

Setting Up the DellTM DR Series System as an RDA or VTL Backup Target for DellTM NetVault Backup

Dell Engineering June 2015

Revisions

Date	Description
January 2014	Initial release
May 2014	Updated to add suggested block size on NVBU device configuration
April 2015	Added VTL content for v3.2 Release
June 2015	Added content for configuring an iSCSI target on Linux

This document 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.

© 2015 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: http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector 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

Еx	ecutive summary	5
1	Installing and configuring the DR Series system for use with NetVault Backup	6
	1.1 NetVault software prerequisites	6
	1.2 Installing and configuring the DR Series system	6
2	Creating and configuring the RDA target container(s) for NetVault Backup	
	2.1 Adding the RDA target container(s) for NetVault Backup	11
	2.2 Configuring transport modes for NetVault Backup	
	2.2.1 Setting the mode using the CLI	
	2.2.2 Setting the mode using the GUI	
	2.3 Configuring a backup job for NetVault Backup	
3	Configuring VTL	
	3.1 Creating and configuring iSCSI target container(s) for NetVault Backup	
	3.1.1 Creating an iSCSI VTL container for NetVault Backup	
	3.1.2 Configuring the iSCSI target – Windows	
	3.1.3 Configuring the iSCSI target – Linux	22
	3.1.4 Configuring NetVault Backup to use the newly created iSCSI VTL	23
	3.2 Creating and configuring NDMP target container(s) for NetVault Backup	25
	3.2.1 Creating the NDMP VTL container for NetVault Backup	25
	3.2.2 Configuring NetVault Backup to use the newly created NDMP VTL	27
4	Setting up the DR Series system cleaner	
5	Monitoring deduplication, compression, and performance	
А	VTL configuration guidelines	
	A.1 Managing VTL protocol accounts and credentials	
	A.1.1 iSCSI account details and management	
	A.1.2 NDMP account details and management	
	A.1.3 VTL Default Account Summary Table:	
	A.2 Managing VTL media and space use	
	A.2.1 General performance guidelines for DMA configuration	
	A.2.2 Physical DR space sizing and planning	
	A.2.3 Logical VTL geometry and media sizing	
	A.2.4 Media retention and grouping	
	A.2.5 VTL media count guidelines	
	A.2.6 Adding media to the VTL container	
	A.2.7 Updating NetVault Backup to identify newly added VTL media	
	A.2.8 Space reclamation guidelines	



Executive summary

This white paper provides information about how to set up the Dell DR Series system as a backup target for Dell NetVault Backup. 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://www.dell.com/powervaultmanuals

NOTE: The DR Series system and NetVault build versions and screenshots used for this paper may vary slightly, depending on the version of the DR Series system and NetVault software version used.

IMPORTANT: About VTL Replication Support: It is important to note that VTL-to-VTL replication is not currently supported. If you require replication of your VTL backup data, you should use the NetVault "nVTL" approach.

1 Installing and configuring the DR Series system for use with NetVault Backup

1.1 NetVault software prerequisites

The instructions in this document apply to NetVault Backup version 9.2 and later. The screenshots used in this document may vary slightly, depending on the version NetVault Backup software version used.

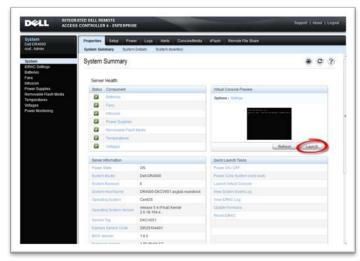
The NetVault Backup and NetVault Backup Supported VTLs, Libraries, Tape and Optical Drives compatibly guides should be referenced to determine the latest version requirements for RDA and VTL use.

http://documents.software.dell.com/NetVault%20Backup/10.0.1/Compatibility%20Guide

For NetVault Backup version 9.2, 10.0.0, and 10.0.1, there are patch requirements to add support for NDMP VTL. Refer to the NetVault Backup Compatibility Guide or contact support for details.

1.2 Installing and configuring the DR Series system

- Rack and cable the DR Series system, and power it on. In the *Dell DR Series System Administrator Guide*, refer to the sections "iDRAC Connection", "Logging in and Initializing the DR Series System", and "Accessing IDRAC6/Idrac7 Using RACADM" for information about using the iDRAC connection and initializing the system.
- 2. Log on to iDRAC using the default address 192.168.0.120, or the IP address that is assigned to the iDRAC interface. Use the user name and password: "root/calvin".



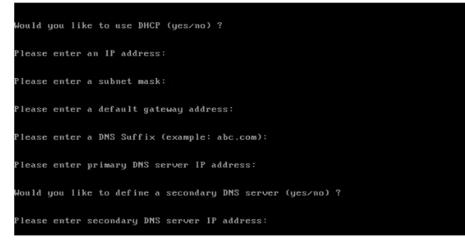
3. Launch the virtual console.

System	Properties Selup	Power Logs Alets ConsoleMedia	witash Renote File Share	
Dell DR 4000 root , Admin		stem Details System inventory		
System	System Summary	1		a c ?
IDRAC Settings Exitinities				
Fans Intrusion	Server Health			
Power Supplies	Blatus Component		Virtual Consule Preview	
Removable Flash Vedia Temperatures	Daterrer .		Ophone 1 Semipe	
Voltages	Di Fara			
Power Monitoring	B interes		a local provide the	
	2 Protections	and the second se		
	Carrowalda 1	Foulin Bierdia		
	Tampetature			
	Voltages			Baltash. Lauren.
	Server Information		Quick Launch Taxita	
	Pener State	CH4	Peak Diricht	
	System Model	Dell DR4000	Planet Code System (celd boot)	
	Salara Revision	1 C	Lauren Vetual Carante	
	Epsiette Martin Martin	DR4005-DKCV951 asglab mundrock	Voter Ballers Court Log	
	Operating System	CentOS	Vew IORACLES	
	Operating Bystern Ver	release 5.4 (Final) Kemet	Update Fernance	
	terrina tap	DKCv801	Aeset IDAAC	
	Kanana Satura Cali	29529104401		

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



5. Set the user-defined networking preferences.



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

Set Static IP Address IP Address : 10.10.86.108 Metwork Mask : 255.255.255.128 Default Gateway : 10.10.86.126 DNS Suffix : idmdemo.local Primary DNS Server : 10.10.86.101 Secondary DNS Server : 143.166.216.237 Host Name : DR4008-5		
Network Mask : 255.255.255.128 Default Gateway : 10.10.86.126 DNS Suffix : idmdemo.local Primary DNS Server : 10.10.86.101 Secondary DNS Server : 143.166.216.237 Host Name : DR4000-5	Set Static IP A	ddress
Default Gateway : 10.10.86.126 DNS Suffix : idmdemo.local Primary DNS Server : 10.10.86.101 Secondary DNS Server : 143.166.216.237 Host Name : DR4000-5	IP Address	: 10.10.86.108
DNS Suffix : idmdemo.local Primary DNS Server : 10.10.06.101 Secondary DNS Server : 143.166.216.237 Host Name : DR4000-5	Network Mask	: 255.255.255.128
Primary DNS Server : 10.10.86.101 Secondary DNS Server : 143.166.216.237 Host Name : DR4000-5	Default Gateway	: 10.10.86.126
Secondary DNS Server : 143.166.216.237 Host Name : DR4000-5	DNS Suffi×	: idmdemo.local
Host Name : DR4090-5	Primary DNS Server	: 10.10.86.101
	Secondary DNS Server	: 143.166.216.237
Are the above settings correct (yes/no) ? _	Host Name	: DR4000-5
	Are the above settings correct	(yes/no) ? _

