

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

Technical White Paper

Quest Engineering

November 2017



© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

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

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. 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. Zmanda is a trademark of Zmanda Incorporated in the USA. All other trademarks and registered trademarks are property of their respective owners.

Legend

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Setting up the DR Series system for NetVault Backup

Updated – December 22, 2017

Contents

Installing and configuring the DR Series system	6
Configuring the DR Series system as an RDA repository	10
Creating an RDS container for NetVault: Backup	10
Adding a DR Series device and LSU container for use with NetVault: Backup.....	11
Configuring transport modes for NetVault: Backup	15
Example: Setting the mode by using the DR Series system CLI	15
Example: Setting the mode using the DR Series system GUI	16
Configuring the DR Series system as an FC VTL target for NetVault: Backup.....	17
Creating and configuring FC target container(s) for NetVault: Backup	17
General FC SAN infrastructure guidelines	17
Zoning and port mapping association example.....	18
Infrastructure prerequisites.....	19
Creating an FC VTL container for NetVault: Backup	22
Verifying initiators are connected to the FC VTL container for NetVault: Backup.....	23
Configuring NetVault: Backup to use the newly created FC VTL.....	25
Configuring the DR Series as a iSCSI VTL target for NetVault: Backup	34
Creating and configuring iSCSI target containers for NetVault: Backup.....	34
Verifying initiators are connected to the iSCSI VTL container for use with NetVault: Backup.....	35
Configuring NetVault: Backup to use the newly created iSCSI VTL – Automatic Library Detection.....	40
Configuring the DR Series as a NDMP VTL target for NetVault: Backup.....	44
Creating and configuring NDMP target containers for NetVault: Backup	44
Configuring the DR Series NDMP service with NetVault: Backup	45
Configuring NetVault: Backup to use the newly created NDMP VTL – Automatic Library Detection.....	46
Using VTL replication	50

Configuring the DR Series system for VTL replication	50
Restoring from a replica or replica cascade	53
Setting up the DR Series system cleaner	59
Monitoring deduplication, compression and performance	61
A - VTL configuration guidelines.....	62
Managing VTL protocol credentials	62
Setting the NDMP tape server credentials	62
Setting the iSCSI target CHAP credentials	62
Managing VTL Media	63
Adding additional media to the VTL container.....	63
Managing VTL space use	64
General performance guidelines for DMA configuration	64
Physical DR space sizing and planning	65
Logical VTL geometry and media size	65
Media retention and grouping.....	66
VTL media count guidelines	67
Space reclamation	67
General guidelines.....	67

Executive Summary

This white paper provides information about how to set up the DR Series system as a backup target for 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:

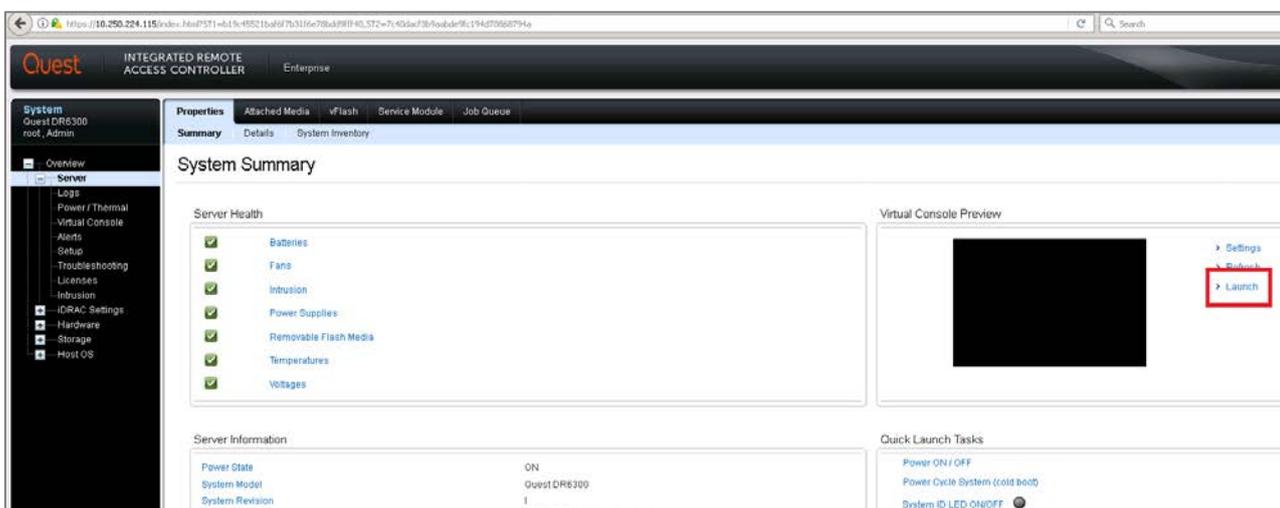
<http://support.quest.com/DR-Series>



NOTE: The DR Series system and NetVault: Backup screenshots used in this document might vary slightly, depending on the DR Series system firmware version and NetVault: Backup version you are using.

Installing and configuring the DR Series system

- 1 Rack and cable the DR Series system, and power it on. In the *Quest DR Series System Administrator Guide*, see the following sections for information about using the iDRAC connection and initializing the appliance.
 - “iDRAC Connection”,
 - “Logging in and Initializing the DR Series system”
 - “Accessing iDRAC6/iDRAC7 Using RACADM”
- 2 Log on to iDRAC using the default credentials (username: `root` and password: `calvin`) and either:
 - the default address `192.168.0.120`
 - or the IP address that is assigned to the iDRAC interface
- 3 Launch the virtual console.



- 4 After the virtual console opens, log on to the system (with the username: administrator and password: St0r@ge! where the "0" in the password is the numeral zero).

```
DR6300 release 4.0.3028.0
dr6300-45 login: administrator
Password: _
```



- 5 Set the user-defined networking preferences.

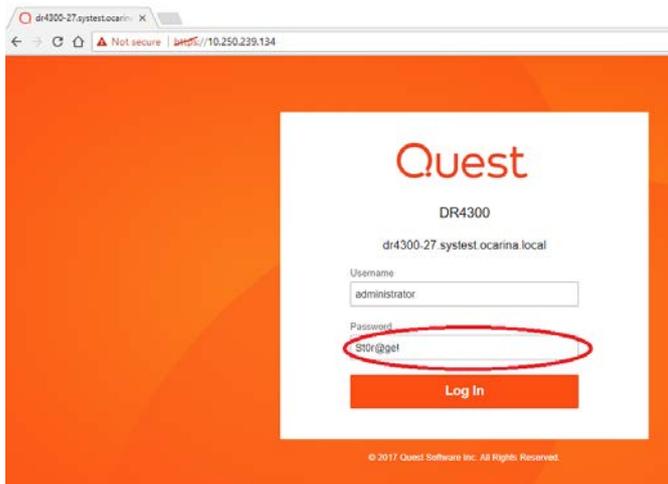
```
Would you like to use DHCP (yes/no) ?
Please enter an IP address:
Please enter a subnet mask:
Please enter a default gateway address:
Please enter a DNS Suffix (example: abc.com):
Please enter primary DNS server IP address:
Would you like to define a secondary DNS server (yes/no) ?
Please enter secondary DNS server IP address:
```

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

```
=====
                        Set Static IP Address
=====
IP Address           : 10.10.86.108
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

Are the above settings correct (yes/no) ? _
```

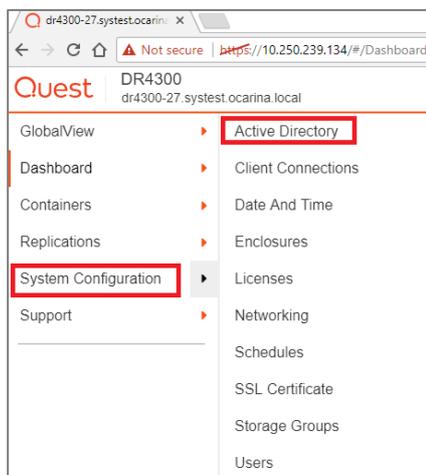
- 7 Log on to the DR Series system administrator console, using the IP address with username administrator and password St0r@ge! (The “0” in the password is the numeral zero.).



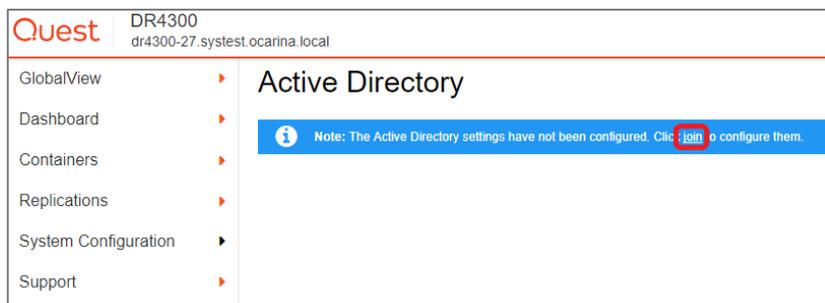
- 8 Join the DR Series system to Active Directory.

