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

Dell Engineering
April 2015

A Dell Technical White Paper

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

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. 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

Executive 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 10

2.1 Adding the RDA target container(s) for NetVault Backup 11

2.2 Configuring transport modes for NetVault Backup 14

2.2.1 Setting the mode using the CLI 14

2.2.2 Setting the mode using the GUI 14

2.3 Configuring a backup job for NetVault Backup 16

3 Configuring VTL 17

3.1 Creating and configuring iSCSI target container(s) for NetVault Backup 17

3.1.1 Create an iSCSI VTL container for NetVault Backup 17

3.1.2 Configure the iSCSI target – Windows 19

3.1.3 Configure 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 Create the NDMP VTL container for NetVault Backup 25

3.2.2 Set up NetVault Backup to use the newly created NDMP VTL 27

4 Setting up the DR Series system cleaner 30

5 Monitoring deduplication, compression, and performance 31

A VTL configuration guidelines 32

A.1 Managing VTL protocol accounts and credentials 32

A.1.1 iSCSI account details and management 32

A.1.2 NDMP account details and management 33

A.1.3 VTL Default Account Summary Table: 34

A.2 Managing VTL media and space use 34

A.2.1 General performance guidelines for DMA configuration 34

A.2.2 Physical DR space sizing and planning 34

A.2.3 Logical VTL geometry and media sizing 35

A.2.4 Media retention and grouping 36

A.2.5 VTL media count guidelines 36

A.2.6 Adding media to the VTL container 37

A.2.7 Updating NetVault Backup to identify newly added VTL media 37

A.2.8 Space reclamation guidelines 38

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 NOTE: **About VTL Replication**: 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.

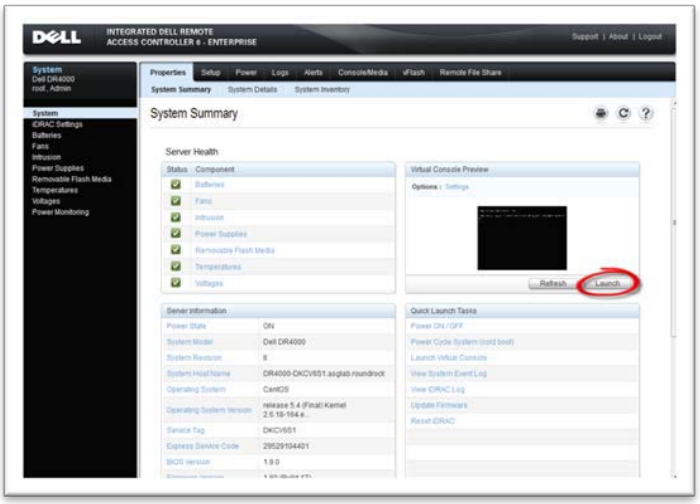
http://documents.software.dell.com/NetVault%20Backup/10.0.1/Compatibility%20Guide

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.

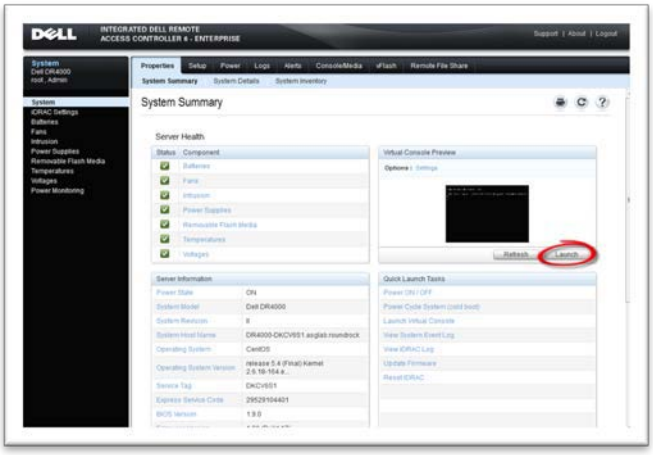
1.2 Installing and configuring the DR Series system

1. 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".

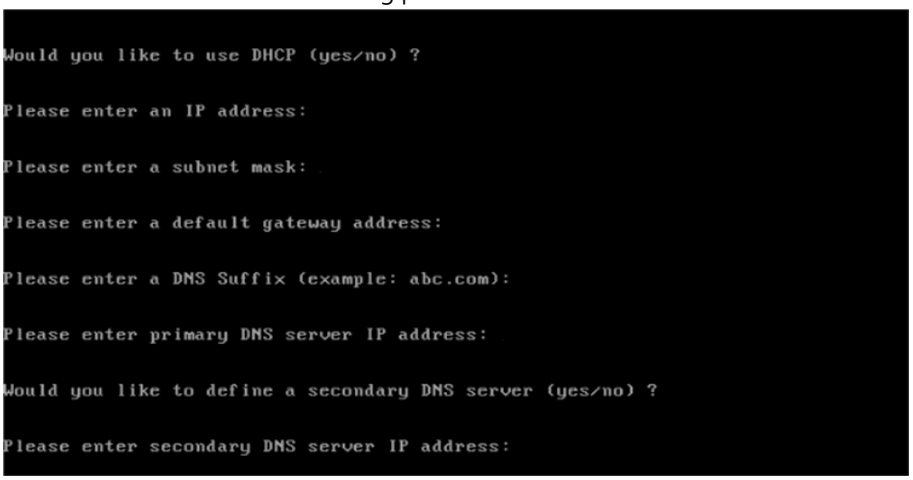


3. Launch the virtual console.

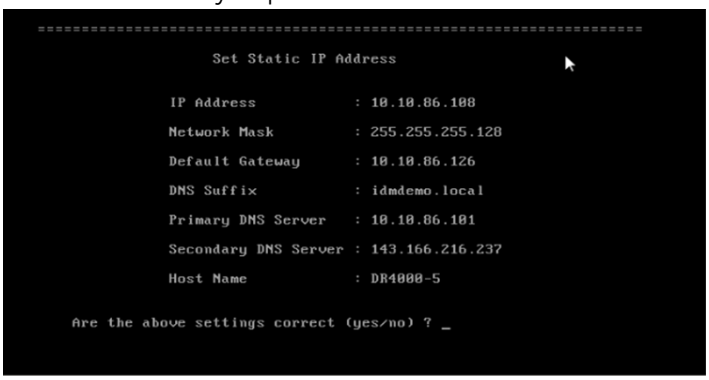


4. After the virtual console is open, log on to the system as user administrator and the password St0r@ge! (The "0" in the password is the numeral zero).

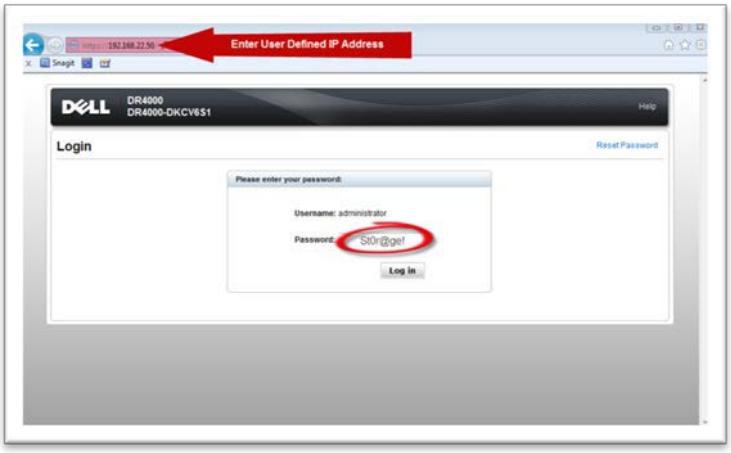
5. Set the user-defined networking preferences.



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



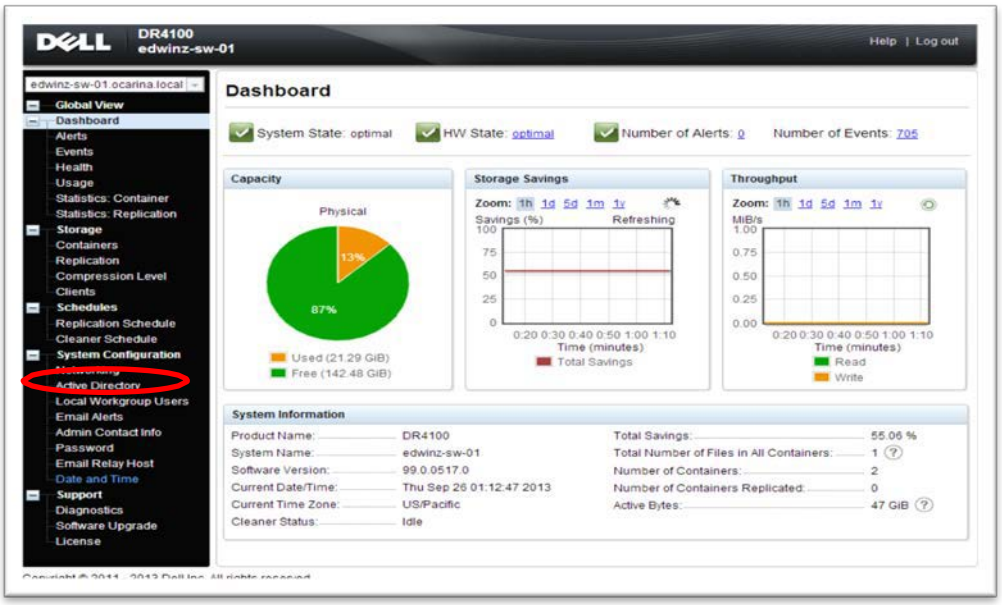
7. Log on to the DR Series system administrator console, using the IP address you just provided for the DR Series system, with username administrator and password St0r@ge! (The "0" in the password is the numeral zero.).



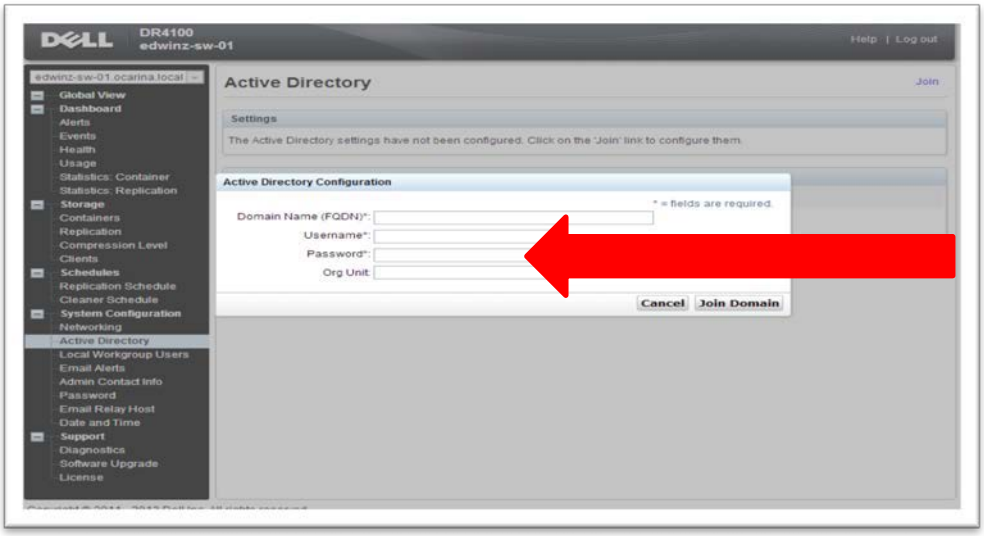
8. Join the DR Series system to Active Directory.