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

Login		Reset Password
	Please enter your password	
	Username: administrator	
	Password, Storigge!	
	Log in	

8. 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 GUI

inz-sw-01.ocarina.local + Global View	Dashboard				
Dashboard Alerts Events	System State: opti	mal W State: optimal	Number of A	lerts: 0 Number of E	vents: 705
Health Usage	Capacity	Storage Saving	5	Throughput	
Statistics: Container Statistics: Replication Storage Containers Replication Compression Level Clients Schedules	Physical 13%	Zoom: 1h 15 Savings (%) 100 75 50 25	50 1m 1x ** Refreshing	Zoom: 1h 1d 5d 1 MB/s 1.00 0.75 0.50 0.25	© vi m
Replication Schedule Cleaner Schedule System Configuration Active Directory Local Workgroup Users	Used (21 29 6	HB)	0 0:40 0:50 1:00 1:10 fime (minutes) fotal Savings	0.00 0.20 0.30 0.40 Time () Re Wri	minutes) ad
Email Alerts	System Information				
Admin Contact Info Password Email Relay Host Date and Time Support Diagnostics Software Upgrade	Product Name: System Name: Software Version: Current Date/Time: Current Time Zone: Cleaner Status:	DR4100 edwinz-sw-01 99.0.0517.0 Thu Sep 26 01:12:47 2013 US/Pacific Idle	Number of Con	f Files in All Containers: tainers: tainers Replicated:	- 55.06 % - 1 ? - 2 - 0 - 47 GIB ?

b. Enter your Active Directory credentials.

edwinz-sw-01 ocarina.local -	Active Directory		Join
Global View	rioure birectory		
Dashboard Alerts	Settings		
Events			
Health	The Active Directory settings have not been configu	red. Click on the Join link to configure them.	
Statistics: Container	Active Directory Configuration		
Statistics: Replication		* = fields are required.	
Containers	Domain Name (FQDN)*:		
Replication	Username*:		
Compression Level	Password*:		
Clients Schedules	Org Unit		
Replication Schedule	org one		
		Cancel Join Domain	
System Configuration			
Networking Active Directory			
Local Workgroup Users			
Admin Contact Info			
Password Email Relay Host			
- Date and Time			
Support			
Diagnostics			
Software Upgrade			

2 Creating and configuring the RDA target container(s) for NetVault Backup

1. Create the RDS container in the Dell DR Series system by selecting **Containers** in the left navigation area, and then clicking **Create** at the top of the page.

	Dashboard Alerts Events		Containers				Create	Edit Delete Dis	
	-Events -Health		Number of Containers: 12					Container Pa	th: /containe
	-Usage -Statistics: Conta	ainar	Containers	Files	NFS	CIFS	RDA	Replication	Select
	Statistics: Conta Statistics: Replic		backup	0	~	~		Not Configured	0
_	Storage Containers	Create New	Container:						
	Schedules		ame°: *: ⊂ None				, - and _ oharacter	¥.	
	Schedules Replication Sch Cleaner Schedu System Configu	Marker Type Connection		O Networker O TSM O #			Cancel		Container
	Replication Sch Cleaner Schedu System Configu Networking	Marker Type Connection	*: O None Auto O CommVault	O Networker O TSM O #					Container C
	Replication Sch Cleaner Schedu System Configu Networking Active Directory	Marker Type Connection	*: ○ None ● Auto ○ CommVault Type*: ● None ○ NFS/CIFS ○ R	C Networker C TSM C ∌ DA ?			Cancel	Create a New (
	Replication Sch Cleaner Schedu System Configu Networking	Marker Type Connection	*: C None © Auto C CommVault Type*: © None C NFS/CIFS C R R310-Perf-06_src	C Networker C TSM C # DA ? 2			Cancel	Create a New O	O
	Replication Sch Cleaner Schedu System Configu Networking Active Directory Local Workgrou	Marker Type Connection p Users	*: C None © Auto C CommVault Type*: © None C NFS/CIFS C R R310-Perf-06_src R310-Perf-07_src	C Networker C TSM C # DA ? 2 2			Cancel RDS RDS	Create a New O	0

2. Enter a Container Name, select the Connection Type as **RDA**, and then select the RDA type as **RDS**.

_		Create New Container:	
-	Dashboard	" = required fields	
	Alerts	Choose the type of container to create ((NFS and/or CIFS) or RDA) and add clients that need access.	
	- Events	Container Name [*] : RDS Max 32 characters and only letters, numbers, - and _ characters.	
	Health	Marker Type": @ None @ Auto @ CommVauit @ Networker @ TSM @ ARCserve @ HPDP ?	1
	Usage		
	Statistics: Cont		
	Statistics: Repl		
	Storage Containers	RDA type°. C OST®RDS ⑦ Capacith°:	
	Replication	Outpacity . Outpacity . Outpacity .	
	-Compression I		
	Clients		
	Schedules		
	Replication Scl		
	Cleaner Sched		
-	System Config		
	Networking		
	Active Directory		
	- Local Workgro		
	-Email Alerts		
	-Admin Contact		
	Password		
	-Email Relay Ho		
	Date and Time		
	-Support -Diagnostics		
	-Software Upgra		
	License		
	21001100		-



3. Click Create a New Container. Confirm that the container is added.

Dashboard Alerts Events	Containers				Creat	e Edit Delete Dis	
Health	Message						
Usage Statistics: Container Statistics: Replication	Successfully added Container 'RDS' has	container "RDS". the following marker(s)	None.				
- Storage Containers	Number of Containers: 13					Container Pa	th: /containers
Replication	Containers	Files	NFS	CIFS	RDA	Replication	Select
-Compression Level	backup	0	~	~		Not Configured	0
Clients	new	11			RDS	N/A	0
Schedules Replication Schedule	new2	11			RDS	N/A	C
Cleaner Schedule	R310-Perf-01_src	2			RDS	N/A	0
System Configuration	R310-Perf-02 src	2			RDS	N/A	0
Networking	R310-Perf-03 src	2			RDS	N/A	C
Active Directory	R310-Perf-04 src	2			RDS	N/A	0
– Local Workgroup Users – Email Alerts	R310-Perf-05 src	2			RDS	N/A	0
Admin Contact Info	-						
Password	R310-Perf-06_src	2			RDS	N/A	0
-Email Relay Host	R310-Perf-07_src	2			RDS	N/A	0
Date and Time	R310-Perf-08_src	2			RDS	N/A	0
Support	rda1	174			RDS	N/A	0
- Diagnostics - Software Upgrade	RDS	0			RDS	N/A	0