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 In the left navigation area of the DR Series system GUI, click **System Configuration** and then select **Active Directory**.



- b Click **Join**.



c Enter valid credentials and click **Join**.

The screenshot shows the Quest Active Directory configuration interface. The top header includes the Quest logo and system information: DR4300 and dr4300-27.systest.ocarina.local. A left-hand navigation menu lists: GlobalView, Dashboard, Containers, Replications, System Configuration, and Support. The main content area is titled 'Active Directory' and contains a 'Join' dialog. This dialog has four input fields: 'Domain Name (FQDN)' (Required), 'Username' (Required), 'Password' (Required), and 'Org Unit'. At the bottom of the dialog are two buttons: 'Join' (highlighted with a red box) and 'Cancel'.

Configuring the DR Series system as an RDA repository

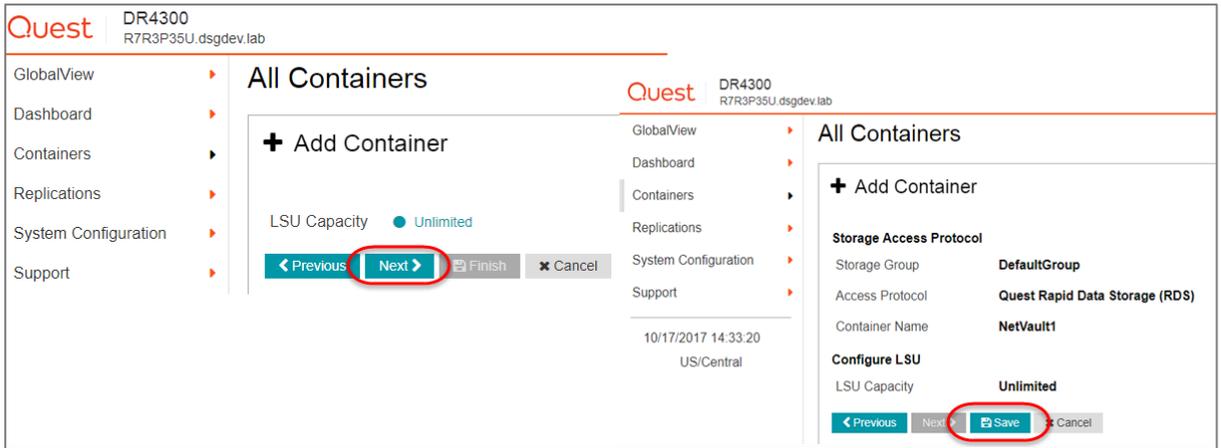
Creating an RDS container for NetVault: Backup

i **NOTE:** Storage Groups are managed under the DR Series System Configuration. Refer to the *DR Series System Administrator Guide* for details about Storage Groups.

- 1 Do the following:
 - a Select Containers in the left navigation area of the DR Series system GUI ①.
 - b On the Action Menu in the upper right corner, click the **Add Container** option ②.
 - c Select the **Storage Group** ③.
 - d Select **RDS** from the Access Protocol drop down menu ④.
 - e Enter a name for the container ⑤ and click the **Next** button ⑥.

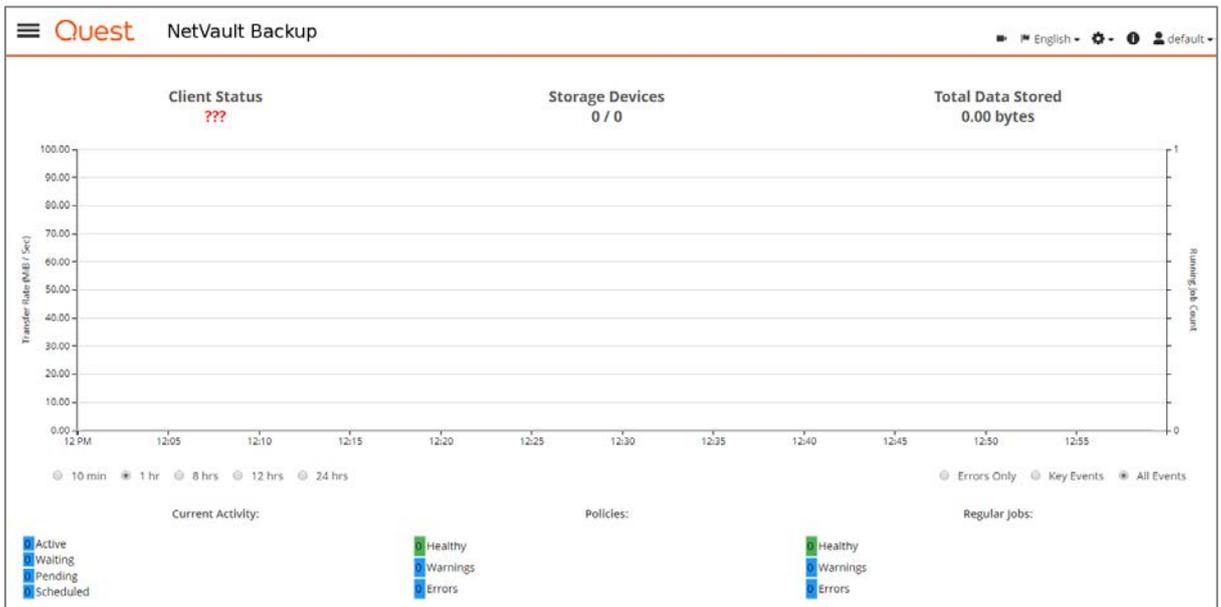
The screenshot shows the Quest DR Series System GUI. The left navigation menu has 'Containers' selected (1). The main area is titled 'All Containers' and contains an 'Add Container' form. The form has the following fields: 'Storage Group' (3) set to 'DefaultGroup', 'Access Protocol' (4) set to 'Quest Rapid Data Storage (RDS)', and 'Container Name' (5) set to 'NetVault1'. A 'Next' button (6) is highlighted. The top right corner shows the user 'administrator' and a 'Log Out' button.

- 2 Click **Next** and then click **Save** to complete container creation.



Adding a DR Series device and LSU container for use with NetVault: Backup

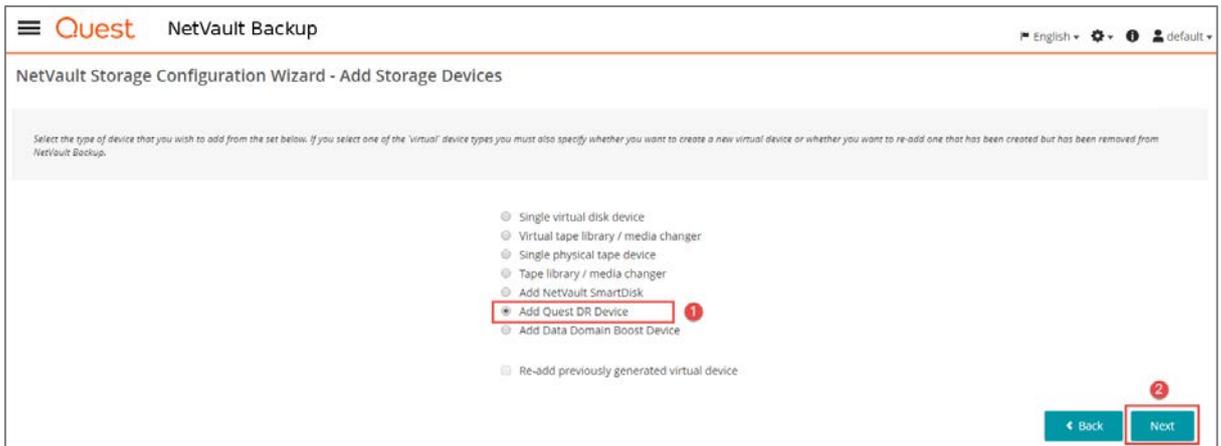
- 1 Open the NetVault: Backup Web Console.



- 2 Add the RDA container to NetVault: Backup by opening the menu drawer (1) and selecting the Manage Devices wizard (2).