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

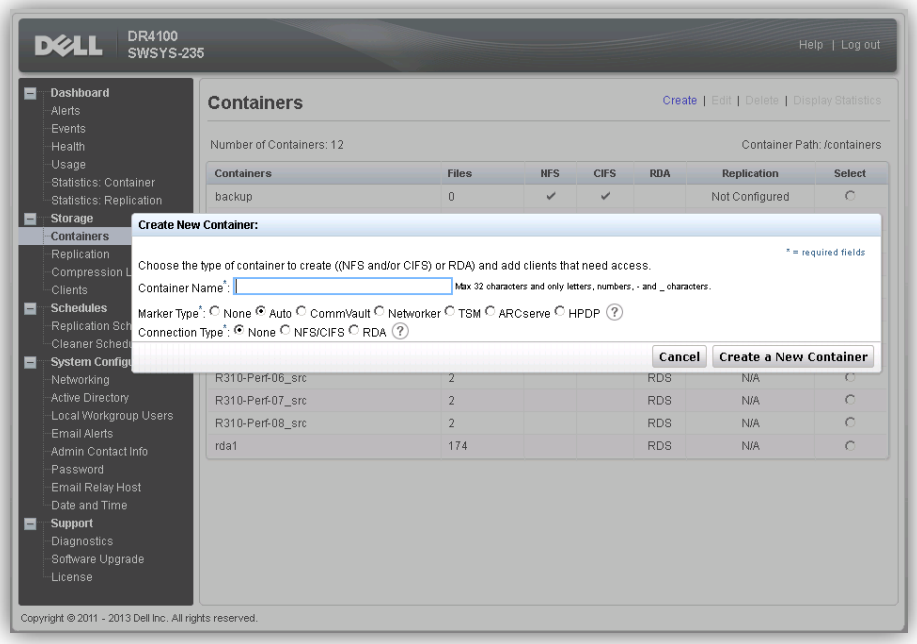


b. Enter your Active Directory credentials.

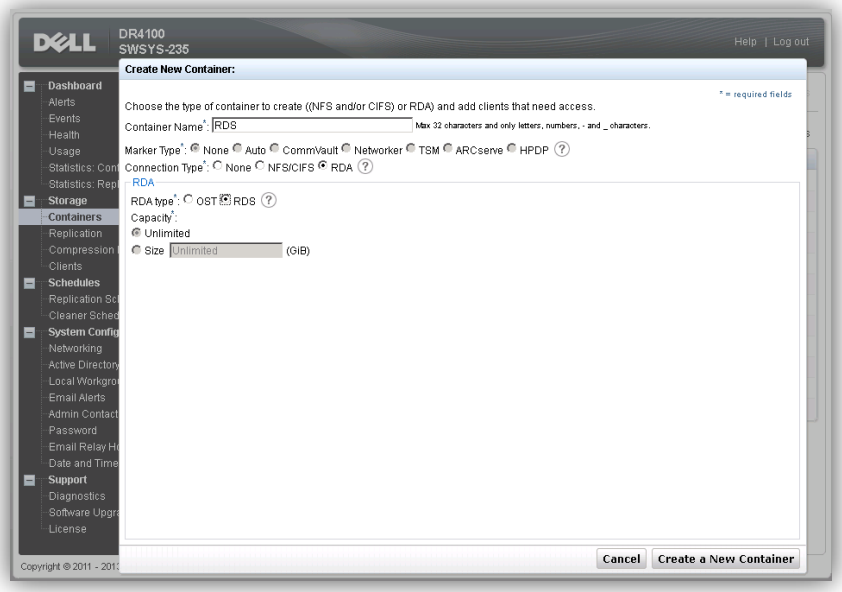


2 Creating and configuring the RDA target container(s) for NetVault Backup

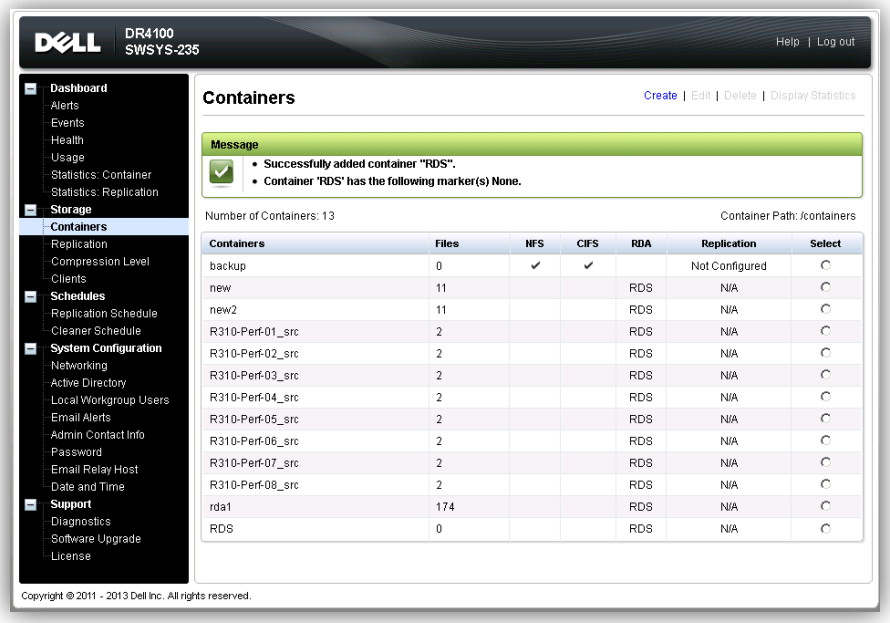
1. Create the RDS container in the Dell DR Series system. Select Containers in the left navigation area, and then click Create at the top of the page.



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

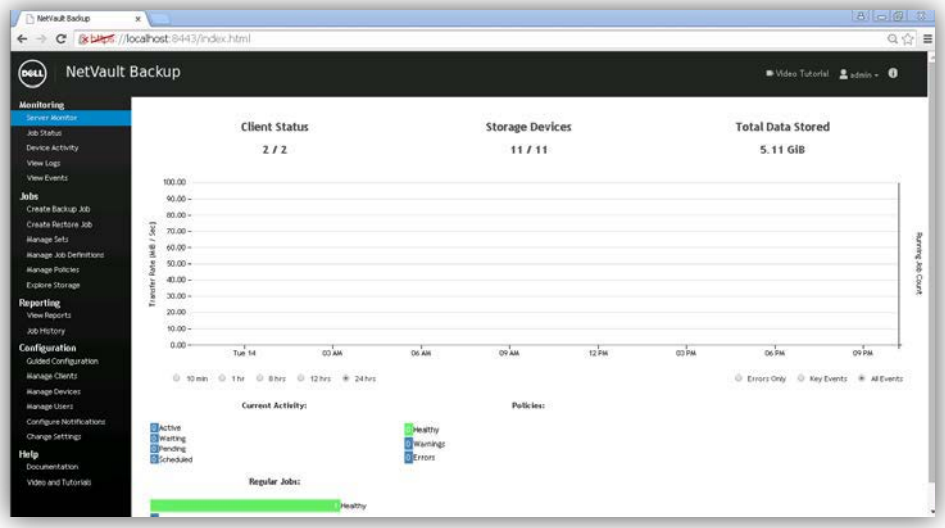


3. Click **Create a New Container**. Confirm that the container is added.

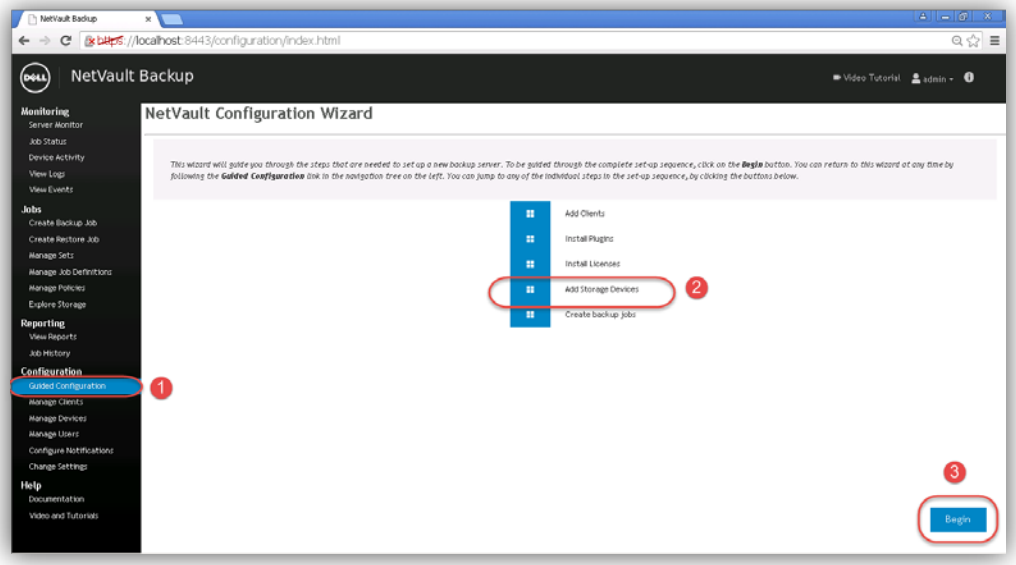


2.1 Adding the RDA target container(s) for NetVault Backup

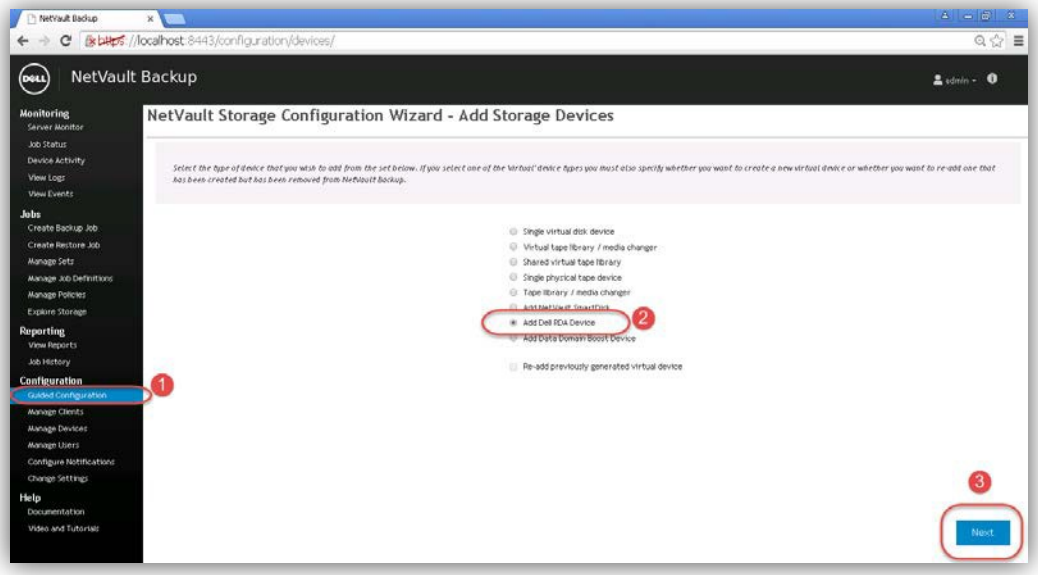
1. Open the NetVault Backup web console.