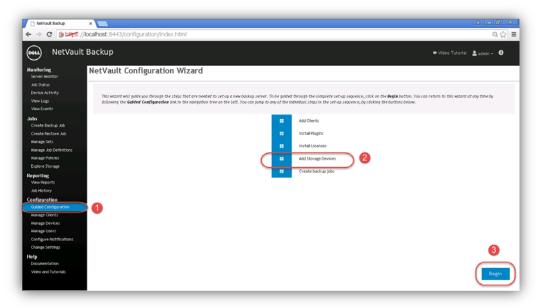
2.1 Adding the RDA target container(s) for NetVault Backup

•••• NetVault Backup							■ Video Tuto	rist 🙎 admin = 🛛 🛛
onitaring General Konflar Ald Stebul Device Activity View Logs	Client St 2 / 2	atus		Storage Devie 11 / 11			Total Data Stor 5.11 GiB	ed
Venue Exercici: 100.00 Ibb 00.00 Create for Extractory, XID 00.00 Manage Arcticity 70.00 Manage Arcticity 70.00 Manage Arcticity 40.00 Copies of Extractory 40.00 Dependence 40.00 Dependence 40.00 Venue Reports 20.00 Venue Reports 20.00								
onfiguration 0.00-	Tue 14	ma ¹ co	OS AM	09 AM	12 PM	03 PM	D6 PM	09 PM
Hanage Devices Hanage Users	nin © thr © Bhrs CurrentAct			Policies:			Ó Errors Only Ó Ke	y Events 🔹 Al Events
Configure Notifications Oninge Settings Owerting			Healthy Wiamings					

1. Open the NetVault Backup web console.



2. Add the RDA container to NetVault Backup by selecting and starting the wizard, **Guided Configuration** > Add Storage Devices.



3. In the Storage Configuration Wizard – Add Storage Devices page, select Add Dell RDA Devices.

🕐 NetYault Backup		A - 8 X
← → C (Botho	ps://localhost:8443/configuration/devices/	Q 🏠 🔳
NetVau	ault Backup	🛔 edmin + 🛛 🛈
Monitoring Server Monitor	NetVault Storage Configuration Wizard - Add Storage Devices	
Job Status Device Activity View Logs View Events	Select the type of denke that you wask to and from the set below. If you select one of the Wrhold denke types you must also specify whether you want to create a new wirbuil denke or whet Bas been created but has been removed from Netword Backup.	ter you want to re-add one that
Jobs Create Backup Job Create Restore Job Manage Sets Manage Alto Definitions Manage Policies	Single virtual disk device Virtual tage library / molia changer Shareb virtual tage library Single physical tage divice Tage library / molia changer Antical changer	
Explore Storage Reporting View Reports	* ASI DEI TICA Device 2	
Job History Configuration Guided Configuration Manage Clients Manage Devices Manage Users	Pe-add previously generated virtual device	
Configure Notifications Charge Settings Help Documentation Video and Tutorials		(Next





4. Enter the DR Series system hostname, username, and password to add the RDA device. Enter the RDA container name and save.

Note: The default username is backup_user and the password is St0r@ge! (The "0" in the password is the numeral zero). The suggested Block Size is 524288 bytes (512KB) to achieve optimal performance. Also, specify the Stream Limit required.

You now need to specify the details below to allow the Dell RDA storage device t	o be added to the NetVault Backup Server.	
If the formed desire is strengt, whiled is smaller backup it for the former with the		
If the target device is already added to another NetNault Backup Server with the where the NetNault Backup Server has been last and rebuilt.	same name, select the rorce way option to pirce the device to a	e abard to the carrency selected server. This can be asept in solution
Network name / 1P address:		
Uperturbe:	-	
(Production)		
Patsword		
Password: LSUP		
	512	

5. Confirm the RDA device is created by navigating to **Manage Devices**.

🗅 NetVault Backup 🛛 🛪		6 - Ø 3
← → C (sback://loc	alhost.8443/devicemanagement.html	Q 🕁 :
NetVault B	ackup	🖝 Video Tutorial 🚊 admin 🖌 🛈
Monitoring Nonitor	lanage Devices	
Job Status Device Activity	* Tape Library: AUTOINT8: Device DRv32:L700-5R0EAW_00 (STK L700) Drives: 10 Slots: 10 (Online)	c • • \$
View Logs View Events	RAS: Dell DR (autoint&rde) + 10.8.230.100 (Idle)	•• •
Jobs Create Backup Job Create Restore Job Manage Sets Manage Job Ceffiltions Manage Policies Explore Storage	2	
Reporting View Reports		
Job History Configuration Guided Configuration Manage Clients		
Manage Devices Manage Users Configure Notifications Change Settings		
lelp Documentation Video and Tutorials		🕈 Add Davice



2.2 Configuring transport modes for NetVault Backup

There are two transport modes for backing up data over RDA: Optimized / Dedup and Passthrough. Optimized backup does source side dedupe on the NVBU clients. The Passthrough mode does target side dedupe on the DR Series system.

The default mode for each client is decided based on the number of CPU cores in the client machine and whether the architecture is 32-bit or 64-bit. In general, there is no need to change the mode. In the event you want to change the mode, it can be done by setting the RDA mode in the DR Series system command prompt or through the GUI.

2.2.1 Setting the mode using the CLI

Open an ssh session to the DR Series system and run the following command:

rda --update_client --name <hostname of client> --mode <dedupe/passthrough>

[root@SWSYS-235 ~]# rdaupdate_c Rapid Data Access (RDA) client R31 [root@SWSYS-235 ~]# rdashowc	.0-SYS-86 wit						
RDA Client(s)	Type	Plugin	OS	Backup Software	Last Access	Connection(s)	Node
R310-Perf-01	RDS	2.1.0241	Linux 2.6.18-274.e15	NetVault 9.2 Build 16		0	Dedupe
R310-Perf-02	RDS	2.1.0241	Linux 2.6.18-274.e15	NetVault 9.2 Build 16		0	Dedupe
R310-Perf-03	RDS	2.1.0241	Linux 2.6.18-274.el5	NetVault 9.2 Build 16		0	Dedupe
R310-SYS-86	RDS					0	Passthrough

2.2.2 Setting the mode using the GUI

In the DR Series system GUI, follow the steps:

- 1. Navigate to the Clients page, and select the **RDA** tab. The list of clients that have active connections is shown.
- 2. Select the client for which you want to change the mode.
- 3. On the top right side of the page, click the **Update Client** link.
- 4. Select the required mode from the drop down menu, and click **Submit**.