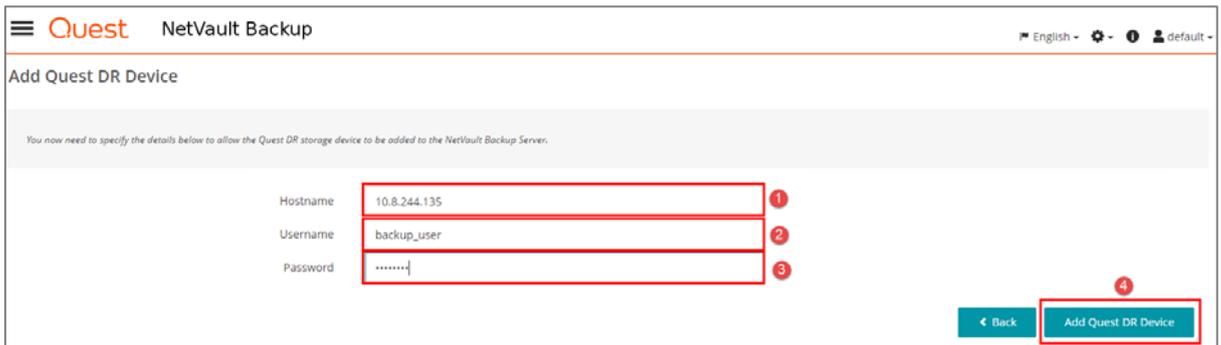
3 Click the **Add Device** button.

- 4 Click **Add Quest DR Device** ❶ and click the **Next** button ❷.

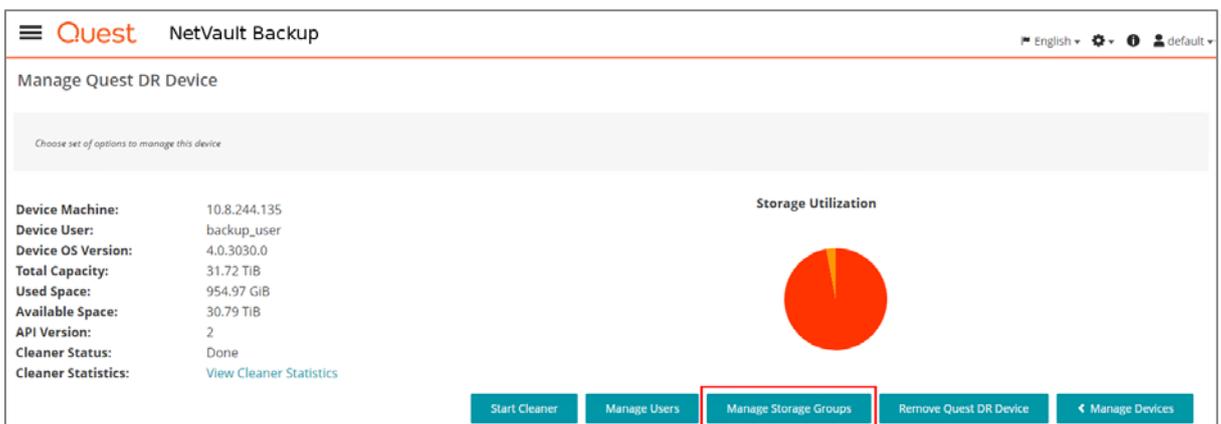


- 5 Do the following:
 - a Specify the IP Address or FQDN (resolvable) of the DR Device ❶.
 - b Enter the RDA Username ❷ and Password ❸.
 - c Select the **Add Quest DR Device** button ❹ in the bottom right corner.

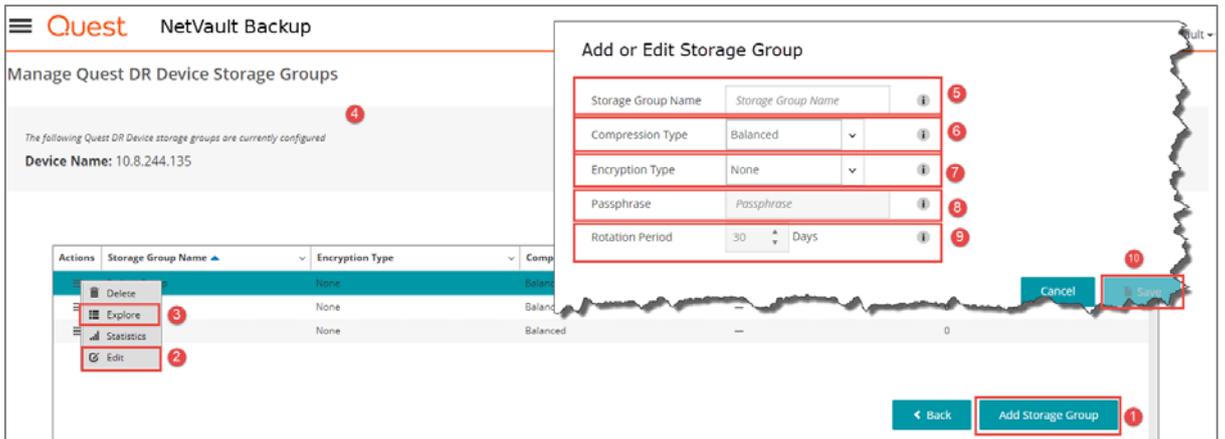
i **NOTE:** The default username is `backup_user` and the password is `St0r@gE!` (The “0” in the password is the numeral zero). The suggested Block Size is 524288 bytes (512KB) to achieve optimal performance. Also, the Stream Limit required.



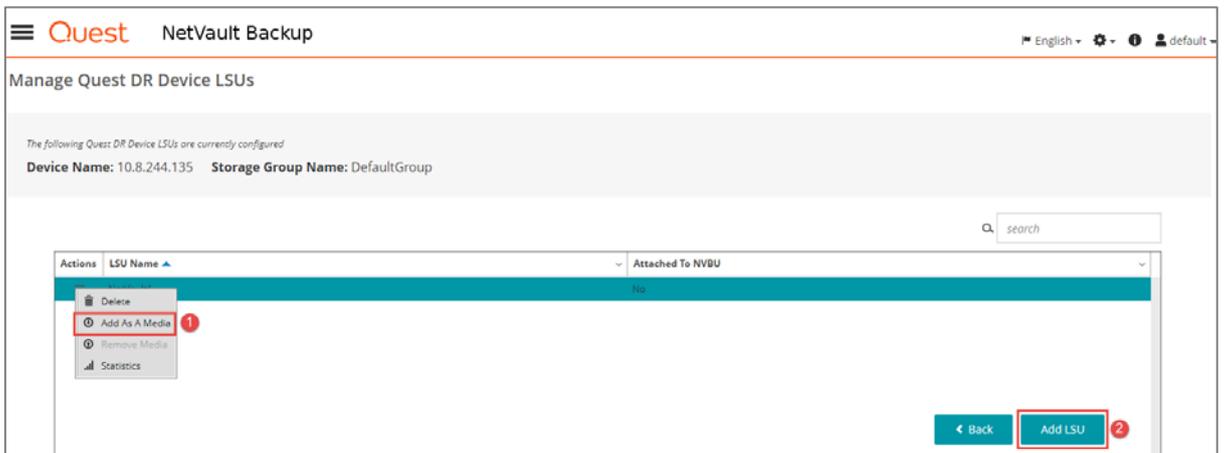
- 6 After the DR Series system has been added, proceed to **Manage Storage Groups**.



- 7 Do the following:
 - a Select to add a storage group ①, modify ② an existing storage group or manage and explore an existing storage group ③ for the respective DR Device ④.
 - b If selecting to add or modify an existing Storage Group proceed by specifying the Name ⑤, Compression Type ⑥, Encryption Type ⑦, Encryption Paraphrase ⑧ and Rotation Period ⑨. For specific details on each of these features, refer to the *DR Series System Administrators Guide* or the *NetVault: Backup Administrators Guide*.



- 8 To add a Container LSU for NetVault: Backup operations, select the appropriate Storage Group and click **Explore**.
- 9 Proceed to Add an existing container LSU as Media ① or adding a new Container LSU altogether by selecting the Add LSU Button ②.



- 10 If adding a new Container LSU, specify the Container name ❶ and select to save the workflow ❷. Otherwise, select the Container LSU and click to **Add As A Media**. Proceed by specifying the Block Size ❸ and Stream Limit ❹. Use the force add ❺ option if this Container LSU had been previously added and not removed properly. Finally, select the **Add As A Media** button to complete the workflow ❻.

The screenshot shows a two-part GUI. The top part, titled 'Add LSU', has a text field for 'Add LSU Name' containing 'NetVault2', a 'Cancel' button, and a 'Save' button. The bottom part, titled 'Add As A Media', shows 'LSU: NetVault1', a 'Block Size (in KiB): 512' field, a 'Stream Limit: 256' field, a 'Force Add' checkbox, a 'Cancel' button, and an 'Add As A Media' button. Red boxes and numbers 1-6 highlight these elements: 1 (text input), 2 (Save button), 3 (Block Size input), 4 (Stream Limit input), 5 (Force Add checkbox), and 6 (Add As A Media button).