2. Add the RDA container to NVBU. Select to begin the guided configuration Add Storage Devices Wizard.

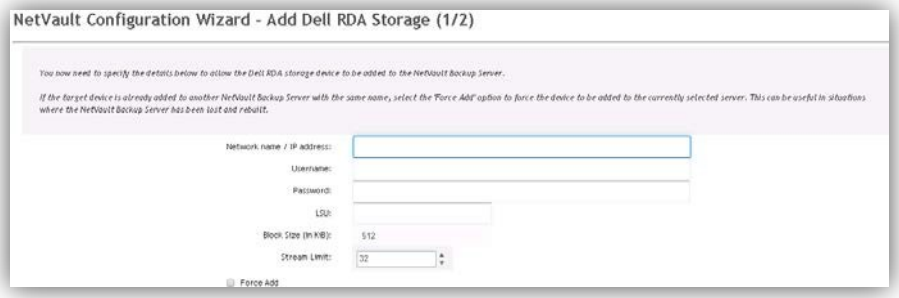


3. In the Storage Configuration Wizard – Add Storage Devices page, select Add Dell RDA Devices.

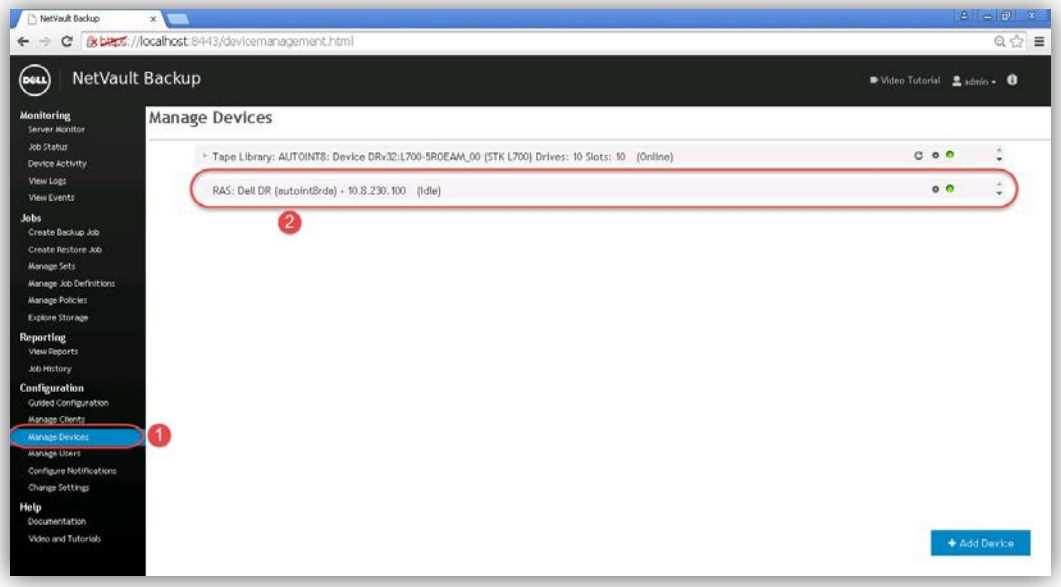


4. Enter the DR Series system hostname, username, and password to add the RDA device. Enter the RDA container name and save.

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



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



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 command:

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

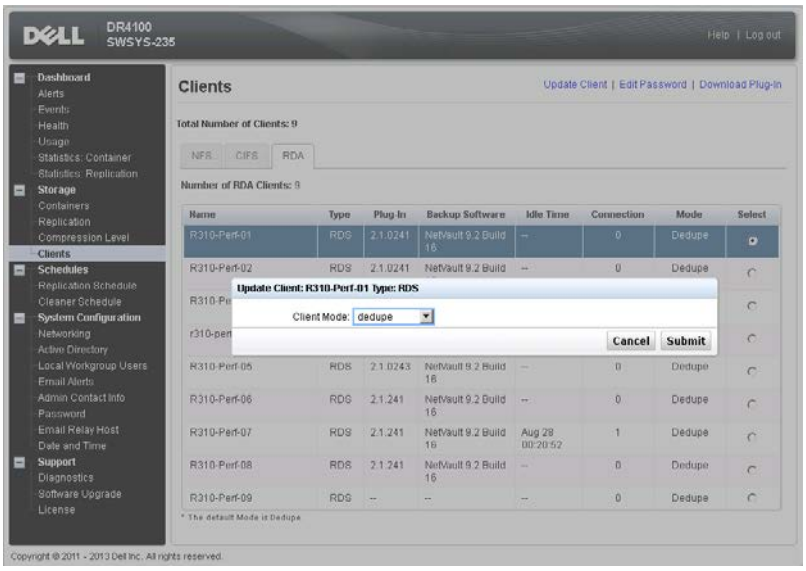
```
[root@SWSYS-235 ~]# rda --update_client  --name R310-SYS-86 --mode passthrough
Rapid Data Access (RDA) client R310-SYS-86 with mode Pass-through added successfully.
[root@SWSYS-235 ~]# rda --show --clients

RDA Client(s)                   Type    Plugin      OS                      Backup Software         Last Access     Connection(s)   Mode
R310-Perf-01                    RDS     2.1.0241    Linux 2.6.18-274.el5    NetVault 9.2 Build 16   --              0               Dedupe
R310-Perf-02                    RDS     2.1.0241    Linux 2.6.18-274.el5    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 are 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**.



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 about

- Creating a backup job for NetVault 9.2:

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

- Creating a backup job for NetVault 10:

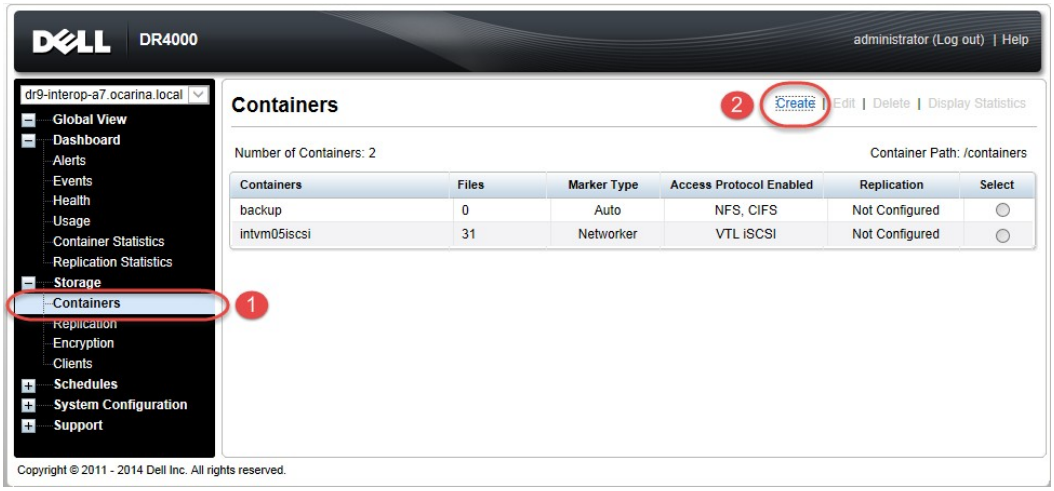
  http://documents.software.dell.com/DOC229690

3 Configuring VTL

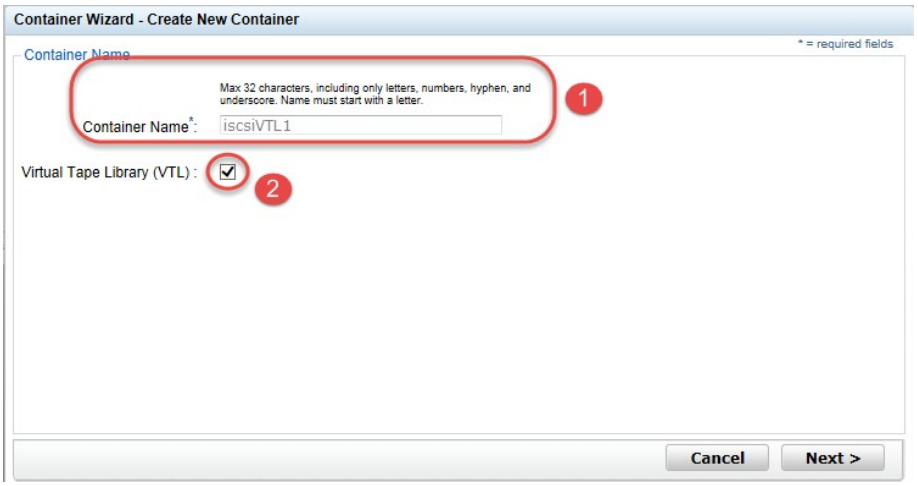
3.1 Creating and configuring iSCSI target container(s) for NetVault Backup

3.1.1 Create an iSCSI VTL container for NetVault Backup

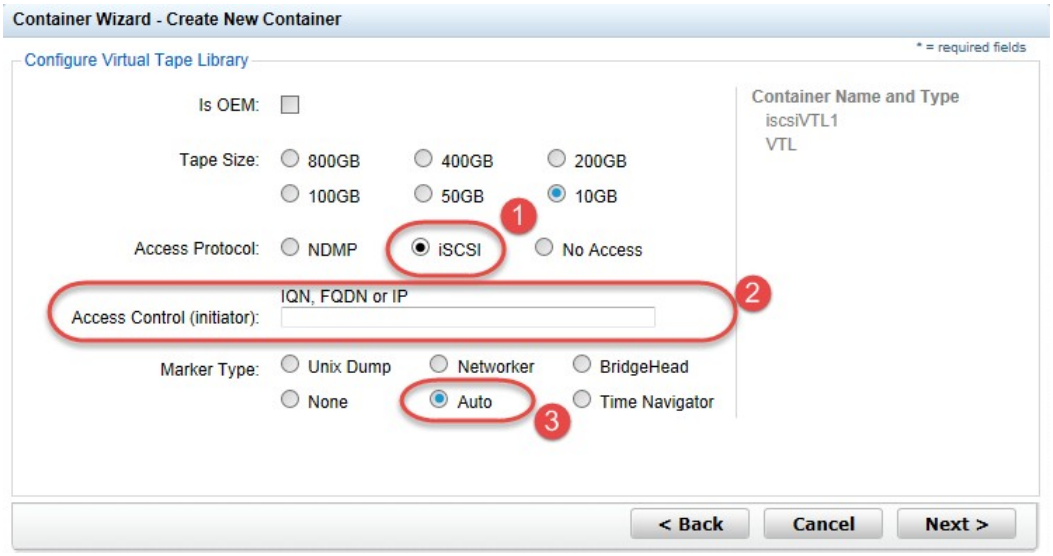
1. Create and export the iSCSI container.
   a. Select Containers in the left navigation area, and then click **Create** at the top of the page.



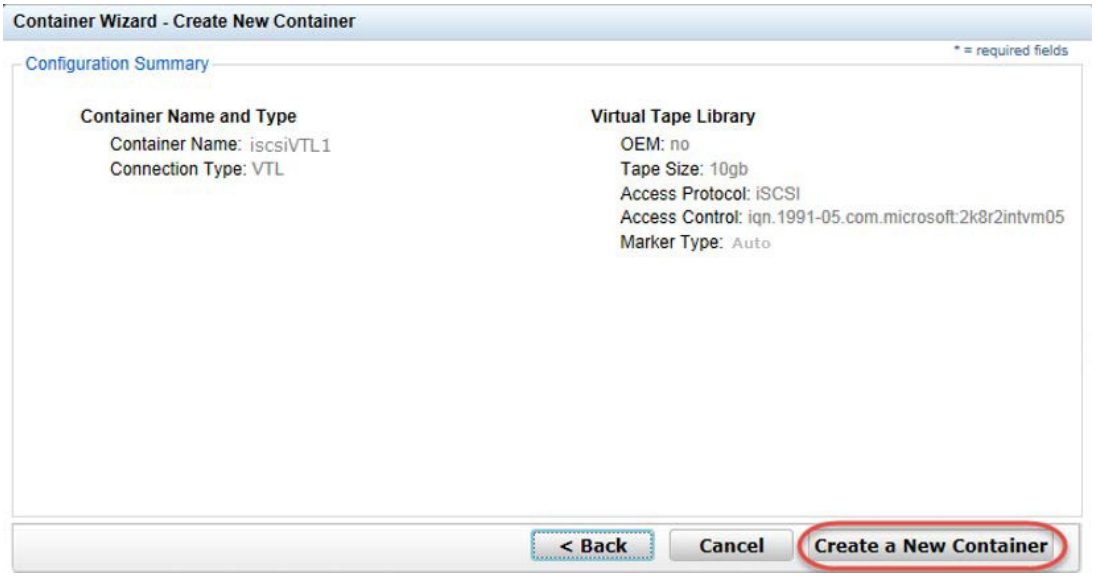