Dashboard Alerts	Clients				Update	Client Edit Pas	sword Dow	nload Plu
Events Health	Total Number of Clients: 5	1						
Usage Statistics: Container Statistics: Replication	NES CIES RE	A						
Storage	Number of RDA Clients:	9						
Containers Replication	Name	Туре	Plug-In	Backup Software	Idle Time	Connection	Mode	Select
Compression Level Clients	R310-Perf-01	RDS	2.1:0241	NetVault 9.2 Build 16	-	0	Dedupe	0
Schedules	R310-Perf-02	RDS	2.1.0241	NetVault 9.2 Build	(147) (147)	0	Dedupe	c
Replication Schedule Cleaner Schedule	Update Client: R310-Perf-01 Type: RDS							
System Configuration		Client Mode:	ledupe					С
Networking Active Directory	r310-pen					Cancel	Submit	0
-Local Workgroup Users -Email Alerts	R310 Perf 05	RDS	2.1.0243	NetVault 9.2 Build 16	-	0	Dedupe	Ç
	R310-Perf-06	RDG	2.1.241	NetVault 9.2 Build 16		0	Dedupe	C
Email Relay Host Date and Time	R310-Perl-07	RDS	2.1.241	NetVault 9.2 Build 16	Aug 28 00:20:52	1	Dedupe	c
Support Diagnostics	R310-Perf-08	RDS	21.241	NetWault 9.2 Build 16		0	Dedupe	с
Software Upgrade License	R310-Perf-09	RDS		-	177.12	0	Dedupe	C



NOTE: Except for the NetVault Backup file system plug-in, all the other plug-ins are 32- bit binaries on Windows (64-bit or 32-bit versions). There is a known issue because of which optimized back-ups with 32 bit plug-ins provide less performance than passthrough back-ups. It is recommended to keep the default that the DR Series system chooses to use rather than forcing the mode to be optimized even if the client has more power. A NetVault Backup client running on a 64-bit Linux machine has 64-bit plugins.

2.3 Configuring a backup job for NetVault Backup

Refer to the following resources for information.

• Creating a backup job for NetVault 9.2:

http://documents.software.dell.com/doc107040

• Creating a backup job for NetVault 10:

http://documents.software.dell.com/DOC229690

3 Configuring VTL

3.1 Creating and configuring iSCSI target container(s) for NetVault Backup

3.1.1 Creating an iSCSI VTL container for NetVault Backup

- 1. Create and export the iSCSI container.
 - a. Select **Containers** in the left navigation area, and then click **Create** at the top of the page.

r9-interop-a7.ocarina.local View	Containers			2 Create	Edit Delete Displ	
Dashboard Alerts	Number of Containers: 2				Container Path	/containe
Events	Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
Health	backup	0	Auto	NFS, CIFS	Not Configured	0
Usage Container Statistics	intvm05iscsi	31	Networker	VTL iSCSI	Not Configured	0
Replication Statistics Storage Containers Replication Encryption Clients Schedules System Configuration Support	•					

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

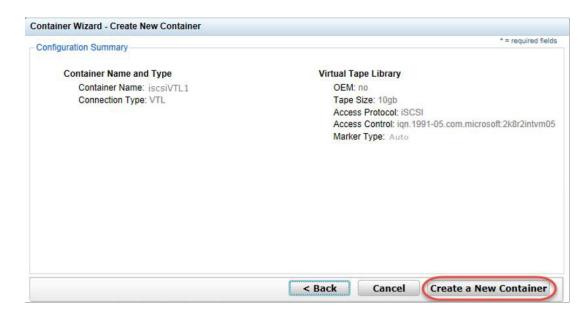
ontainer Name		* = required field
	Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter.	
Container Name*:		
tual Tape Library (VTL) :		
tual Tape Library (VTL).		



3. Select the **iSCSI** Access Protocol. Specify the DMA Access Control by providing the storage node / media node IP Address, IQN or FQDN. For NetVault, you must also specific **Auto** as the Marker Type. Click **Next**.

Configure Virtual Tape Library —		* = required field
Is OEM:		Container Name and Type iscsiVTL1 VTL
Tape Size:	○ 800GB ○ 400GB ○ 200GB	VIL
	○ 100GB ○ 50GB 10GB	
Access Protocol:	O NDMP O ISCSI No Access	
Access Control (initiator):	IQN, FQDN or IP	2
Marker Type:	O Unix Dump O Networker O BridgeHead	
	None Auto Time Navigator	
	< Back	Cancel Next >

4. Finalize VTL creation by clicking **Create a New Container**.



3.1.2 Configuring the iSCSI target – Windows

1. Configure the iSCSI Initiator Software for Windows by providing the IP or FQDN of the DR Series system in the Quick Connect, **Target** field. Click **Quick Connection** to open the Quick Connect dialog box, which indicates a connection was made but is set as inactive.

iSCSI Initiator Properties	×
Targets Discovery Favorite Targets Volumes and Devices Quick Connect To discover and log on to a target using a basic connection, typ DNS name of the target and then click Quick Connect. Target: I Discovered targets	
	Quick Connect 🛛 🗙
Name 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. For configuration of devices associated with a target, select the target and then click Devices. More about basic ISCSI connections and targets	Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually. Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts. Discovered targets Name Status Ign.1984-05.com.dell:dr4000.9lbp8r1.intvm05lscsi.10 Inactive Progress report Unable to Login to the target.
	Connect Done



2. 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 Initiator Properties	×
	Targets Discovery Favorite Targets Volumes and Devices Quick Connect To discover and log on to a target using a basic connection, t DNS name of the target and then click Quick Connect.	
	Target:	Quick Connect,
	Discovered targets	Refresh
	Name ign.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Status Inactive
		2
	To connect using advanced options, select a target and then	
Connect To Target	×	Disconnect
Target name:	ll:dr4000.9lbp8r1.intvm05iscsi.10	Properties
Add this connecti This will make the	on to the list of Favorite Targets. system automatically attempt to restore the time this computer restarts.	Devices
C Enable multi-pa	OK Cancel	
		/
	ОК	Cancel Apply



3. In Advanced Settings, select to **Enable CHAP log on** and enter the User Name and Target Secret / Password. Select **OK**. Refer to Appendix A for further details about accounts and credentials.

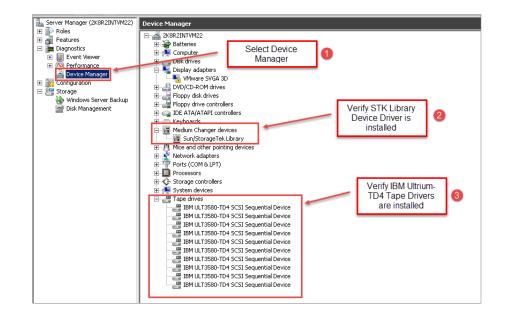
dvanced Settings		? ×
General IPsec		
Connect using		
Local adapter:	Default	•
Initiator <u>I</u> P:	Default	_
<u>T</u> arget portal IP	Default	•
CRC / Checksun		
🔲 Data digest	🔲 Header digest	
Enable CHAP		
CHAP helps ensu an initiator.	e connection security by providing authentication between a	target and
	e same name and CHAP secret that was configured on the ta e will default to the Initiator Name of the system unless anot	
Name:	dr9-interop-a7	
Target <u>s</u> ecret:	, ••••••••••	— J
	al authentication AP, either specify an initiator secret on the Configuration pag	ge or use
Use RADIUS	o generate user authentication credentials	
Use <u>R</u> ADIUS	o authenticate target credentials	
	OK Can	cel <u>A</u> pply

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

	, ind log on to a target using a basic connection, the target and then click Quick Connect.	type th	ne IP addres	s or
DINS Name or	the target and then tlick Quick Connect.			
Target:			Quick Cor	nnect,.,
Discovered ta	irgets			
			Refr	esh
Name		Statu	JS	
iqn.1984-05	.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Conr	nected	
	sing advanced options, select a target and the	n	Conn	nect
click Connect To completely	, v disconnect a target, select the target and	n	Conn	
click Connect To completely	, v disconnect a target, select the target and	n		
click Connect To completely then click Dis For target pr	, v disconnect a target, select the target and	n		nnect
click Connect To completely then click Dis For target pr select the tar For configura	, y disconnect a target, select the target and connect. operties, including configuration of sessions,		Discor	nnect

4. Open the Server Manager Snap-in and verify that the newly connected devices show up in the Device Manager. Verify that the STK Library and IBM Ultrium-TD4 Device Drivers are installed.