- 11 You can now proceed to use the DR Series system container by configuring new target sets accordingly.

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, proceed by setting the RDA mode in the DR Series system command prompt or through the GUI.

Example: Setting the mode by using the DR Series system CLI

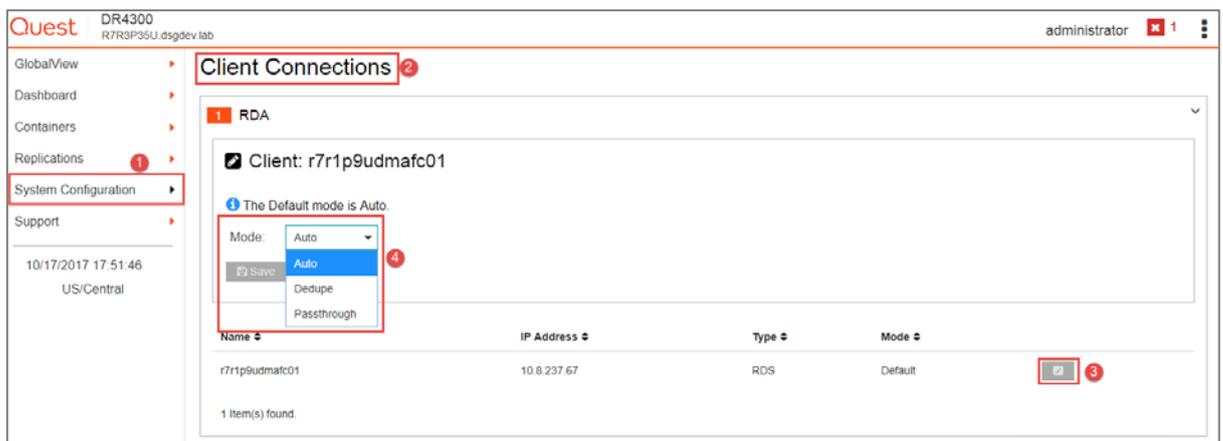
Open an ssh session to the DR Series system and run the following command:

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

Example: Setting the mode using the DR Series system GUI

In the DR Series system GUI, follow these steps:

- 1 Navigate to the System Configuration **1** >> Client Connections **2** Page. The list of clients that have active connections is shown.
- 2 Select the client for which you want to change the mode and modify **3**.
- 3 Select the required mode from the drop down menu, and click Submit **4**.



Configuring the DR Series system as an FC VTL target for NetVault: Backup

Creating and configuring FC target container(s) for NetVault: Backup

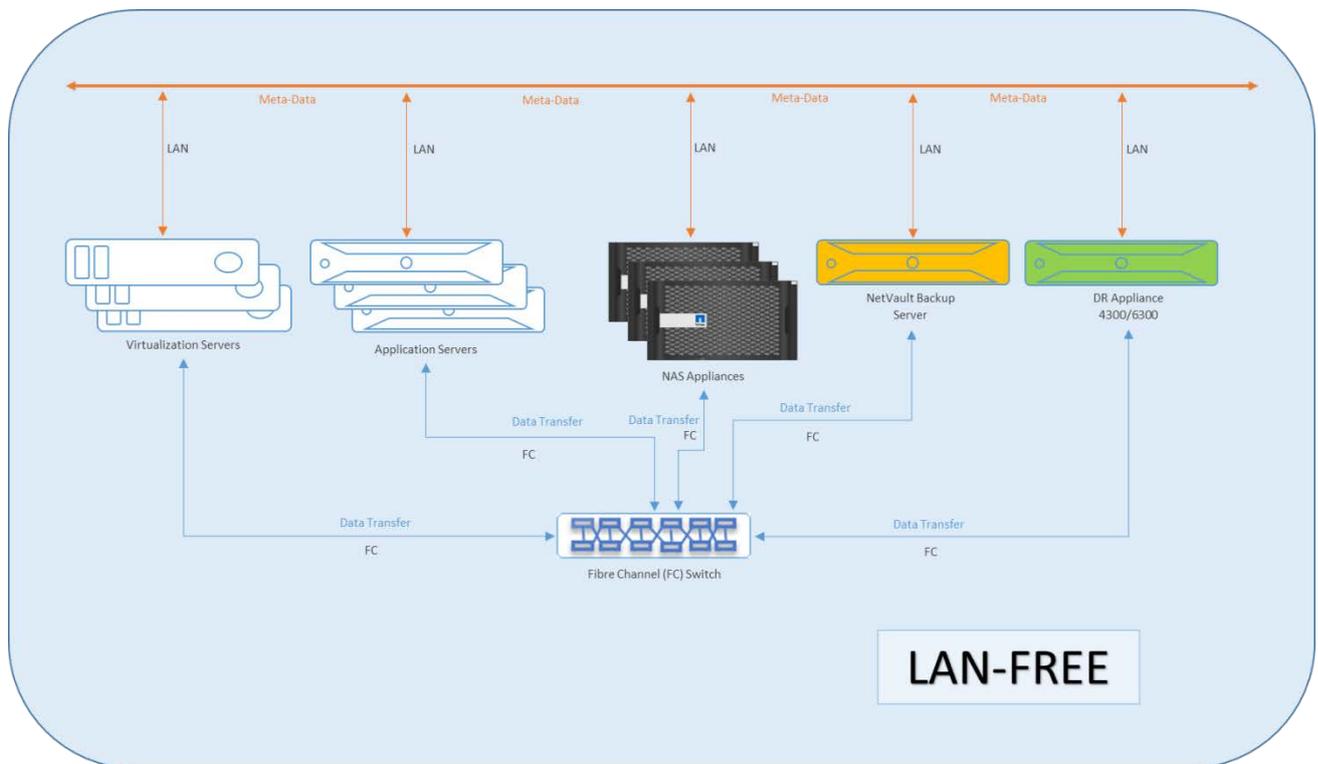
General FC SAN infrastructure guidelines

- Disk and Tape devices are recommended not to be on the same Fibre Channel HBAs. Disk and Tape IO should be isolated at all times as the nature of their IO patterns do not mix well. Disk and Tape zones should not share devices.
- Disable SCSI Bus Reset to tape devices, whenever possible.
- Enable PLOGI instead of PDISC after LIP.
- NetVault: Backup does not support native load balanced multi-pathing or HA features.
- Zoning guidelines should include isolating tape traffic:
 - Use WWPN Zoning for target and initiator ports.
 - Add individual pairs of initiator and DR Target Ports per zone.
 - The DR Target Ports should reside in multiple Initiator Zones so that Initiators are isolated from one another.
 - This will help isolate FC infrastructure disruption from one node to impact the operation of another during normal operations.
 - Configure the individual initiator ports per node evenly across target ports so as to maximize performance by spreading the IO across DR Target Ports if possible.

- Persistent Binding allows devices to be persistent across power-cycles, reboots and SAN HW changes. Persistent Binding settings should be used throughout the Storage Area Network Configuration particularly those involved with the NetVault: Backup software such as changer and tape drive LUNs.
- Device Aliases should be set up so that the devices are easily identifiable and are persistent through power outages and reboots. Refer to your HBA manufacturer for details.

Zoning and port mapping association example

The following graphic shows a LAN-Free Zoning example that includes a NetVault: Backup Server and a NAS Filer Cluster with two nodes configured to share a DR FC VTL. Infrastructure Details:



Backup Server:

WWN Initiator Port 1: 20:01:00:0e:1e:d1:d5:6a

WWN Initiator Port 2: 20:01:00:0e:1e:d1:d5:6b

NAS Node 1:

WWN Initiator Port 1: 50:0a:09:83:06:8f:54:40

WWN Initiator Port 2: 50:0a:09:82:06:8f:54:40

NAS Node 2:

WWN Initiator Port 1: 50:0a:09:82:06:8d:c6:c1

WWN Initiator Port 2: 50:0a:09:83:06:8d:c6:c1

DR Series Appliance:

WWN Target Port 1: 50:00:65:b7:86:93:42:24

WWN Target Port 2: 50:00:65:b7:86:93:42:25

Example: Initiator to Target Port Zone Summary

		DR Series Appliance WWN Target Port 1	DR Series Appliance WWN Target Port 2
Zone A	Backup Server	20:01:00:0e:1e:d1:d5:6a	20:01:00:0e:1e:d1:d5:6a
	WWN Initiator Port 1	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25
Zone B	Backup Server	20:01:00:0e:1e:d1:d5:6b	20:01:00:0e:1e:d1:d5:6b
	WWN Initiator Port 2	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25
Zone C	NAS Node 1	50:0a:09:83:06:8f:54:40	50:0a:09:83:06:8f:54:40
	WWN Initiator Port 1	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25
Zone D	NAS Node 1	50:0a:09:82:06:8f:54:40	50:0a:09:82:06:8f:54:40
	WWN Initiator Port 2	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25
Zone E	NAS Node 2	50:0a:09:82:06:8d:c6:c1	50:0a:09:82:06:8d:c6:c1
	WWN Initiator Port 1	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25
Zone F	NAS Node 2	50:0a:09:83:06:8d:c6:c1	50:0a:09:83:06:8d:c6:c1
	WWN Initiator Port 2	50:00:65:b7:86:93:42:24	50:00:65:b7:86:93:42:25

Infrastructure prerequisites

Netapp filer configuration

To ensure that SCSI command processing is not interrupted, the NetApp Filer(s) should be configured such that they do not use any SCSI reservations. In addition, to use the multi-pathing configuration, all NetApp Filer Nodes in a C-Mode cluster that will share VTL tape devices are to be configured with Storage Tape Load-Balancing settings enabled.