2. Specify your container name and select the VTL option.



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.

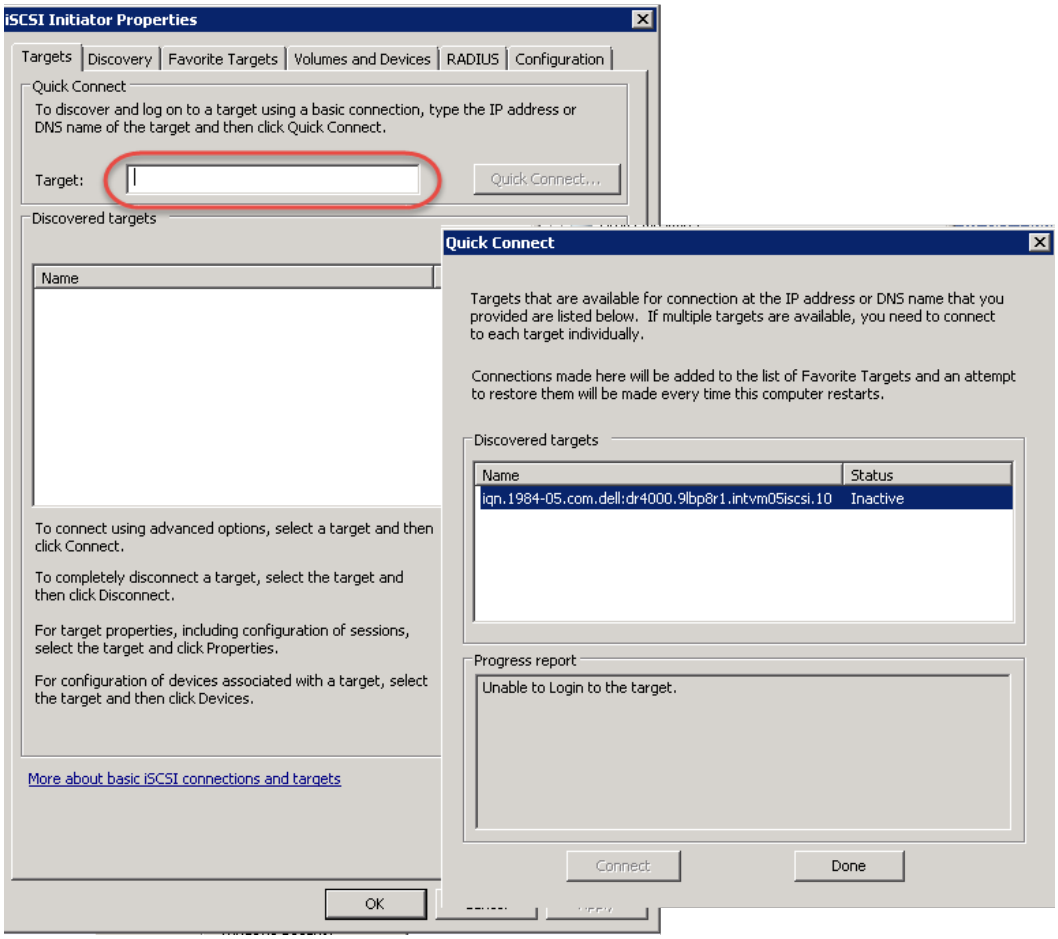


4. Finalize VTL creation by clicking **Create a New Container**.

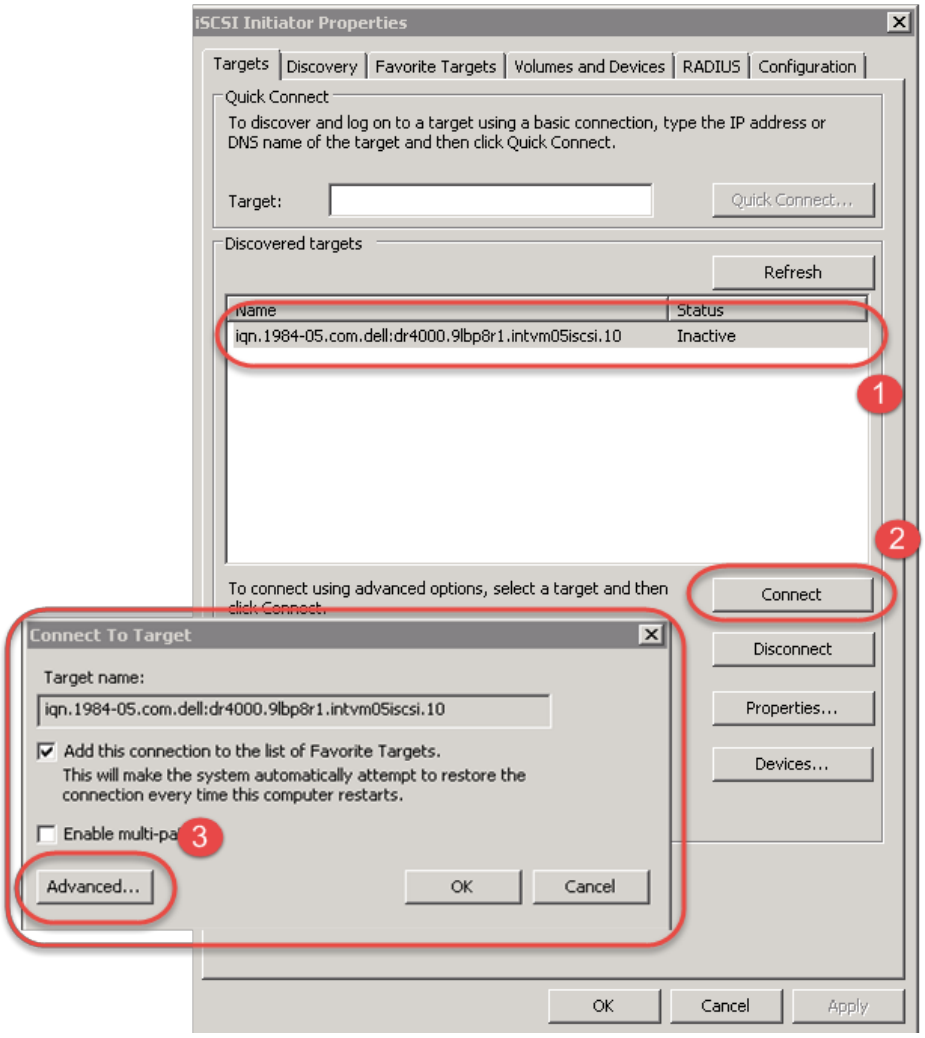


3.1.2 Configure the iSCSI target – Windows

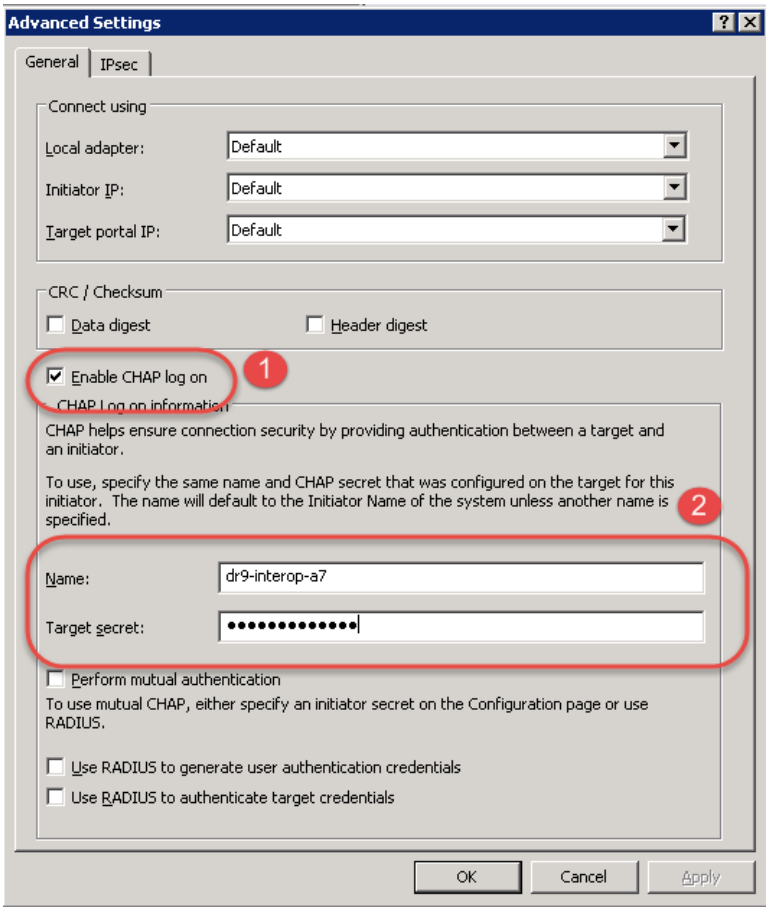
1. Configure the iSCSI Initiator Software for Windows by providing the IP or FQDN of the DR Series system into the Quick Connect, Target field. Click **Quick Connection** to open the Quick Connect dialog box, which indicates a connection was made but is set as inactive.



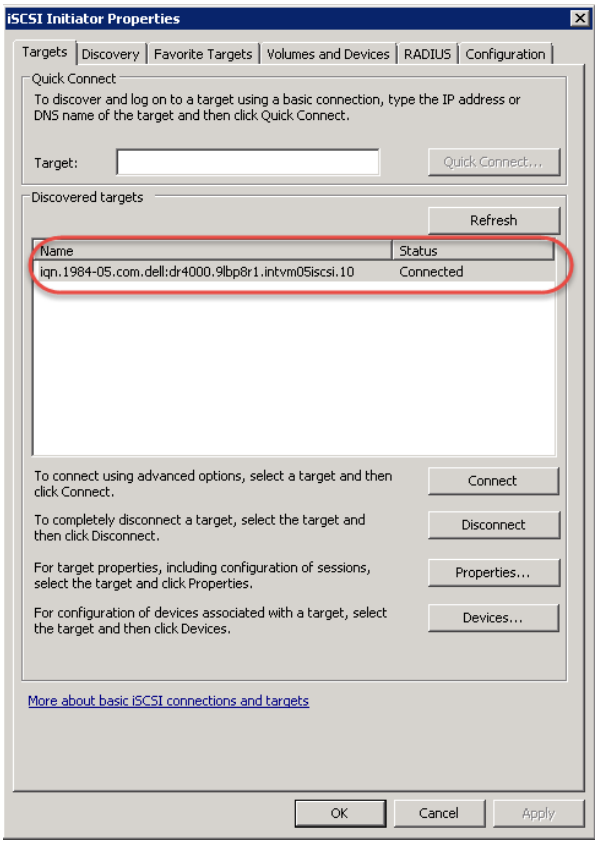
2. Close the dialog box and proceed by selecting the newly discovered target. This target will have an Inactive Status as it requires authentication parameters to be provided for iSCSI logon. Select the Target from the list, click the **Connect** button, and then in the Connect To Target dialog box,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



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.

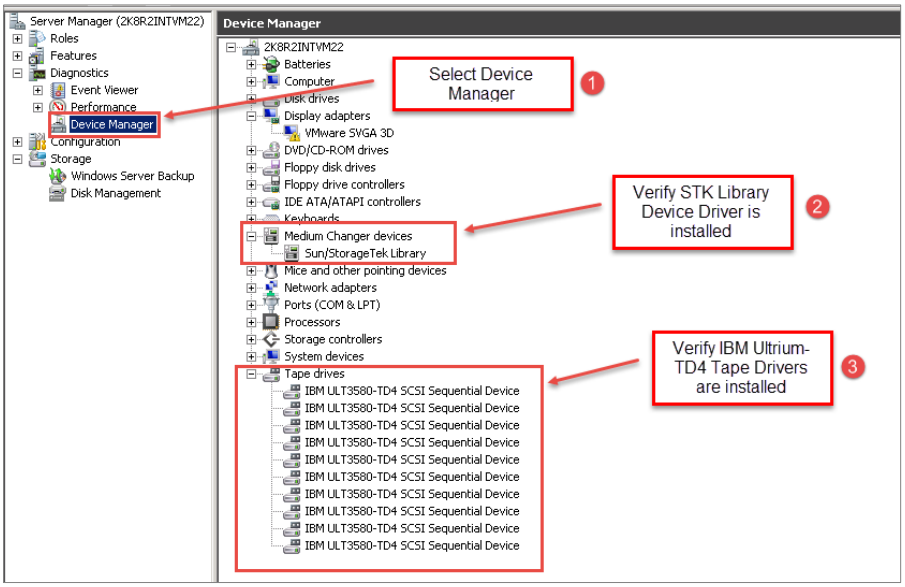


The iSCSI target should now show as connected and the device discovery can now proceed.



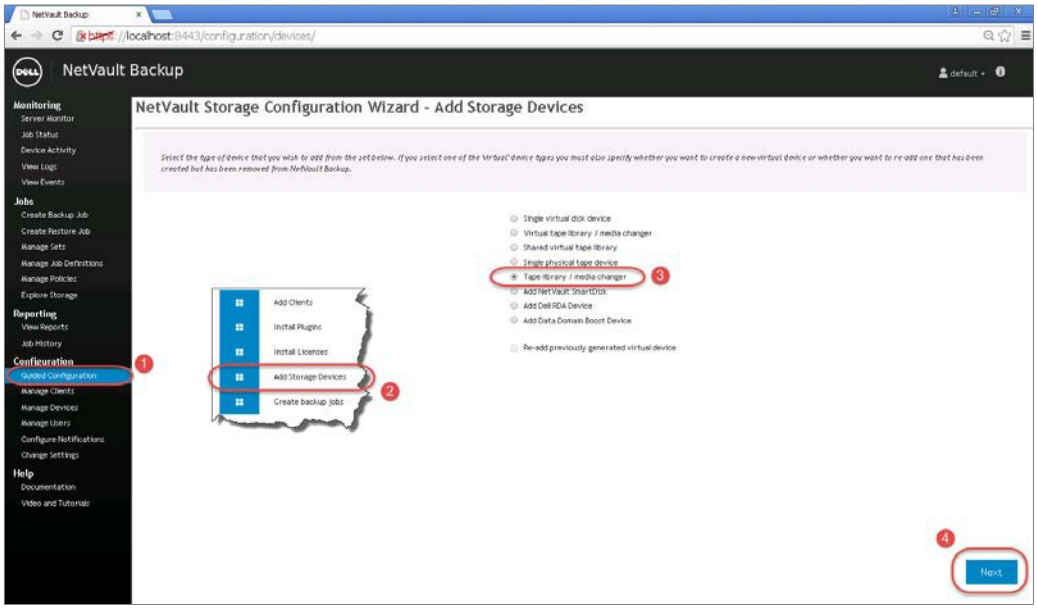
4. Open the Server Manager Snap-in and verify that the newly connected devices show up in the Device Manager. Verify that the STK Library and IBM Ultrium-TD4 Device Drivers are installed.

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

