IP 10.8.238.125 	 400GB 50GB iSCSI 	200GB 10GB No Access	Container Name and Ty TEST_VTL_LALA VTL	уре
Vystem comguration letworking ocal Workgroup Users mail Alerts Mrmin Contact Info assword Email Relay Host ate and Time upport Nagnostics	Is OEM: Tape Size: Access Protocol: Access Control: Add More Tape (no. of tape):	800GB 100GB NDMP FODN or IP 10.8.238.125	 400GB 50GB iSCSI 	200GB 10GB No Access	Container Name and Ty TEST_VTL_LALA VTL	/pe
ystem computation letworking cal Workgroup Users smail Alerts drain Contact Info 'assword mail Relay Host bate and Time isupport liagnostics offware Upgrade inense	Is OEM: Tape Size: Access Protocol: Access Control: Add More Tape (no. of tape): Marker Type:	 800GB 100GB NDMP FQDN or IP 10.8.238.125 Unix Dump 	○ 400GB ○ 50GB ○ ISCSI	200GB 10GB No Access	Container Name and Ty TEST_VTL_LALA VTL	/pe

Alternatively, you can also use the "vtl -create_carts" CLI command for this operation:

> vtl --create_carts --name TEST_VTL_LALA --tapes 10

Created 10 cartridges

4. After the VTL media has been added to the target VTL container, Microsoft DPM must now be updated to be able to use said media. Select the VTL and conduct an inventory update.