- SVM Mode Settings
 - Disable SCSI Reservations.

```
>options -option-name tape.reservations -option-value off
```

- Enable Load Balancing:

```
>storage tape load-balance modify -node * true
```

Due to the nature of SCSI command processing workflows the default SCSI command timeout should be changed. Specifically the IBM ULT3580 TD4 tape configuration files should be setup with the recommended SCSI command timeouts listed below:

```
cmd_timeout_0x00=5m
```

```
cmd_timeout_0x12=5m
```

```
cmd_timeout_0x15=5m
```

```
cmd_timeout_0x1A=5m
```

```
cmd_timeout_0xA0=5m
```

```
cmd_timeout_0x34=5m
```

- Setup the tape configuration files to use the above mentioned timeout values:

```
>run -node * -command wrfile /etc/tape_config/IBM_LTO4_ULT3580.TCF
```

- For each filer node prompted enter the following (Note: Control-C to end editing)

```
# Configuration file for IBM tape drive IBM LTO Gen4 AKA ULT3580-  
TD4
```

```
# Version 1.1
```

```
# Copyright (c) 2008 NetApp
```

```
# All rights reserved.
```

```
vendor_id="IBM"
```

```
product_id="ULT3580-TD4"
```

```
id_match_size=11
```

```
vendor_pretty="IBM"
```

```
product_pretty="LTO 4 ULT3580"
```

```
l_description="LTO 2 ro 200GB cmp"
```

```
l_density=0x00
```

```
l_algorithm=0x01
```

```
m_description="LTO 3 800GB cmp"
```

```
m_density=0x00
```

```
m_algorithm=0x01
```

```
h_description="LTO 4 800GB"
```

```
h_density=0x46
```

```
h_algorithm=0x00
```

```
a_description="LTO 4 1600GB cmp"
```

```
a_density=0x46
```

```
a_algorithm=0x01
```

```
autoload="yes"
```

```
cmd_timeout_0x12=5m
```

```
cmd_timeout_0x15=5m
```

```
cmd_timeout_0x1A=5m
```

```
cmd_timeout_0xA0=5m
```

```
cmd_timeout_0x34=5m
```

- Verify the tape configuration files to use the above mentioned timeout values:

```
>run -node * -command rdfile /etc/tape_config/IBM_LTO4_ULT3580.TCF
```

See the following NetApp Reference, *How to add lines to a configuration file on the storage system using wrfile*, at:

https://kb.netapp.com/support/s/article/how-to-add-lines-to-a-configuration-file-on-the-storage-system-using-wrfile-the-command-wrfile-does-not-have-an-option-to-exit-without-saving?language=en_US

Windows configuration

Sun/StorageTek Library Driver Requirements: Refer to the article at:

<http://catalog.update.microsoft.com/v7/site/home.aspx> for information about acquiring Microsoft Device Drivers, for example, StorageTek Library Drivers

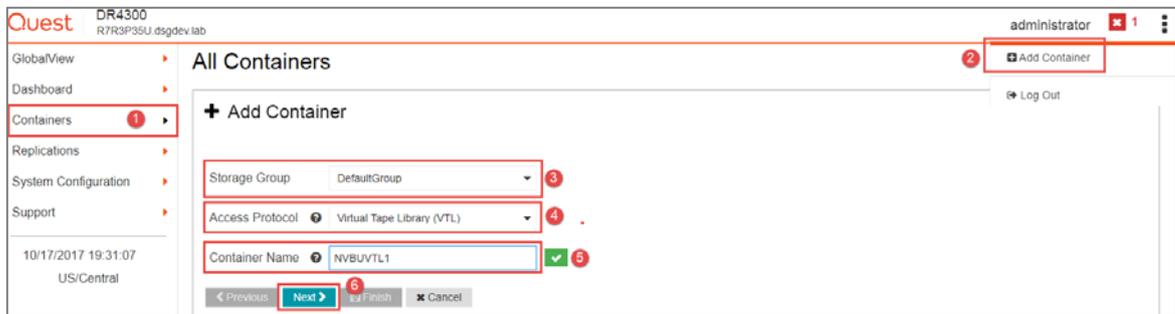
IBM Tape Drive Driver Requirements: When using the IBM device drivers ensure that the following requirements are met:

- Driver is installed in **Non-Exclusive** mode

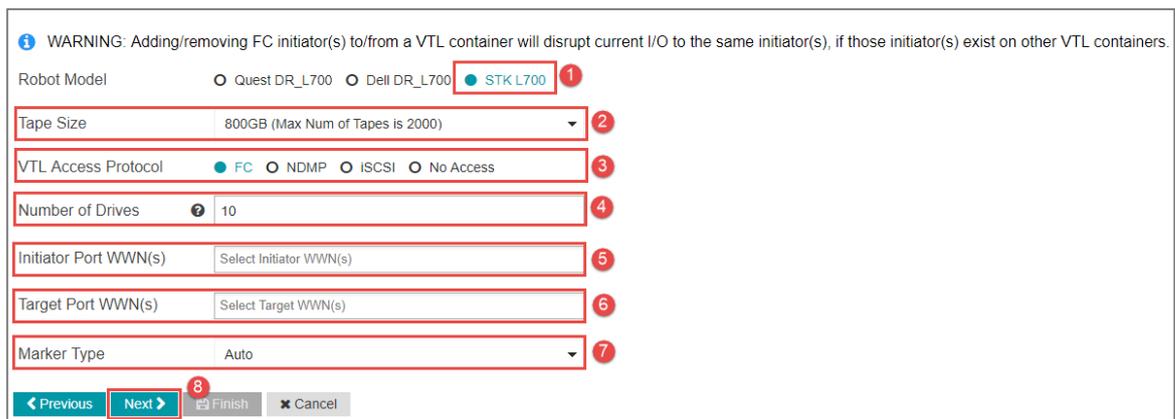
- DPF (Data Path Failover) is **Disabled**
- Persistent Reservations are **Disabled**
- Media Polling is **Disabled**

Creating an FC VTL container for NetVault: Backup

- 1 Select Containers in the left navigation area of the DR Series system GUI (1), and then select the Action Menu in the upper right corner. Click the Add Container option at the top of the menu (2). Enter a Container Name (3), and select **Virtual Tape Library (VTL)** from the Access Protocol drop down menu (4). Provide a name for the container (5) then click next (6).



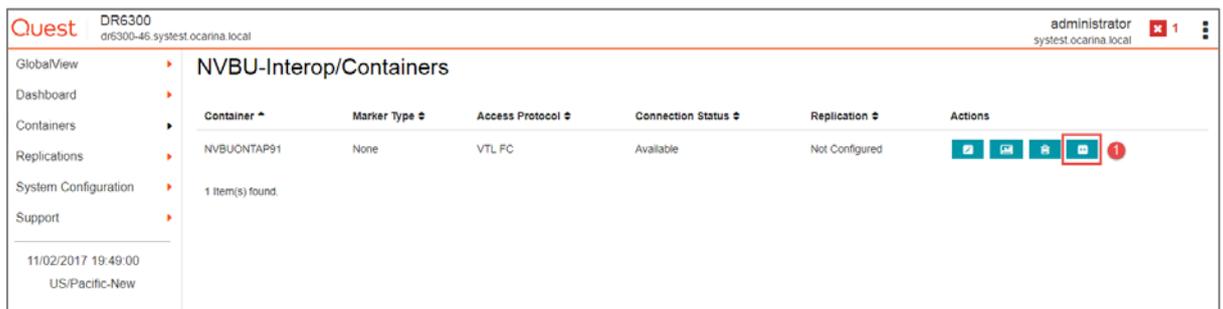
- 2 When prompted, select the **STK L700** Robot Model (1). Select the Tape Size (2), the **FC** VTL Access Protocol (3) and number of drives (4). Designate the Initiator Port WWN(s) Access Control by selecting the FC Initiator WWPN of the NetVault: Backup Server, respective Smart Clients or NAS Filer Appliance Nodes as needed (5) which are to be configured to share the Virtual Tape Library and drives. Select the Target Ports WWN(s) (6) for those ports on the DR Appliance that are configured for Initiator access. For NetVault, you must also specify **Auto** (7) as the Marker Type. Click Next (8).