Note: Refer to the article at <u>http://catalog.update.microsoft.com/v7/site/home.aspx</u> for information about acquiring Microsoft Device Drivers, e.g., StorageTek Library Drivers.



3.1.3 Configuring the iSCSI target – Linux

Before you begin this procedure, ensure that the iSCSI initiator is installed (iscsi-initiator-utils). For example:

yum install iscsi-initiator-utils ; /etc/init.d/iscsi start

To configure the iSCSI target for Linux, follow these steps.

Add the CHAP Authentication details for the DR Series system on the Linux Initiator as follows:
 a. Edit /etc/iscsi/iscsid.conf and un-comment the following line:

node.session.auth.authmethod = CHAP

b. Modify the following lines:

To set a CHAP username and password for initiator # authentication by the target(s), uncomment the following lines: node.session.auth.username = iscsi_user node.session.auth.password = St0r@ge!iscsi

2. Set the Discovery Target Node(s) by using this command:

iscsiadm -m discovery -t st -p <IP or IQN of DR>

For example:

iscsiadm -m discovery -t st -p 10.8.230.108

3. Enable logon to the DR Series system iSCSI VTL target(s) by using the following command: iscsiadm -m node --portal <IP or IQN of DR:PORT> --login For example:

iscsiadm -m node --portal "10.8.230.108:3260" --login

4. Display the open session(s) with DR VTL(s) by using the following command:

iscsiadm -m session

For example:

iscsiadm -m session = tcp: [8] 10.8.230.108:3260,1 iqn.1984-05.com.dell:dr4000.3071067.interoprhel52n1.30

5. Review dmesg or /var/log/messages for details about the tape devices created upon adding the DR Series system iSCSI VTL.

3.1.4 Configuring NetVault Backup to use the newly created iSCSI VTL

1. Access the Storage Configuration Wizard menu within the NetVault Administration interface. Select the **Add Storage Devices** button and then proceed to the Tape library/ medium changer submenu.

NetVault Backup	×	
← → C (*b#**	localhost:8443/configuration/devices/	ୟ ଦ୍ର ≣
NetVaul	Backup	L defudt - 0
Monitoring Server Wonttor Job Status Device Activity View Logs View Events	NetVault Storage Configuration Wizard	• Add Storage Devices
Jobs Create Rostans Jab Create Rostans Jab Kanaga Sab Rospan Jab Rospan Jab Rospan Jab Rospan Jab Nawa Rostans Jab Histony Confluence Nawage Creats Nawage C	ti Ad Clends India Rugor India Loorass I Add Storage Devices II Create Backup Jobr	 Steps vitual dis divise Historia tasse tasses David vitual vitas divise Test vitual dis divise Test vitual dis divise Add bill divise Add bill divise time Add bill divise time Test divise time time Add bill divise time Test divise time time time time time time time Test divise time time time time time time time tim

2. Select the NetVault node that has the iSCSI device configured, and, after the scan has completed, select the tape library to be added. Click **Next** to add the iSCSI tape library.

hetvauk Sadkup	× 🔄		
← → C (states	//iocalhost:8443/configuration/devices/addilbrary2.html		옥 습 🖩
NetVau	lt Backup		2 defeuit - 0
Monitoring Server Konitor Job Status Device Activity View Logs View Events	NetVault Configuration Wizard - Add Tape Library (2/3) The Johanny Units were book when scanning the science clear. Nexus science the unit that you wish to out to NetWorld Bookage.		
Jobs		Device display name:	Costate some for this deep e
Create Backup Job Create Rectore Job	Denice	Serial Humber	
Manage Sets	(8-0.0.1 pTx LT00)	wweerv_co	
Manage Job Definitions	8-0.1.1 (51K L700)	W1L0K3_00	
Manage Policies Explore Storage	(a) (b) (b) (b)		1 - 2 of 2 Herric
Job History Centicuration Guided Configuration Manage Dievices Manage Dievices Manage Dievices			
Configure Notifications Change Settings			
Help Documentation Video and Tutoriais			
			C Back Next

3. When the tape library has been added, click the **Create Backup job...** button to commit the library. The VTL should show up ready for use.

NetVault Backup	× 🔤	
← → C (states	//localhost:8443/configuration/devices/addilibrary3.html	ର 🏠 🔳
NetVaul	t Backup	🚊 default - 🏾 0
Monitoring Server Monitor	NetVault Configuration Wizard - Add Tape Library (3/3)	
bo Statute Device Activity View Log: View Log: View Device Jobs Create Backup, Job Create Backup, Job Create Backup, Job Create Backup, Job Anage Job Definitions Anage Job Definitions Anage Chef View Reports View Reports View Reports View Reports View Reports View Reports View Reports Configure Schröster Anage Clentos Anage Clentos Charge Sattrigs View Schröster View Reports Configure Schröster Charge Sattrigs		encourt them places press the "Add drives balandsig"buttion to select which top.



4. Label all the media with labels and place them in their respective media groups for use.

ing Mana	ge Devices					
Honitor	ige berices					
rus Activity	Tape Library:	AUTOINT8: 8-0.0.1 (STK L700) Drives: 10	Slots: 10 (Online)			C • •
ei	DRIVE 1	8-0.0.2 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
ents	DRIVE 2	8-0.0.3 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
Backup Job	DRIVE 3	8-0.0.4 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
Restore Job	DRIVE 4					o
Sets Job Definitions		8-0.0.5 (IBM ULT3580-TD4)	Online	(Idle)	Unloaded	•
Policies	DRIVE 5	8-0.0.6 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
Storage	DRIVE 6	8-0.0.7 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
18 ports	DRIVE 7	8-0.0.8 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
ory	DRIVE 8	8-0.0.9 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	0
ration Configuration	DRIVE 9	8-0.0.10 (IBM ULT 3580-TD4)		11	Unloaded	0
Clients	DRIVE		Online	(Idle)		•
Devices	10	8-0.0.11 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
Users re Notifications		T	P I - 1			0
Settings	Slots	Total: 10 (10 Populated, 0 Empty), 0	Blank.			
ntation nd Tutorials						

3.2 Creating and configuring NDMP target container(s) for NetVault Backup

3.2.1 Creating the NDMP VTL container for NetVault Backup

You need to create and export the NDMP container in the DR Series system GUI.