Reaction View Holp		i 🔤 d	1	2)			
rwentory Rescan Refresh Unlock door Libraries	Rename Optimize Disabl usage	le Add Ch upd Tape	ates Options About F DPM Options Help	felp			
Number of disks: 0 Select to Inv	entory the Virtual Tape L	ibrary 0					E Search in details also (Slov
Total capacity: 0 KB	Name /	Status	Tape Label	Barcode	Offsite Ready	Data Written	Protection Group
	E Library: Sun/Stor	rageTek Library					
Online	B Drives (In use:	: 0 ldle: 10)			Inventory Library		R
Begistration status: Unknown	B Slots (Tape av	vailable: 10 Empty	c 0) Select the Virtual	Tape Library	Choose the type of inventory	a sous superit to merinem	
Azure backup agent version: -					 Fast inventory 	y you mak to percent.	
					Only the barcode of eac	ch tape is read.	
Used space: -							
Used space: -		() Cont	firm Detailed Inventory	I	Detailed inventory Each tane is mounted o	n a dive and read	
Used space: -		(d) Cont	firm Detailed Inventory)	Detailed inventory Each tape is mounted or	in a drive and read.	
Used space: - Librarios Total libraries: 1		4 Con	firm Detailed Inventory)	Detailed inventory Each tape is mounted o	n a drive and read.	6
Used space: - Librories: - Total libraries: 1 Total drives: 10	From within th	Cont Cont	firm Detailed Inventory)	C Detailed inventory Each tape is mounted o	in a drive and read.	•
Used space: - Libronies Libronies: 1 Total libranies: 10 Free tapes: 0	From within th	Cont De Libraries Mana	firm Detailed Inventory agement Facility)	Cetalied inventory Each tape is mounted o	in a drive and read. Start Cancel Hel	
Used space: -	From within th Details: Sun/Sto	Cont ne Libraries Mana prageTek Library	firm Detailed Inventory)	Detailed inventory Each tape is mounted o	in a drive and read.	
Used space: - Libronies Total libronies: 1 Total drives: 10 Free tapes: 0 Expired tapes: 0	From within th Details: Sur/Stor Status:	(3) Cont ne Libraries Mana prageTek Library	firm Detailed Inventory]	C Detailed inventory Each tape is mounted o	n a drive and read. Start Cancel Hel	•
Used space: - Libronics Total libraries: 1 Total drives: 10 Free tape: 0 Tapes ready for offile: 0 Expired tapes: 0 Monitoring	From within th Details: Sun/Sto Status: Computer:	(3) Cont ne Libraries Mana prageTek Library	firm Detailed Inventory agement Facility Enabled 2K8R2INTVM22.interopdev.) ab	C Detailed inventory Each tape is mounted o	in a drive and read.	•
Used space: - Libranes: - Total libraries: 1 Total drives: 10 Free tapes: 0 Topes ready for offsite: 0 Expired tapes: 0 Monitoring Double drives: -	From within th Details: Sun/Stor Status: Computer: Number of drives:	Con ne Libraries Mana rrageTek Library	firm Detailed Inventory agement Facility Enabled 2K0R2INTVM22.interopdey: 10) lab	C Detailed inventory Each tape is mounted o	in a drive and read.	
Used space: - Libraries: 1 Total iloraries: 1 Total iloraries: 0 Tapes ready for offsite: 0 Expired tapes: 0 Monitoring Profection	From within th Details: Sun/Sto Status: Computer: Number of drives: Number of stats:	Cont ne Libraries Mana prageTek Library	firm Detailed Inventory agement Facility Enabled 2K8R2INTVM22.interopdev: 10) Iab	C Datalied inventor Each tage is mounted o	n a dive and read. <u>Start</u> Cancel Heb	•
Used space: - Libraries: - Total libraries: 10 Free tapes: 0 Total offer offline: 0 Expired tapes: 0 Monitoring Protection Racovery	From within th Details: Sun/Sto Status: Computer: Number of drives: Number of allots: Number of UE Ports:	Con ne Libraries Mana orageTek Library	firm Detailed Inventory agement Facility	ab	C Datalied inventory Each tage is mounted o	n a dive and read	•
Used space: -	From within th Details: SundSto Status: Computer: Number of drives: Number of slots: Number of JUE Ports: Door:	Con ne Libraries Mana rrageTek Library	firm Detailed Inventory agement Facility Enabled 2K0R2INTVM22 interopdev: 10 10 4 Locked	J	C Detailed inventor Each tige is monthed o	n a dive and read. <u>Start Cancel Hel</u>	
Uted space: -	From within th Details: Sun/Ston Status: Computer: Number of drives: Number of slots: Number of slots: Door: Barcode reader:	Con ne Libraries Mana prageTek Library	firm Detailed Inventory agement Facility Enabled 2K0R2INTVM22.interopdee: 10 10 4 Locked Available] lab	C Datalied inventor Each tige is morried o	n a dive and read. <u>Start</u> Cancel Hel	

B.7 Space reclamation

B.7.1 General guidelines

The DR Series system VTL feature is presented to operating systems and data management applications (DMAs) alike as devices either through iSCSI or NDMP protocol connectivity. The DMA interfaces with the virtual tape library and all its underlying components, including the drives and media though these specific protocols.

The DMA must interact with the virtual tape media during a recycle, reuse or media initialization process in order for the DR to be able to reclaim space during its own cleaning cycle.

This two-step process is required so that the backup software can reconcile the space by marking the media as expired then reusing it, consolidating space across volumes/tapes or by simply recycling the media into a scratch pool. Once these operations have been completed the DR Series system's own cleaning cycle should be used to reclaim that virtual tape media space which in turn will free up physical space on the DR Series system.

Implementing proper media pool, groups and recycling practices will allow the virtual tape media to be used at optimal levels and that the underlying physical space be reclaimed accordingly by the scheduled DR reclamation.

Note: In general the guidelines provided above should be sufficient for normal operations to insure proper reclamation of space is conducted preemptively. Refer to your individual DMA applications for best practices and guidelines regarding tape reuse.

B.7.2 Product specific guidelines

In the event that space becomes an issue or that a user impact requires manual cleaning, media can either be manually Erased, Blanked, and Scratched or otherwise recycled and a manual cleaning cycle initiated on the DR Series system.