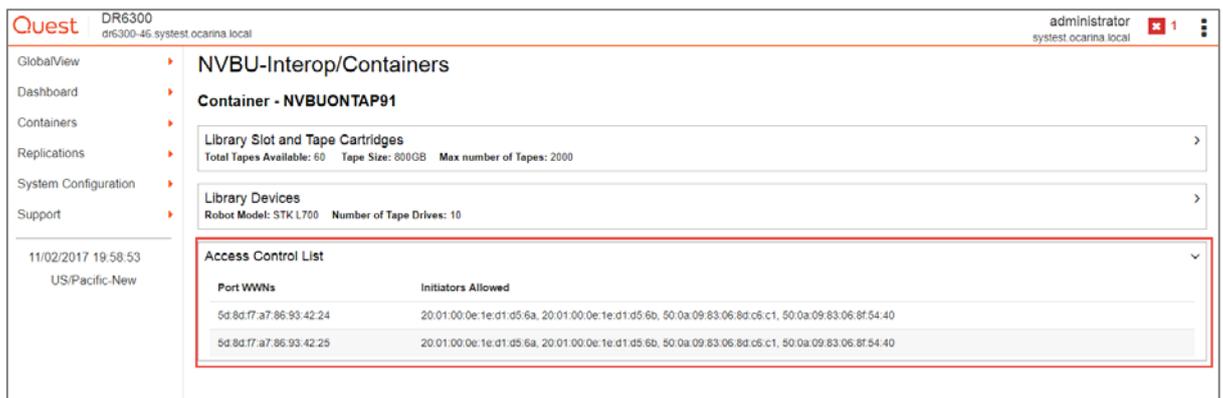
- 3 Finalize VTL creation by clicking **Save**.

Verifying initiators are connected to the FC VTL container for NetVault: Backup

- 1 Navigate to the appropriate Storage Group and select to view the VTL container details **1** to verify that all Initiators have connected and established a FC session with the DR Appliance. Select Containers in the left navigation area, and then click Container Details at the right of the page.

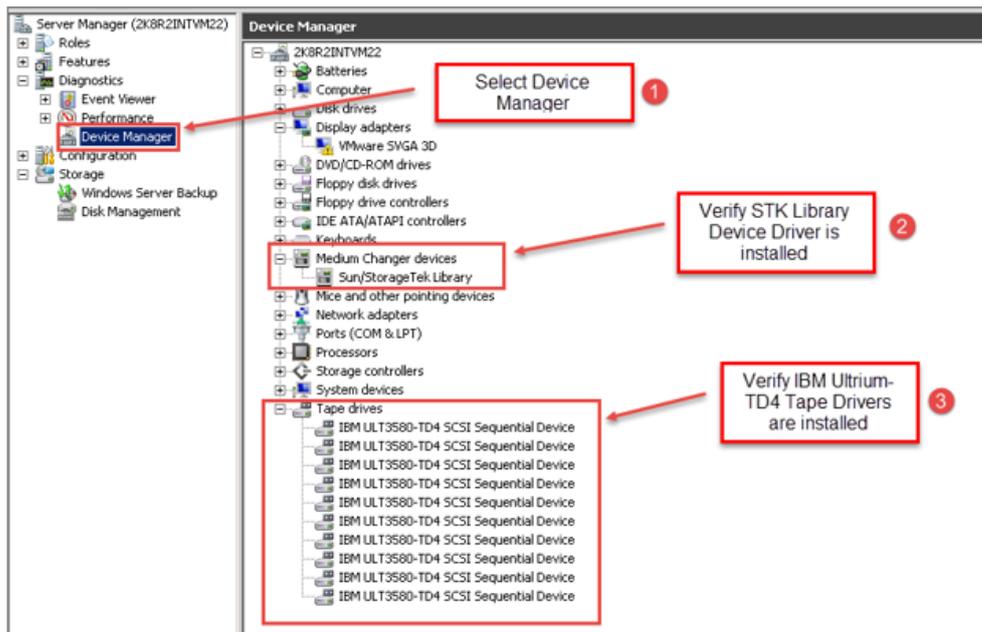


- 2 Verify that all the intended Initiators appear and reflect as having established sessions with the DR FC Target Ports.



Verifying connectivity to the FC target – Windows

- 1 Configure the FC Initiator Software for Windows by installing and configuring your FC HBA drivers and related persistent binding.
- 2 Open the Server Manager Snap-in and verify that the newly connected devices show up in the Device Manager.
- 3 Verify the STK Library and IBM Ultrium-TD4 Device Drivers are installed.



Verifying connectivity to the FC target – Linux

- 1 Configure the FC Initiator Software for Linux by providing installing and configuring your FC HBA drivers and related persistent binding.
- 2 Run the `lsscsi` command.
- 3 Verify that the STK Library and IBM Ultrium-TD4 Device Drivers are installed.

Verifying connectivity to the FC target – NetApp ONTAP 9

- 1 Login to the Linux Client as root and run the following commands:

```
>storage tape show
```

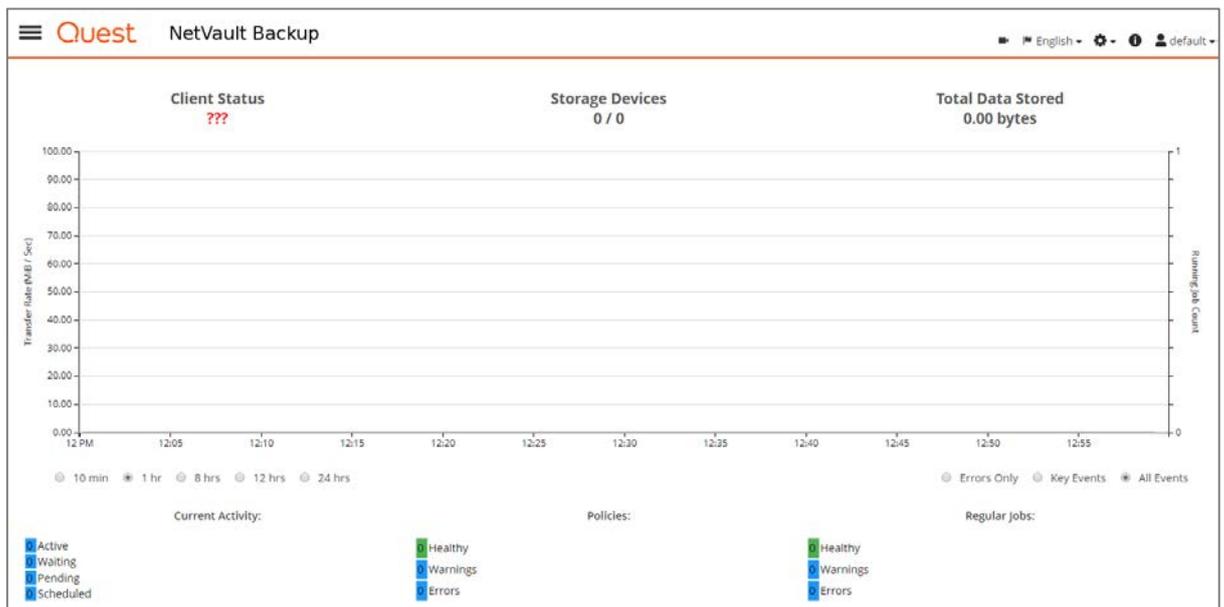
```
>storage library config show
```

- 2 Verify that all VTL LUNs are recognized.