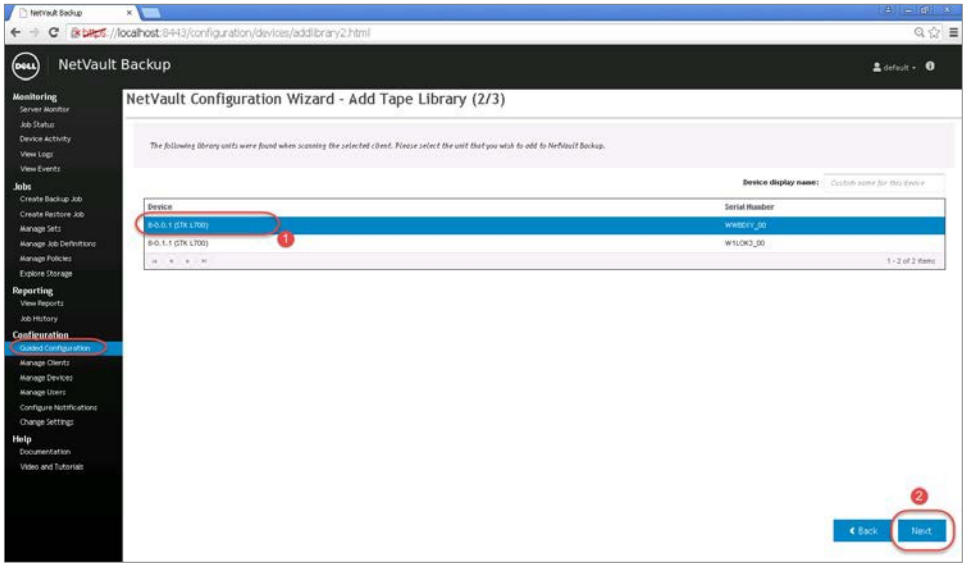


3.1.3 Configure NetVault Backup to use the newly created iSCSI VTL

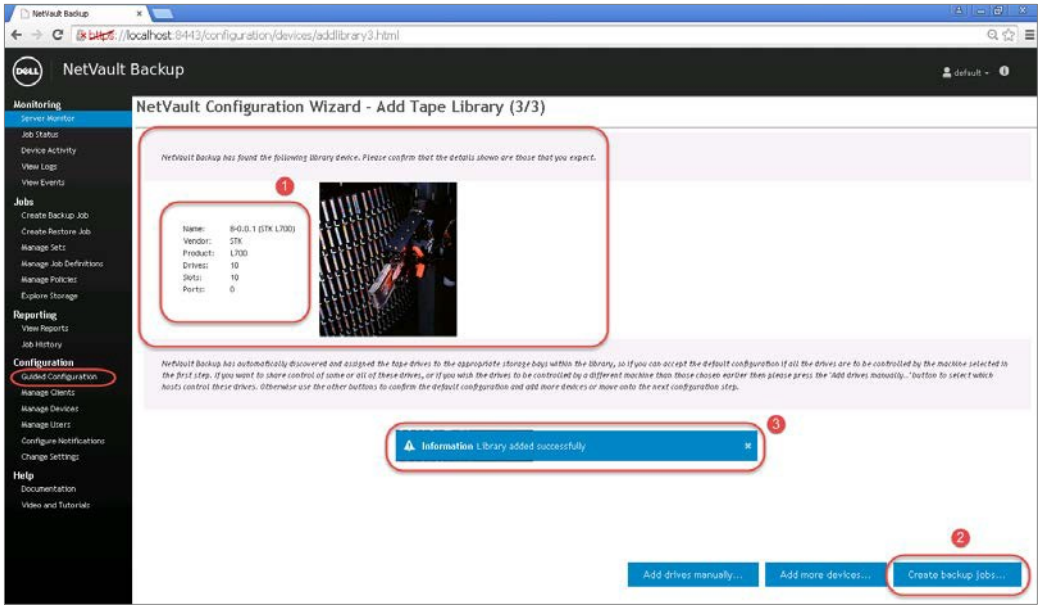
1. Access the Storage Configuration Wizard menu within the NetVault Administration interface. Select the Add Storage Devices button and then proceed to the Tape library/ medium changer submenu.



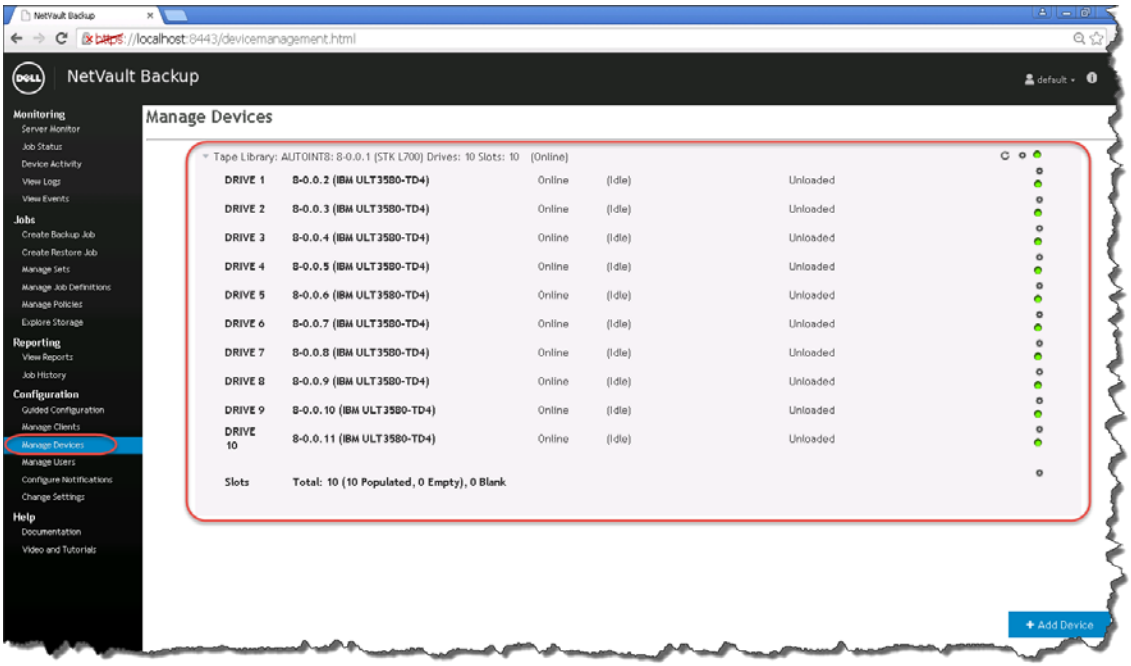
2. Select the NetVault node that has the iSCSI device configured, and, after the scan has completed, select the tape library to be added. Click **Next** to add the iSCSI tape library.



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.



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

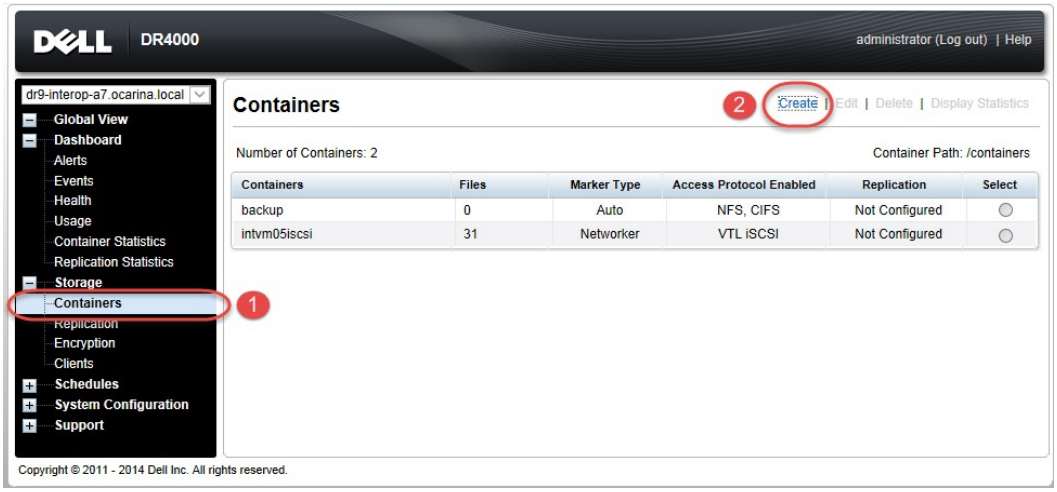


3.2 Creating and configuring NDMP target container(s) for NetVault Backup

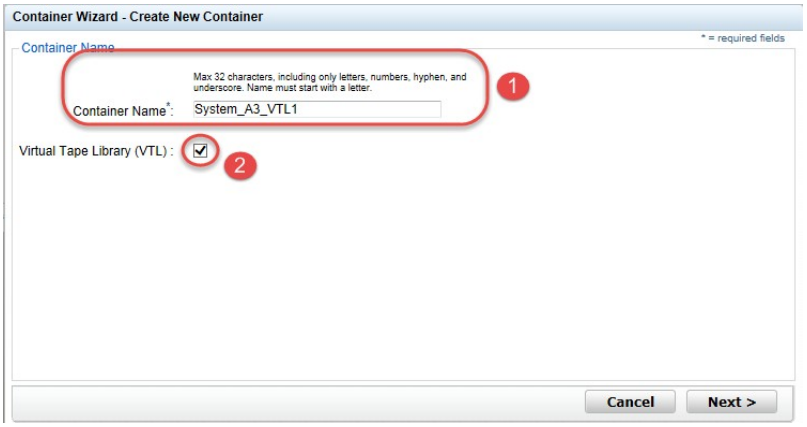
3.2.1 Create the NDMP VTL container for NetVault Backup

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

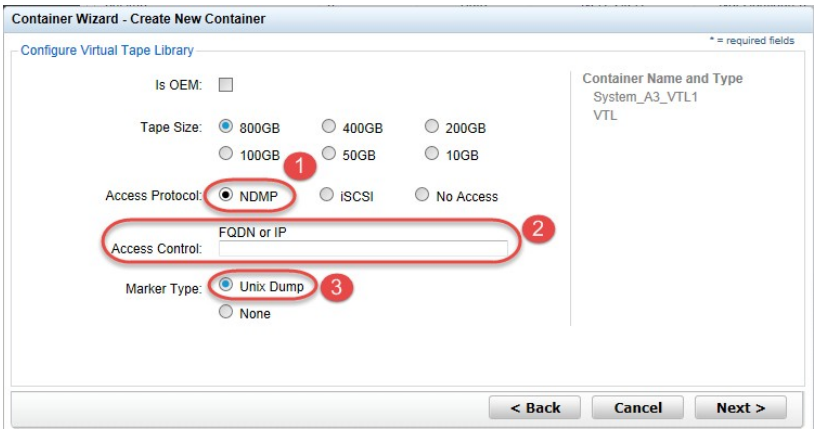
1. Select **Containers** in the left navigation area of the DR Series system, and then click the **Create** link at the top of the page.



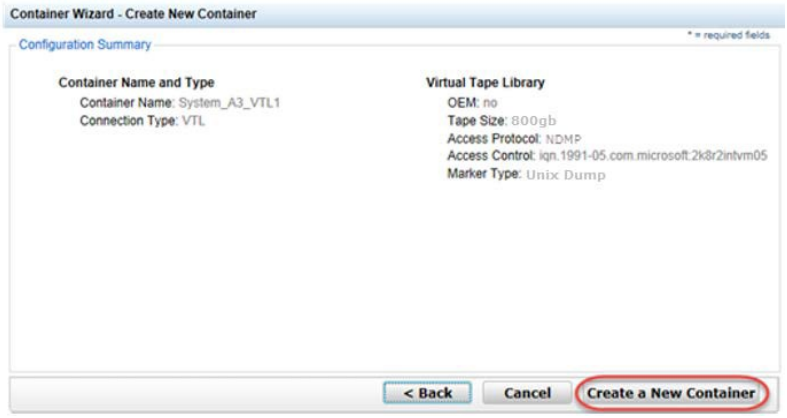
2. Enter your container name and select the **VTL** option.



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**.



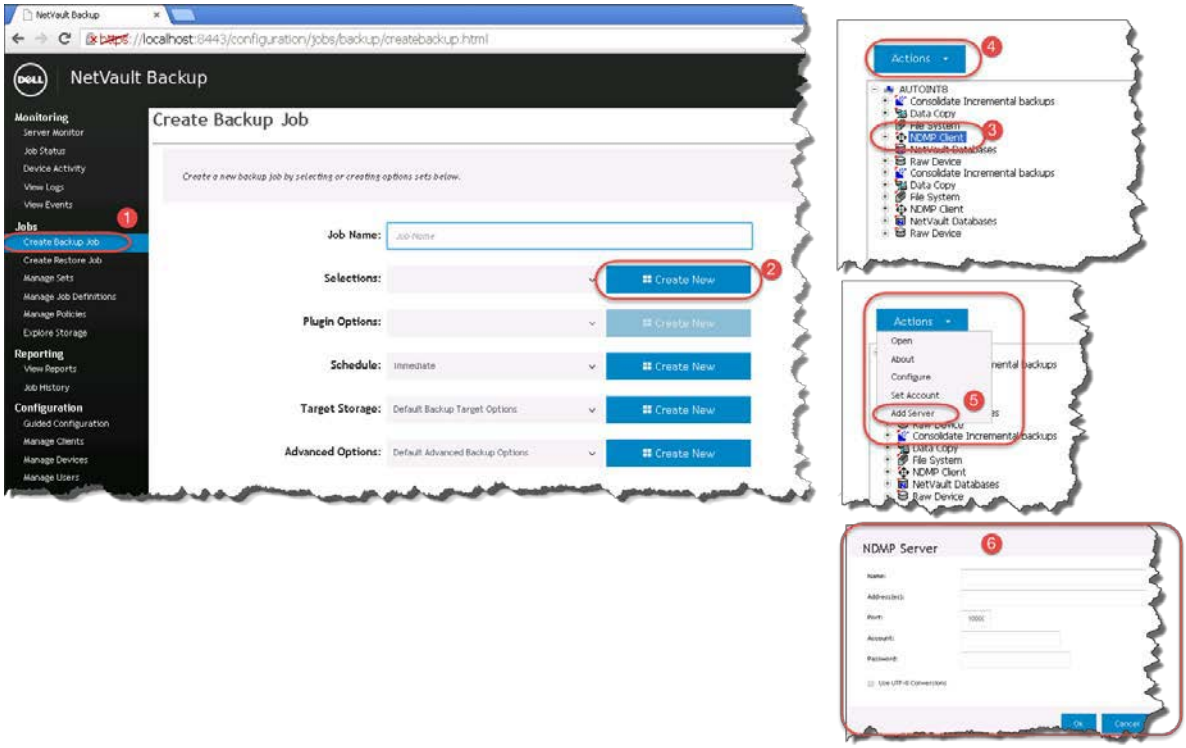
4. Finalize VTL creation by clicking **Create a New Container**.



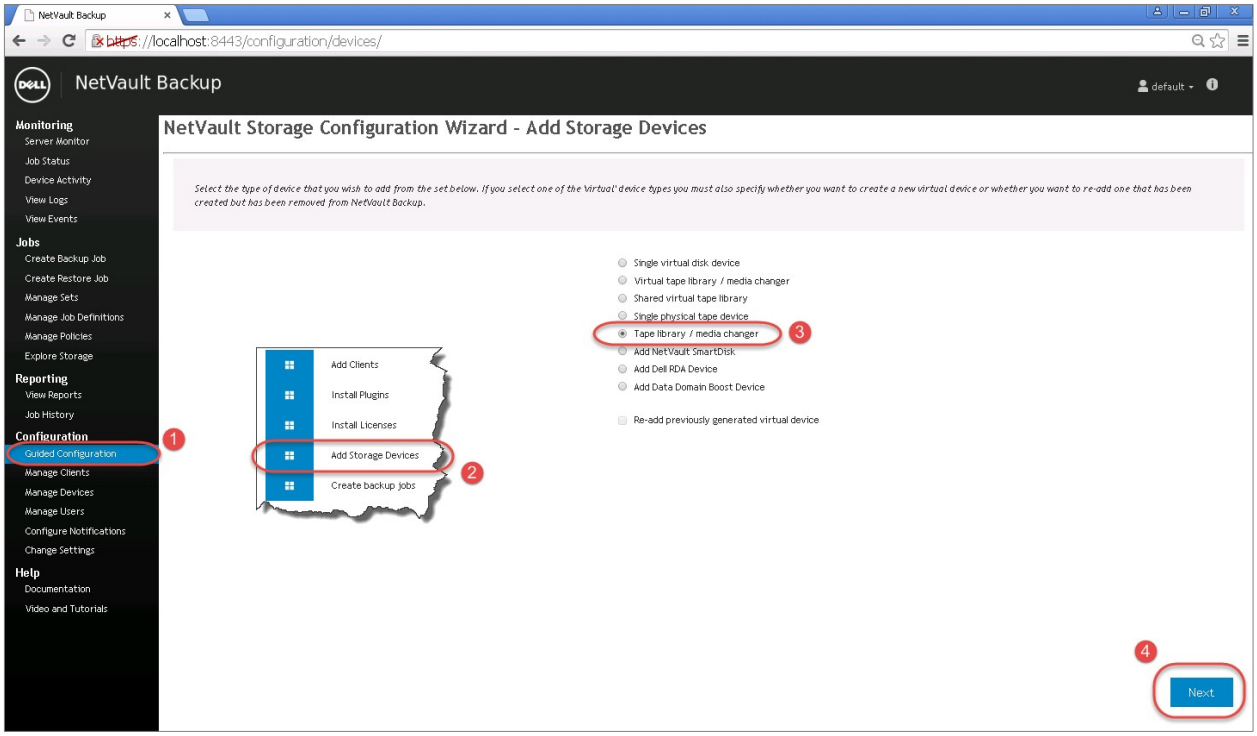
3.2.2 Set up NetVault Backup to use the newly created NDMP VTL