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

-interop-a7.ocarina.local	Containers			2 Create)	Edit Delete Displa	
Dashboard Alerts	Number of Containers: 2				Container Path:	/containe
Events	Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
Health	backup	0	Auto	NFS, CIFS	Not Configured	0
Usage Container Statistics	intvm05iscsi	31	Networker	VTL ISCSI	Not Configured	0
Storage Containers Replication Encryption - Clients Schedules System Configuration	0					

2. Enter the container name and select the Virtual Tape Library (VTL) option. Click Next.

Container Wizard - Create Ne	w Container		
- Container Name			* = required fields
Container Name*: Container Name*: Virtual Tape Library (VTL) :	Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter. System_A3_VTL1	1	- required heros
		Cancel	Next >

3. Select the **NDMP** Access Protocol. Specify the DMA Access Control by providing the storage node or media node IP Address or FQDN. Select the Marker Type as **Unix Dump**. Click **Next**.

ontainer Wizard - Create New (Container			
Configure Virtual Tape Library				* = required field
Is OEM:				Container Name and Type System_A3_VTL1
Tape Size:	800GB	O 400GB	O 200GB	VTL
	O 100GB	○ 50GB	0 10GB	
Access Protocol:	NDMP		O No Access	
Access Control:	FQDN or IP			
Marker Type:	Unix Dump	3		
	None			
			< Ba	ack Cancel Next >

4. Finalize VTL creation by clicking **Create a New Container**.

onfiguration Summary	* = required field
Container Name and Type Container Name: System_A3_VTL1 Connection Type: VTL	Virtual Tape Library OEM: no Tape Size: 800gb Access Protocol: NDMP Access Control: iqn.1991-05.com.microsoft:2k8r2intvm0 Marker Type: Unix Dump
	Sack Cancel Create a New Container

3.2.2 Configuring NetVault Backup to use the newly created NDMP VTL

You need to add the DR Series system as an NDMP node by using the NDMP Plugin.

1. Navigate to the Create Backup Set submenu, and select the NDMP Plugin within the NetVault Create Selection Set navigation pane. Select to add a new NDMP Server node. In the dialog box, enter the name of the node, the IP address, and DR the credentials. Provide the logon credentials for the ndmp user account on the DR Series system.

itoring Create Ba	ckup Job				~	Consolidate Increi Sa Data Copy		
Job Status	v backup job by selecting or creating o	otions sets below.			Ţ	Piersystem MacMarket MacMarket		
IS IN INCOMENTS	Job Name:	Job Nome			5	O NDMP Clent O NDMP Clent O NotVault Databas O Raw Device	8	
anage Sets anage Job Definitions	Selections:			■ Creste New) ° 			
anage Policies iplore Storage	Plugin Options:		*	Create New	5	Actions • Open		
worting ew Reports & History	Schedule:	Immediate	×	Create New	5	About Configure	nental backups	
ifiguration Juded Configuration	Target Storage:	Default Backup Target Options	×	Create New	7	Add Server	н 🕹	
anage Citerits anage Devices anage Users	Advanced Options:	Default Advanced Backup Options	v	# Create New	2	Ele System NDMP Client	- (
the second second	proved and	and and and		Surge according	~~~~ ~~ ~~ ~~ ~~ ~~ ~~ ~~ ~~ ~~ ~~ ~~ ~	• Raw Device	"	
						NDMP Server	6	
						Name: Addressinth		
						Aurosoft.		
						Patimore		

2. Access the Storage Configuration Wizard menu within the NetVault Administration interface. Select the **Add Storage Devices** button and then proceed to the Tape library/ medium changer submenu.

NetVault Bachup	× 💻	
← → C (*bitte:/	localhost:8443/configuration/devices/	ର ଛା ≡
NetVault	Backup	± default - 0
Monitoring Server Monitor Job Status	NetVault Storage Configuration Wizard	- Add Storage Devices
Device Activity View Log: View Events	Select the type of desice that you wish to add from the set below. If you s created but has been removed from NetNoult Backup.	select one of the Virtual device types you must also specify whether you want to croate a new virtual device or whether you want to readd one that has been
Joins Create Bestorp Job Create Bestorp Job Hanage Sets Manage Notices Explore Storage Report Ting View Paperts Job Interny Configuration Manage Devices Manage Ma	ASS Clients Instal Pages Instal Pages Instal Pages Instal Rames Create Dackup Job	 enclosed with a data data data data data data data

3. Select the NetVault node that has the NDMP device configured, and, after the scan has completed, select the tape library to be added. Click **Next** to complete the workflow to add the NDMP tape library. The VTL should now show up ready for use.

NetYault Backup	×		
← → C (sbaps	//localhost:8443/configuration/devices/additorary2.html		ର 🏠 🗄
NetVau	lt Backup		🛔 defeult - 🛛 0
Monitoring Server Monitor Job Status Device Activity	NetVault Configuration Wizard - Add Tape Library (2/3)		
View Logs	The following library units were found when scanning the selected client. Flease select the unit that you wish to add to Nethoult Backup.		
View Events Jobs		Device display name:	Custom nome for this device
Create Backup Job Create Restore Job	Device	Serial Number	
Manage Sets	8-0.0.1 (STK L700)	WW8DIY_00	
Manage Job Definitions	8-0.1.1 (5TK L200)	W1L0K3_00	
Manage Policies	Device DRv22:1700-Ni YONH _00 _01K L700)	NEYCHAL_00	
Explore Storage	Device DRv02:L700-50T02H_00 (5TK L700)	SOT02H_00	
Reporting View Reports	(H, 4, 5, H)		1 - 4 of 4 items
Job History			
Configuration			
Guided Configuration			
Manage Clients Manage Devices			
Manage Users			
Configure Notifications			
Change Settings			
Help Documentation			
Video and Tutorials			
			0
			Š
			& Back Next



4. Label all the media with labels and place them in their respective media groups for use.

ver Monitor Status	ige Devices					
ice Activity		AUTOINT8: 8-0.0.1 (STK L700) Drives: 10 S				C • •
w Logs w Events	DRIVE 1	8-0.0.2 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
w Events	DRIVE 2	8-0.0.3 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
ate Backup Job	DRIVE 3	8-0.0.4 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	°
ate Restore Job	DRIVE 4	8-0.0.5 (IBM ULT 3580-TD4)	Online	(I-die)	Unloaded	0
age Sets age Job Definitions		8-0.0.5 (IBM OLT 3580-104)	Unline	[(die)	Unipaded	•
age Sob Den Incons	DRIVE 5	8-0.0.6 (IBM ULT 3580-TD-4)	Qnline	(Idle)	Unloaded	ō
ore Storage	DRIVE 6	8-0.0.7 (IBM ULT3580-TD4)	Online	(Idle)	Unloaded	•
rting «Reports	DRIVE 7	8-0.0.8 (IBM ULT 3580-TD-4)	Online	(Idle)	Unloaded	0
History	DRIVE 8	8-0.0.9 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	0
guration				1 1		•
led Configuration age Clients	DRIVE 9	8-0.0.10 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
age Devices	DRIVE 10	8-0.0.11 (IBM ULT 3580-TD4)	Online	(Idle)	Unloaded	•
aga Usars figure Notifications rage Settings	Slots	Total: 10 (10 Populated, 0 Empty), 0 E	llank			۰
umentation						



Setting up the DR Series system cleaner

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.