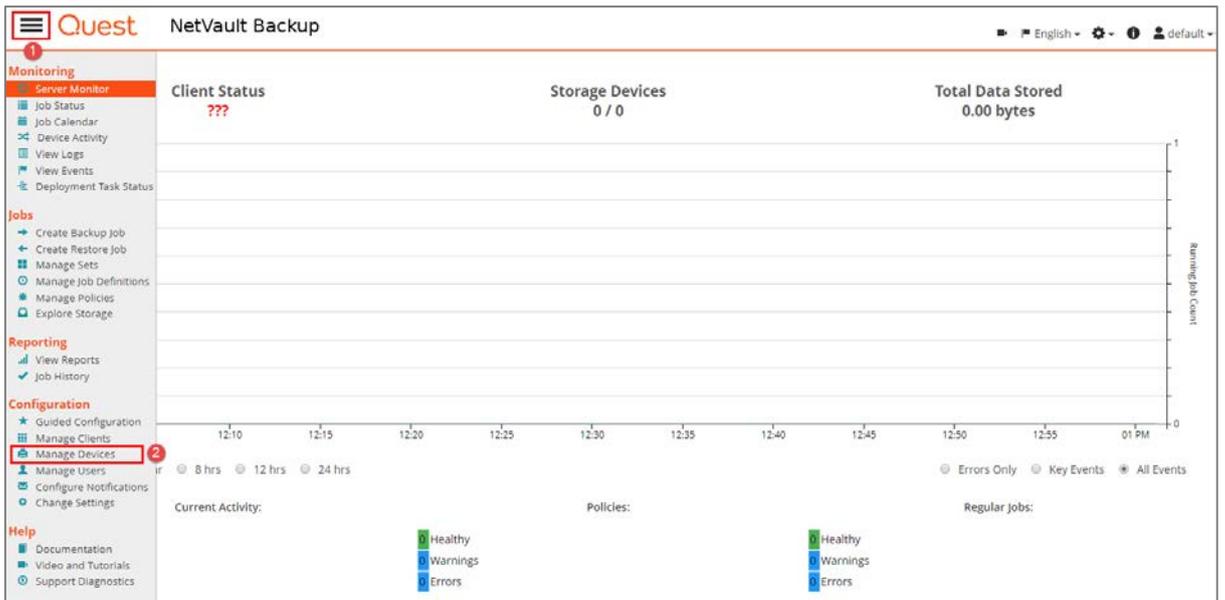
Configuring NetVault: Backup to use the newly created FC VTL

Configuring NetVault: Backup to use the newly created FC VTL Automatic Library Detection – Single Initiator

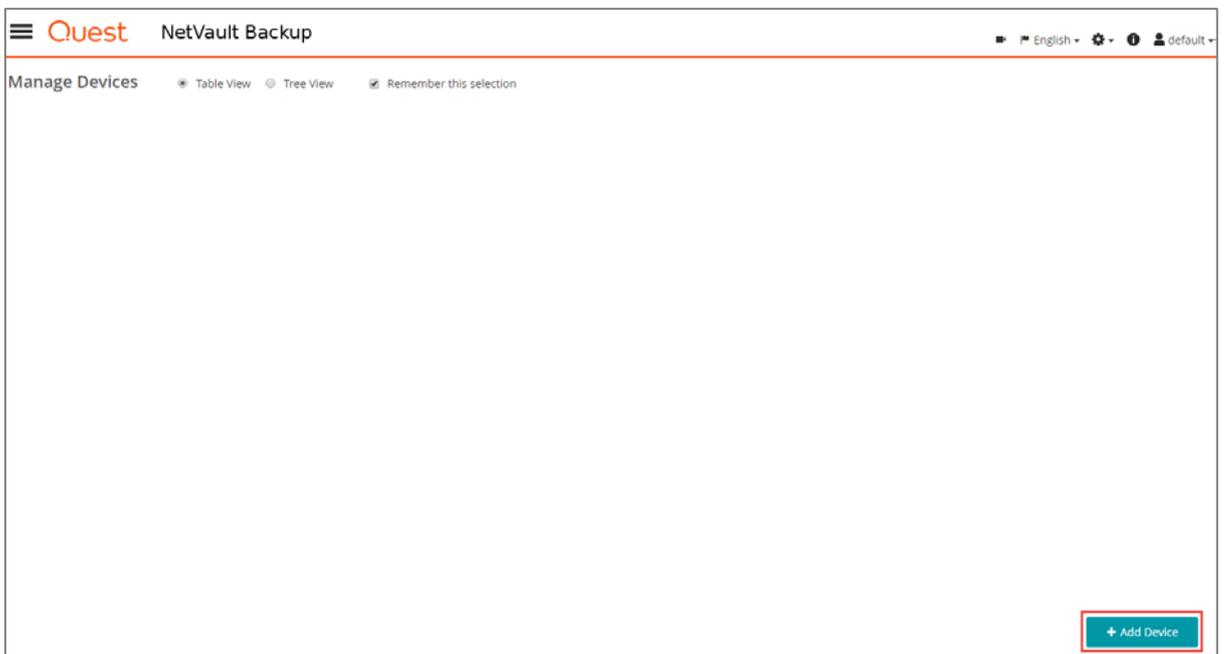
- 1 Open the NetVault: Backup Web Console.



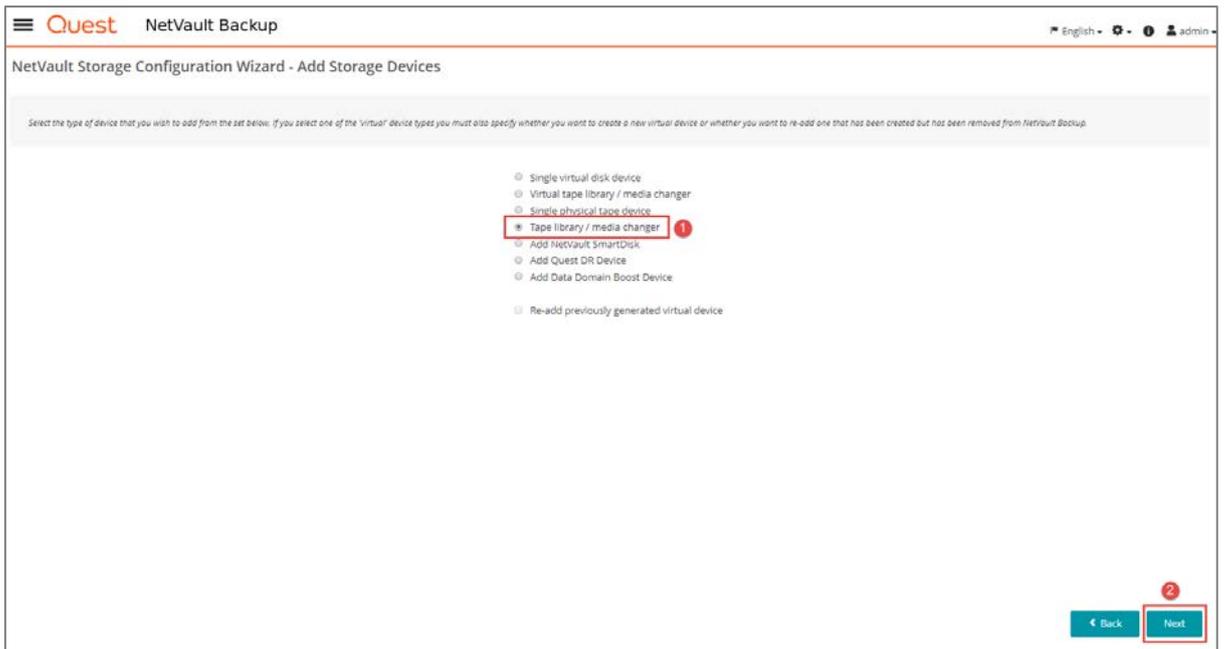
- 2 Add the DR VTL container to NetVault: Backup by opening the menu drawer ❶ and selecting the Manage Devices wizard ❷.



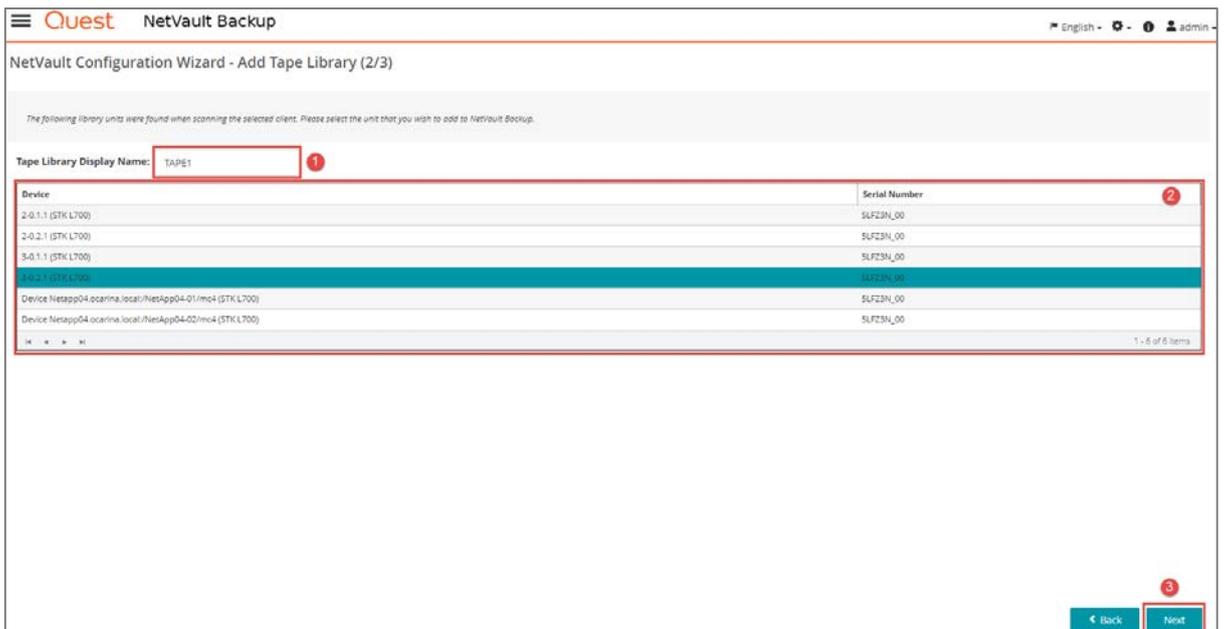
3 Click the **Add Device** button.