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

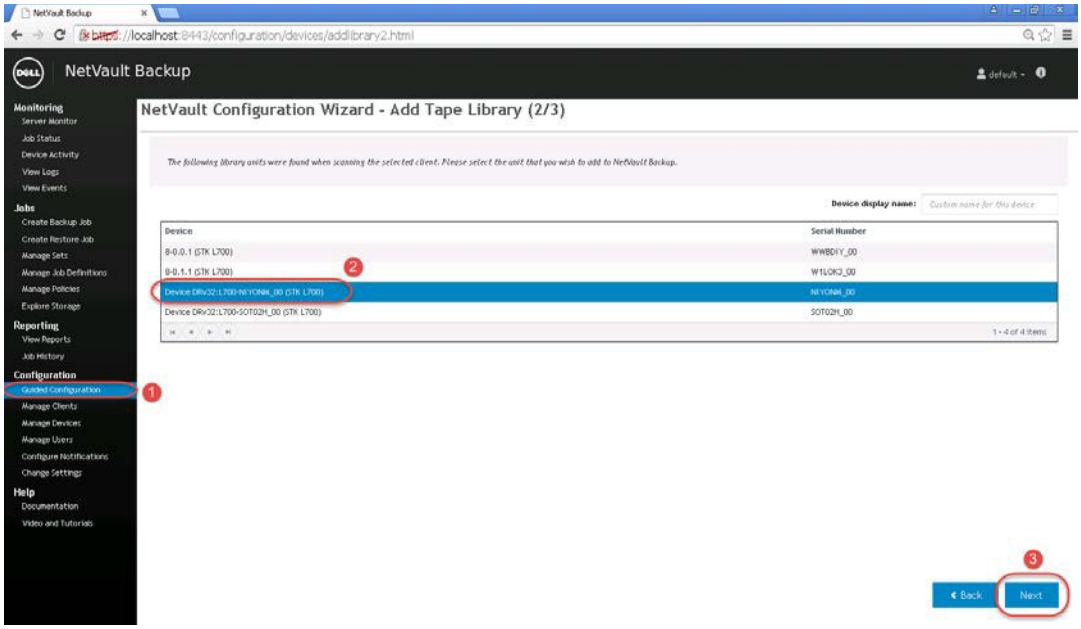
1. Navigate to the Create Backup Set submenu, and select the NDMP Plugin within the NetVault Create Selection Set navigation pane. Select to add a new NDMP Server node. In the proceeding dialog box, enter the name of the node, the IP address and DR the credentials. Provide the login credentials for the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



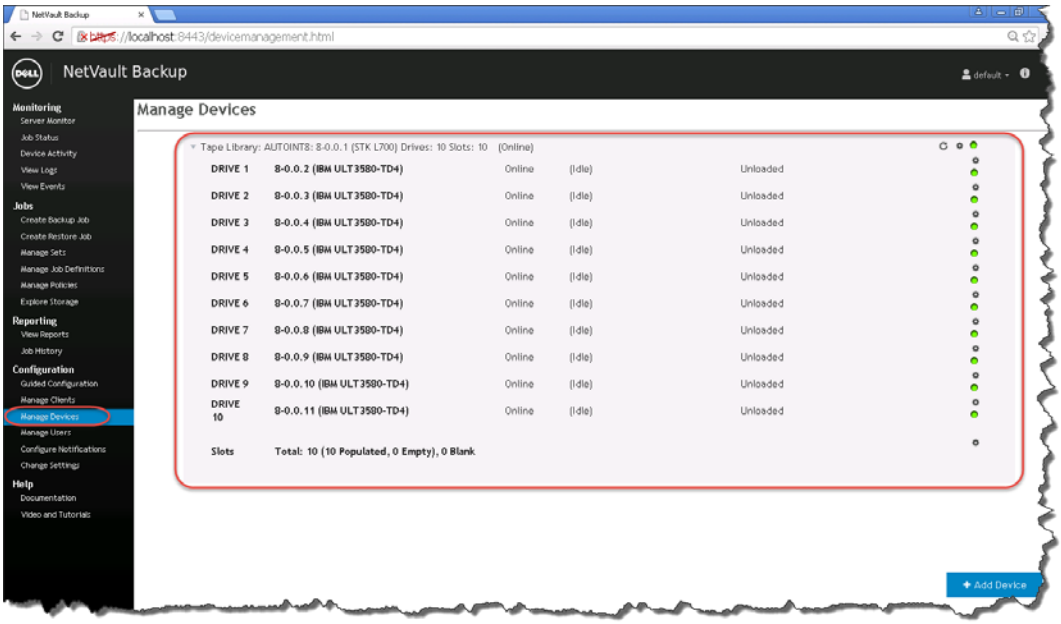
2. Access the Storage Configuration Wizard menu within the NetVault Administration interface. Select the Add Storage Devices button and then proceed to Tape library/ medium changer submenu.



3. Select the NetVault node that has the NDMP device configured, and, after the scan has completed, select the desired 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.



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

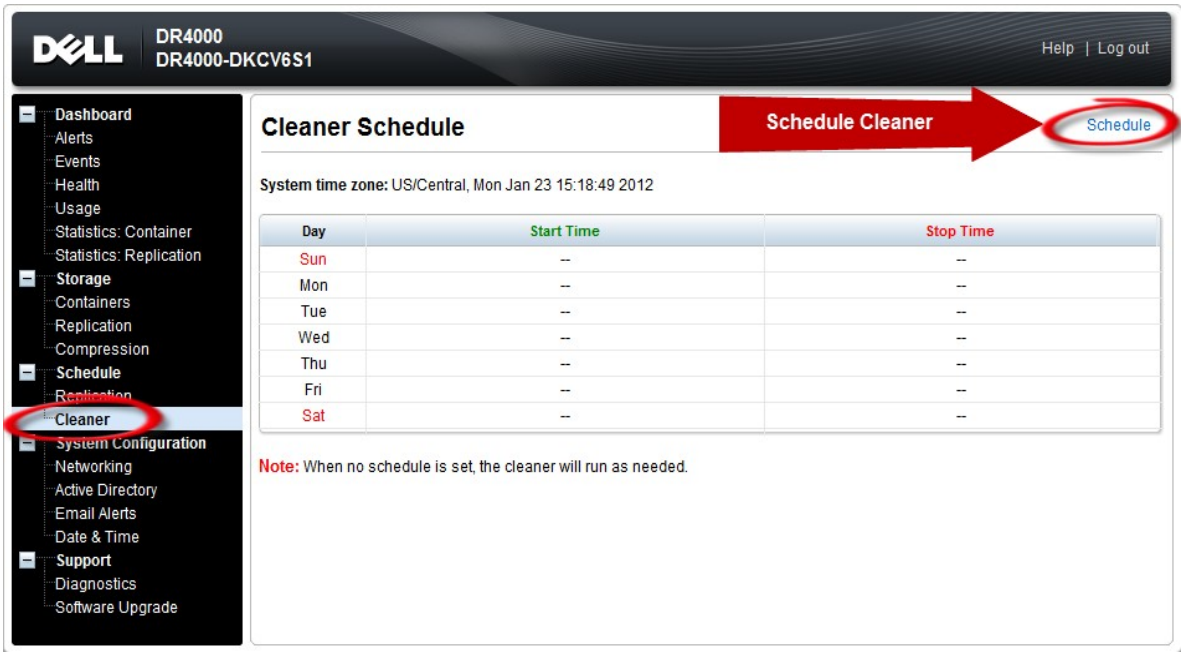


4 Setting up the DR Series system cleaner

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.



5 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

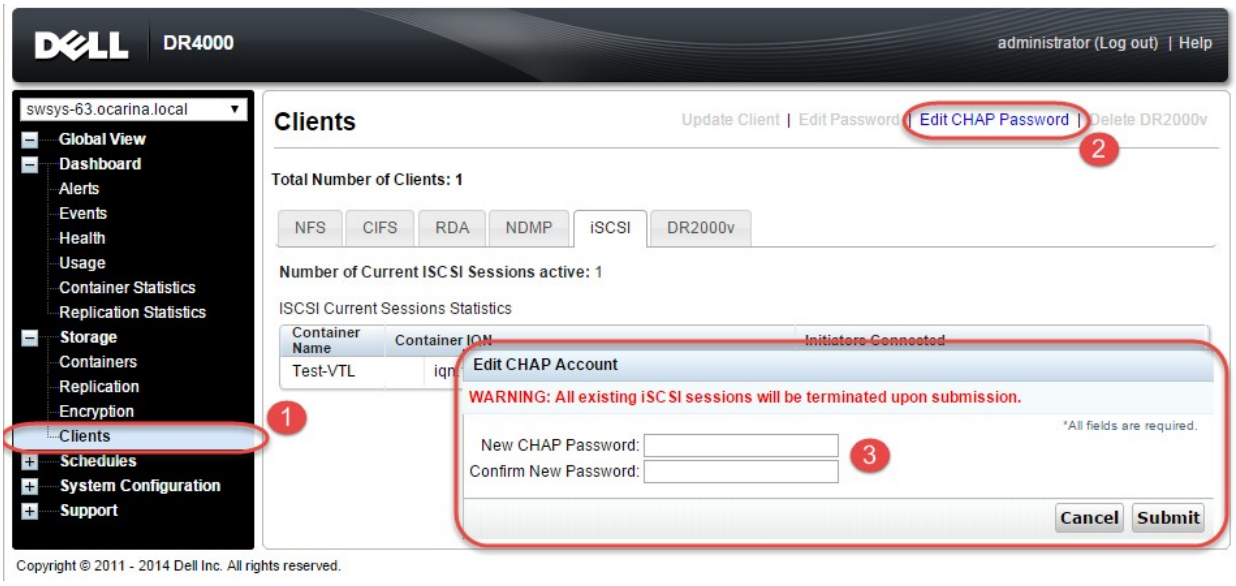
A.1.1 iSCSI account details and management

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 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

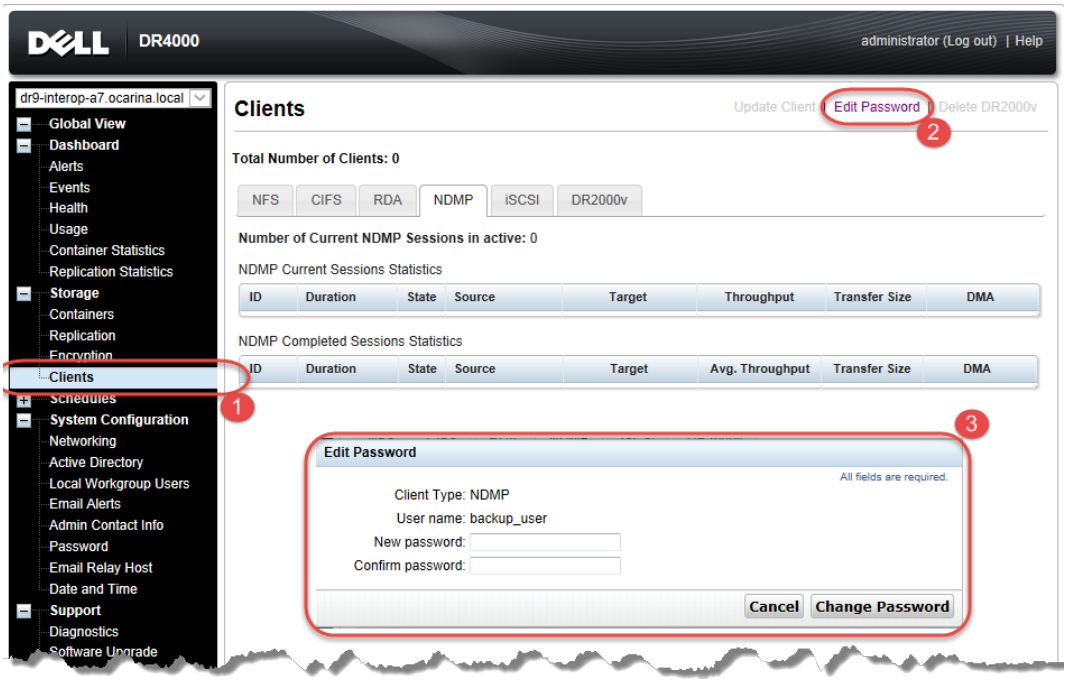


Alternatively, you can also use the iscsi--setpassword CLI command to change the iSCSI CHAP password as shown in the following example:

```
> iscsi --setpassword
WARNING: All existing iSCSI sessions will be terminated!
Do you want to continue? (yes/no) [n]?
Enter new CHAP password:############
Re-type CHAP password:############
```

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.



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

```
> ndmp --show
NDMP User:      ndmp_user
NDMP Port:      10000
```

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

```
> ndmp --setpassword
Enter new NDMP password:#########
Re-type NDMP password:#########
NDMP password successfully updated.
```

A.1.3 VTL Default Account Summary Table:

Service	Account	Default Credentials	CLI Modifier
NDMP	ndmp_user	St0r@ge!	ndmp --setpassword
iSCSI	<Appliance Hostname>	St0r@ge!iscsi	iscsi--setpassword

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 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.

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.

20TB Total initial footprint with a 10% change rate

	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		

A.2.4 Media retention and grouping

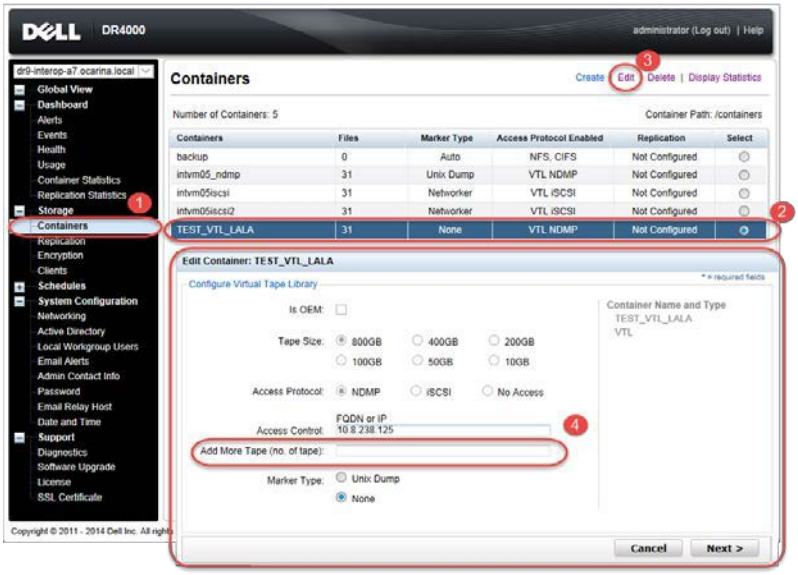
Due to the nature of Virtual Tape Libraries media must be managed in order to insure that physical capacity is reclaimed in an orderly fashion to avoid running out of space and disrupting operations. Media must be grouped within the data management application, such as NetVault Backup, in a way that 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

Type	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.



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

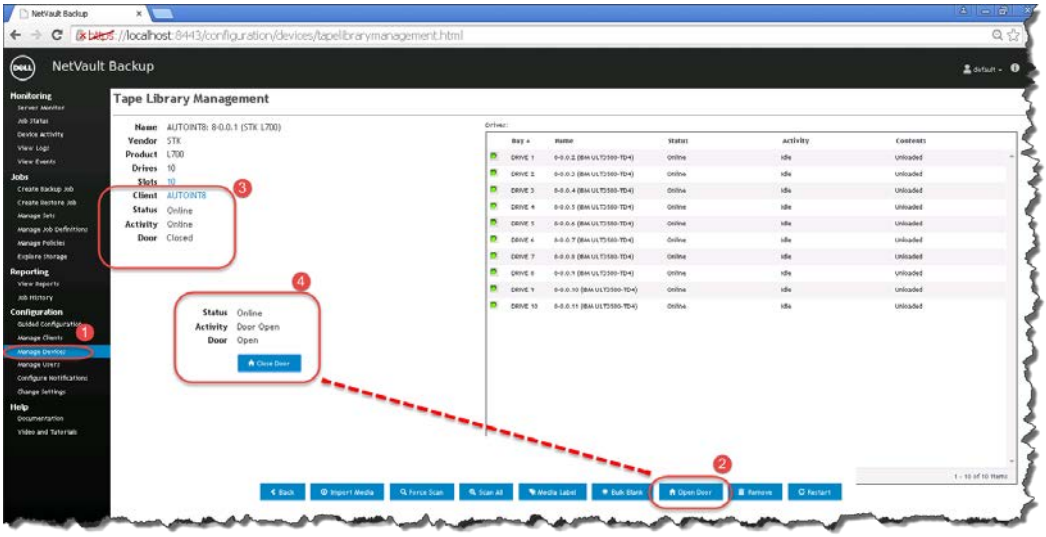
```
> vtl --create_carts --name TEST_VTL_LALA --tapes 10

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.



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.

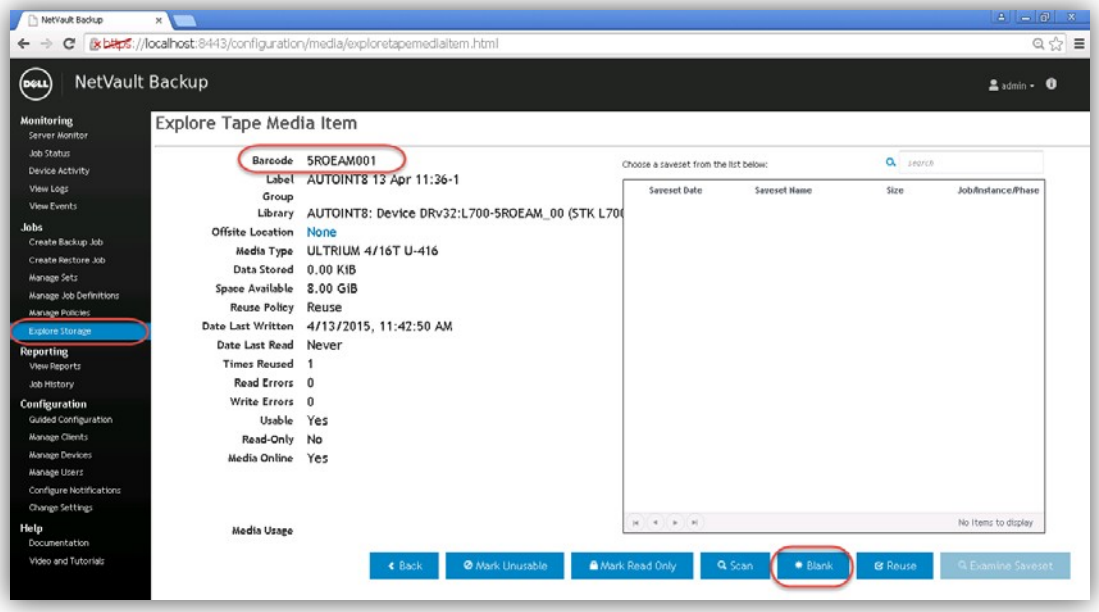
Product Specific Guidelines

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.

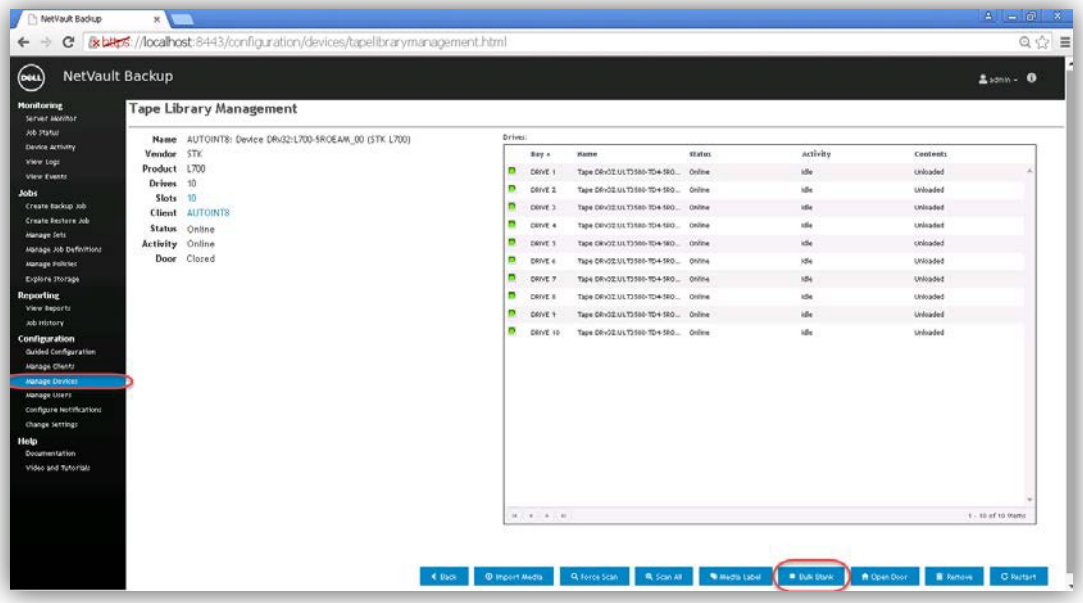
For Netvault Backup the following can be used when a situation dictates that space must be reclaimed manually.

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.



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



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:

```
> stats --system
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 %
```