"Dashboard "Alerts	Cleaner Sched	lule	Schedule Cleaner	Sched
⊡Events ⊡Health ⊡Usage	System time zone: US/C	entral, Mon Jan 23 15:18:49 2012		
Statistics: Container	Day	Start Time	Stop Time	
Statistics: Replication	Sun			
Storage	Mon		-	
Containers	Tue			
Replication	Wed		-	
Compression Schedule	Thu		-	
Replication	Fri		-	
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		

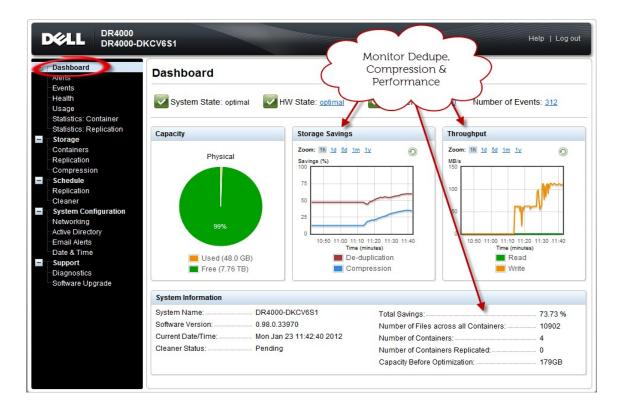


4

Monitoring deduplication, compression, and performance

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 VTL configuration guidelines

A.1 Managing VTL protocol accounts and credentials

A.1.1 iSCSI account details and management

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 StOr@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

sys-63.ocarina.local 🔹	Cliente					Undata O	lient Edit Password	dit CHAP Password Delete DR2000
Global View	Clients					opuate of		dit CHAP Password Delete DR2000
Dashboard Alerts	Total Numbe	r of Clie	ents: 1					2
Events Health	NFS	CIFS	RDA	NDMP	iscsi	DR2000v		
Usage Container Statistics Replication Statistics	Number of ISCSI Curre	nt Sess	ions Stati		ve: 1			
Storage Containers	Name	Co	ntainer IO				Initiatore Connect	od
Replication	Test-VTL		iqn E	dit CHAP A	ccount			
Encryption	-		~	ARNING: A	ll existing i	SC SI sessions	s will be terminated upon	submission.
				New CHAP	Password			*All fields are required
Clients							(3)	
Clients Schedules System Configuration			C	onfirm New I	Password:			

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

A.1.2 NDMP account details and management

The default username for the NDMP service is "ndmp_user." This can be confirmed on the NDMP tab of the Clients page in the DR Series system GUI.

nterop-a7.ocarina.local 🗸	Clien	ts				Update Client	Edit Password	Delete DR2
Global View Dashboard	Total Nu	mber of Clients	· 0					
Alerts Events Health	NFS			DMP iSCSI	DR2000v			
Usage	Numbe	r of Current ND		ana in active: 0				
Container Statistics	Numbe	r or current ND	WP Sessi	ons in active: 0				
Replication Statistics	NDMP	Current Sessions	Statistics					
Storage	ID	Duration	State	Source	Target	Throughput	Transfer Size	DMA
Containers								
Replication	NDMP	Completed Sessi	ons Statis	tics				
Encryption	ID	Duration	State	Source	Target	Avg. Throughput	Transfer Size	DMA
Clients scneaules								
								3
	_							
			word					
Networking		Edit Pass	woru					
Networking Active Directory		Edit Pass					All fields are require	ed.
Networking Active Directory Local Workgroup Users		Edit Pass		ype: NDMP			All fields are require	ed.
Networking Active Directory Local Workgroup Users Email Alerts		Edit Pass	Client T	ype: NDMP me: backup_user			All fields are require	ed.
Networking Active Directory Local Workgroup Users Email Alerts Admin Contact Info			Client T	me: backup_user			All fields are require	ed.
Networking Active Directory Local Workgroup Users Email Alerts Admin Contact Info Password		N	Client T User na	me: backup_user ord:			All fields are require	ed.
System Configuration Networking Active Directory Local Workgroup Users Email Alerts Admin Contact Info Password Email Relay Host Date and Time		N	Client Ty User na ew passw	me: backup_user ord:		Cancel	All fields are require	

You can also use the CLI command ndmp -show as shown in the following example.

> ndmpshow	
NDMP User:	ndmp_user

The default password is St0r@ge! It can be modified by running the ndmp – setpassword command:

```
> ndmp --setpassword
```

NDMP Port:

10000

NDMP password successfully updated.



A.1.3 VTL Default Account Summary Table:

Service	Account	Default Credentials	CLI Modifier
NDMP	ndmp_user	St0r@ge!	ndmpsetpassword
iSCSI	<appliance hostname=""></appliance>	St0r@ge!iscsi	iscsisetpassword

A.2 Managing VTL media and space use

A.2.1 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.

A.2.2 Physical DR 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: 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.

A.2.3 Logical VTL geometry and media sizing

The logical size of the VTL including media size and media count should be made such 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 in 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 and also provides the 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 so care must be taken in order 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 Virtual Tape Library would be created with 152 (121TB divided by 800GB) pieces of media at 800GB for each piece media.



	Pre-Deduplication							
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

A.2.4 Media retention and grouping

Due to the nature of Virtual Tape Libraries media must be managed in order to insure 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, such as NetVault Backup, 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.

A.2.5 VTL media count guidelines

Туре	Capacity	Max number of Tapes supported
LTO-4	800GiB	2000
LTO-3	400GiB	4000
LTO-2	200GiB	8000
LTO-1	100Gib	10000
LTO-1	50Gib	10000
LTO-1	10GiB	10000

A.2.6 Adding media to the VTL container

To add media to an existing VTL container navigate to the containers menu option. Select and edit the target VTL container. Use the resulting dialog box field Add More Tape (no of Tape) field to input the number of tapes to add to the VTL container.

9-interop-a7.ocarina.local View	Containers			Cre	ate Edit Delete Displ	ay Statistic
Dashboard Alerts	Number of Containers: 5				Container Path	/container
Events	Containers	Files	Marker Type	Access Protocol Enab	led Replication	Select
Health Usage	backup	0	Auto	NFS, CIFS	Not Configured	0
-Container Statistics	intvm05_ndmp	31	Unix Dump	VTL NDMP	Not Configured	0
Replication Statistics	intvm05iscsi	31	Networker	VTL ISCSI	Not Configured	0
Storage	intvm05iscsi2	31	Networker	VTL ISCSI	Not Configured	0
Containers	TEST_VTL_LALA	31	None	VTL NDMP	Not Configured	0
Schedules System Configuration Networking Active Directory Local Workgroup Users Email Alerts Admin Contact Into Password Email Relay Host Date and Time Support	-Configure Virtual Tape Library - is GEAt Tape Size: Access Protocol Access Control	 \$ 200GB 100GB NDMP FQDN or IP 10.8 238 125 	0 400GB 0 50GB 0 ISCSI	200GB 10GB No Access	Container Name and T TEST_VIL_LALA VTL	/pe
	Add More Tape (no. of tape):	10				
Diagnostics Software Upgrade						

Alternatively you may also use the "vtl -create_carts" cli command for this operation:

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

```
Created 10 cartridges
```

A.2.7 Updating NetVault Backup to identify newly added VTL media

After the VTL media has been added to the target VTL container, NetVault must now be updated to be able to use the newly created media.

- 1. Select the VTL and conduct an inventory update.
- 2. Navigate to the Tape Library Management menu for the given DR VTL and select to Open Door. The Activity and Door Status will change from (Online;Closed) to (Door Open;Open).
- 3. At this time select the Close Door function, which will force an update to the inventory of the library contents. This will result in a Read Element Status request by the NetVault Software, which in turn will update the new inventory status resulting in the newly added tapes appearing for use within NetVault: Backup.

NetVault Backup					22	1
u) NetVault Backup					1	distant - 1
iterin: Tape Library Management						
Name AUTOINT8: 8-0.0.1 (STK 1200)	Ortwa:					
vice Activity we Loat	0.0	a name	Status	activity	Contents	
Product L700	Direct Direct	E 1 0-0.0.2 (BH ULT2300-TD4)	onine	ide	Unicaded	
Drives 10 Stots 10	CR04	E 2 0-0.0.2 (BM ULT2500-TD4)	Otiline	1de	unicaded	
Client AUTONTS	CR0	E 3 8-8.0.4 (BM ULT3588-TD4)	Otilina	Ide	Unkaded	
Status Calles	P DRM	E 4 8-9.0.5 (BM ULT2589-TD4)	Otiline	ide	Univaded	
age lot Confections Activity Online	Den cen	E 5 8-9.0.6 (BMULTISSO-TD4)	onine	104	Unloaded	
age Potster	D 000	E 6 8-0.0.7 (844 ULTD580-TD4)	driline	ide	univaded	
ire Mirage	💭 (167)	E 7 8-0.0.8 (6M ULT)580-TD4)	Celline	ide	unisaded	
rting	. DRM	E 6 0-9.0.3 (BM ULT2589-TD4)	onine	x5e	unicaded	
Ritisry	Diese	15 T 8-0.0.10 (8M ULYD500-TD4)	Onitria	ide	Unloaded	
status Online	D 580	E 10 8-8-0.11 (BM ULT3586-TD4)	Onine	154	Unloaded	
Activity Door Open						
Door Open						
ge Denker						
ge lettings						
en and Taite Hall						
eo arva na to traite						
			0			
					1.1	and to Harts

A.2.8 Space reclamation guidelines

General Guidelines

The DR v3.2 Appliance Virtual Tape Library feature is presented to operating systems and data management applications 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 DRs own cleaning cycle should be used to reclaim that virtual tape media space which in turn will free up physical space on the DR unit.

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 your individual DMA applications for best practices and guidelines regarding tape reuse.

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, Scratched or otherwise recycled and a manual cleaning cycle initiated on the DR unit.

For Netvault Backup the following can be used when a situation dictates that space must be reclaimed manually.

- 1. From the Explore Storage: Tape & VTL Storage: Explore Tape Storage page select the volume and Blank it.
- 2. Repeat this process as needed with all media items that can be reconciled for reclamation.

CAUTION: This will permanently delete / destroy the data on these virtual volumes.

NetVault B	ackup					🚨 admin - 🛛 🛛
Job Status	Explore Tape Med	FDOE NAME	Choose a saveset from the	NPP Public	Q. search	
Device Activity View Logi View Logi Create Rectore Ab Create Rectore Ab Create Rectore Ab Anage At Anage Ab Create Anage Ab Create Anage Ab Arabit Manage Ab Arabit Anage Ab Arabit Sol Atomy View Reports Job History Configuration Anage Configuration Anage Configuration Anage Configuration	Label Group Library Offsite Location Media Type Data Stored Space Available Reuse Policy Date Last Writee Read Errors Write Errors Usable Read-Only Media Online	AUTOINT® 13 Apr 11:36-1 AUTOINT®: Device DRv32:L700-5ROEAM_00 (STK L700 None ULTRIUM 4/16T U-416 0.00 KIS 8.00 GIB Reuse 4/13/2015, 11:42:50 AM Never 1 0 0 Yes No Yes	Saveset Date	Severand Manne	Size	Job/Instance/Phase
Change Settings fetp Documentation Video and Tutorials	Media Usage	< Back Ø Mark Unussable ■ Mark	(H) (H) (H) < Road Only	Scan 🔶 Blank	& Reuse	No Items to display

Alternatively users can opt to use the bulk blank facility for scale by accessing the Manage Devices: Tape Library Management Page.

NetVault	Backup							Lann - O
toring er sontor Statu	Tape Lib	orary Management						
ka Artivity e Logi e Events are fackup Job	Vendor Product Drives Slots	L700 10	Bay + Derve 1 Derve 2 Derve 3	Rame Tape DRvDI ULT358-TD+580_ Tape DRvDI ULT358-TD+580_ Tape DRvDI ULT358-TD+580_	Online	Activity idle idle idle	Contents Unloaded Unloaded Unloaded	*
ate Restore Job age Job Definitions age Job Definitions age Solicies Iore Storage	Activity	Online Online Closed	DRIVE 4 DRIVE 5 DRIVE 6 DRIVE 7	Tape Deviz UL 13480-TD4-580 Tape Deviz UL 73580-TD4-580 Tape Deviz UL 73580-TD4-580 Tape Deviz UL 73580-TD4-580 Tape Deviz UL 73580-TD4-580	Online Online	atla iche johi iche	Uninaded Chicaded Unicaded Unicaded	_
rting or Reports History iguration ded Configuration			DRIVE 8 DRIVE 1 DRIVE 10	Tape DRVD2.ULT3580-TD+580_ Tape DRVD2.ULT3580-TD+580_ Tape DRVD2.ULT3580-TD+580_	Online	ide ide ide	Univaded Univaded Univaded	
age Cherto age Divitor Age Isors Agare Hetrifications Agare Hetrifications Inge Settings waventation In and Tutoritals	>							
			 1.1.1	i.				1 - 10 of 10 Heres



3. When the reconciliation process has completed on the NetVault: Backup software, from the DR Series system, initiate a cleaning cycle either via the UI or via the command line. For example:

> maintenance --filesystem --reclaim_space

Successfully started cleaner.

4. Make sure that the space has now been reclaimed via the UI or via the command line. The Cleaner Status should transition from Running to Pending at which time the statistics should change to reflect the reclaimed space. For example:

> statssystem	
Capacity Used	: 22.0 GiB
Capacity Used in GB	: 23.666
Capacity Free	: 7970.4 GiB
Capacity Free in GB	: 8558.199
Read Throughput	: 0.00 MiB/s
Write Throughput	: 0.00 MiB/s
Current Files	: 66
Current Bytes	: 33595753405
Post Dedupe Bytes	: 24926224990
Post Compression Bytes	: 22734553886
Post Encryption Bytes	: 0
Post Encryption Bytes in GiB	: 0.0 GiB
Compression Status	: Done
Cleaner Status	: Running
Encryption Status	: Disabled
Total Inodes	: 101
Bytes decrypted	: 0
Dedupe Savings	: 25.81 %
Compression Savings	: 8.79 %
Total Savings	: 32.33 %

D¢LL