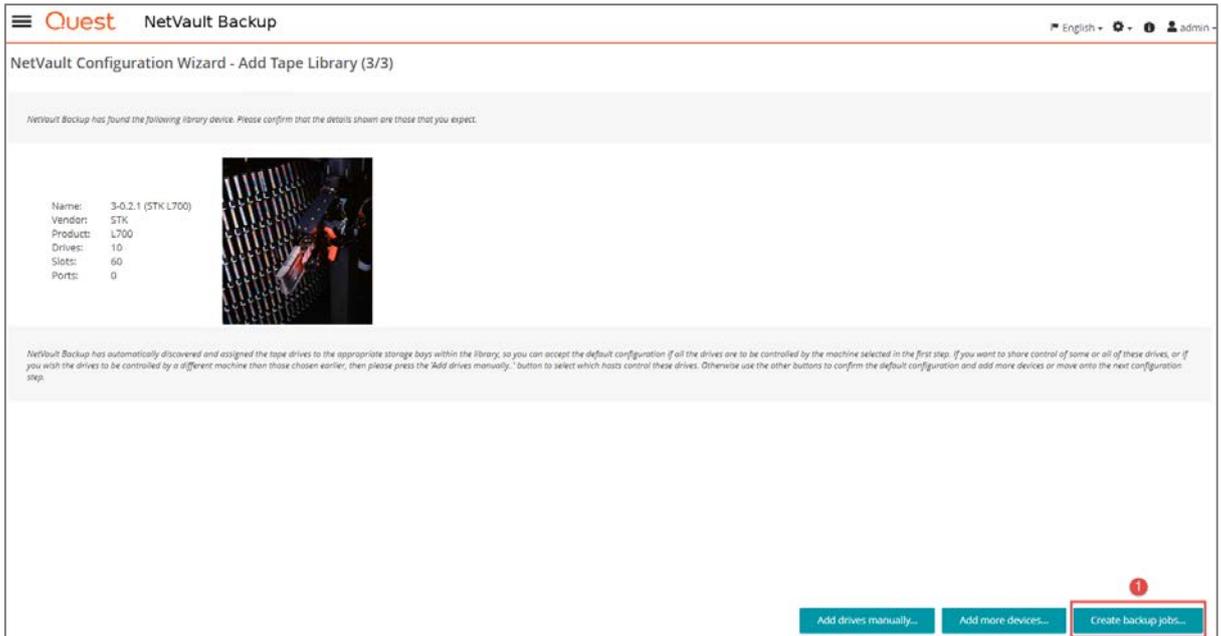
4 Select the Add Tape Library/ media changer ❶ and click the **Next** button ❷.



- 5 Provide a name for the VTL ①, select the VTL changer path intended to control the changer LUN ② and then click **Next** on the lower right ③,

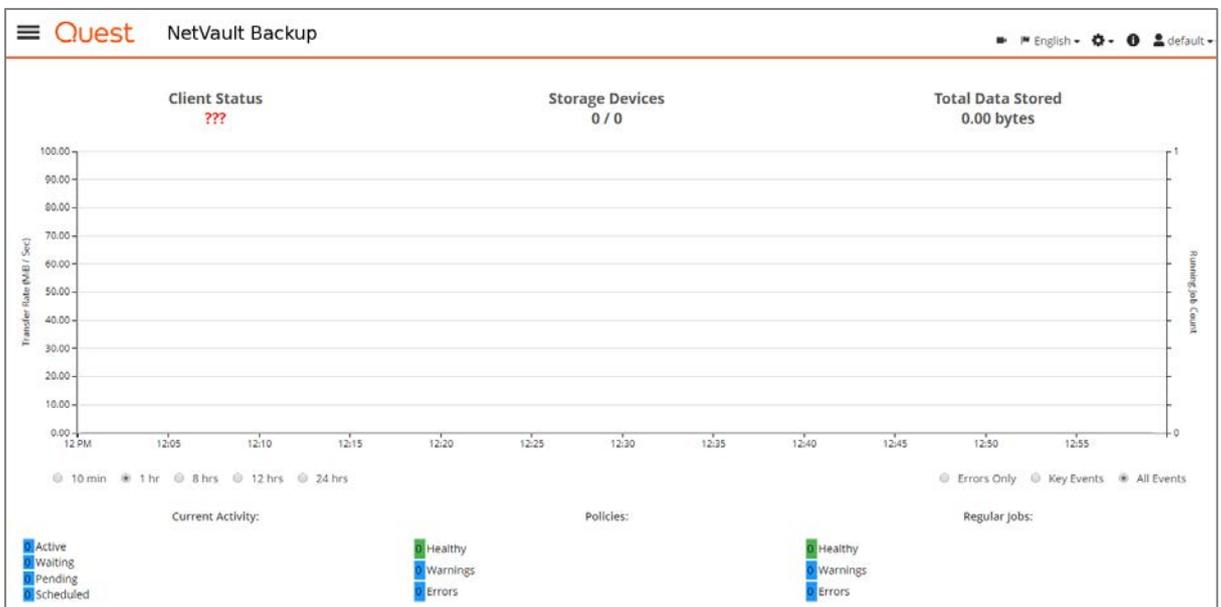


- 6 When the tape library scan is complete, click the **Create Backup job** ① button to commit the library. The VTL should show up ready for use.

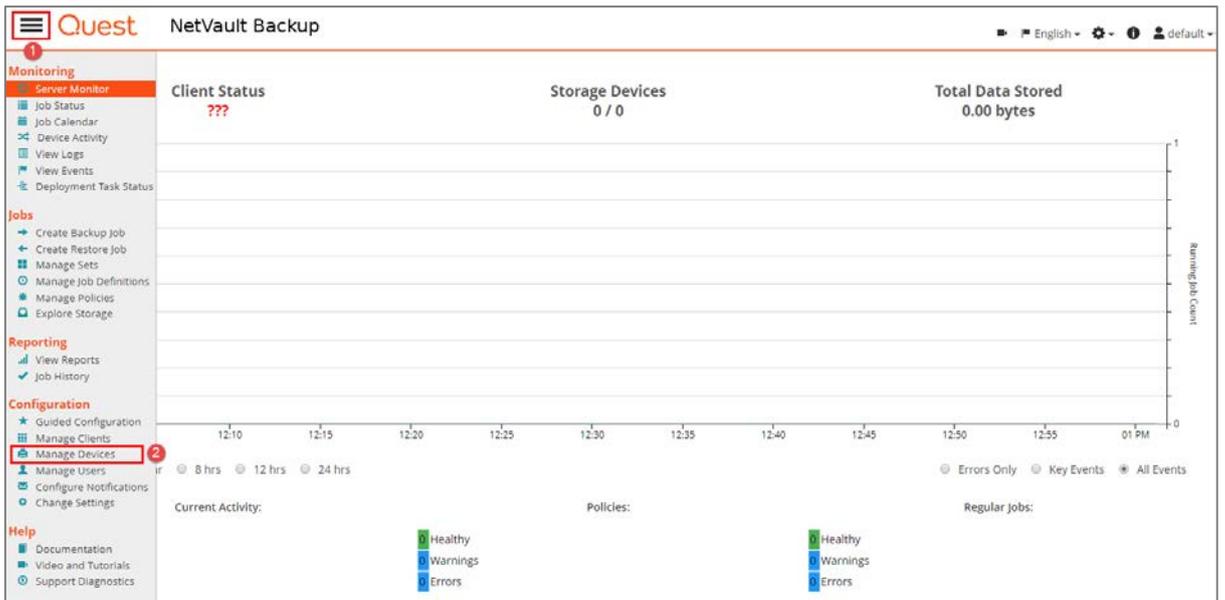


Configuring NetVault: Backup to use the newly created FC VTL Automatic Library Detection – Multi-Initiator / LAN-Free

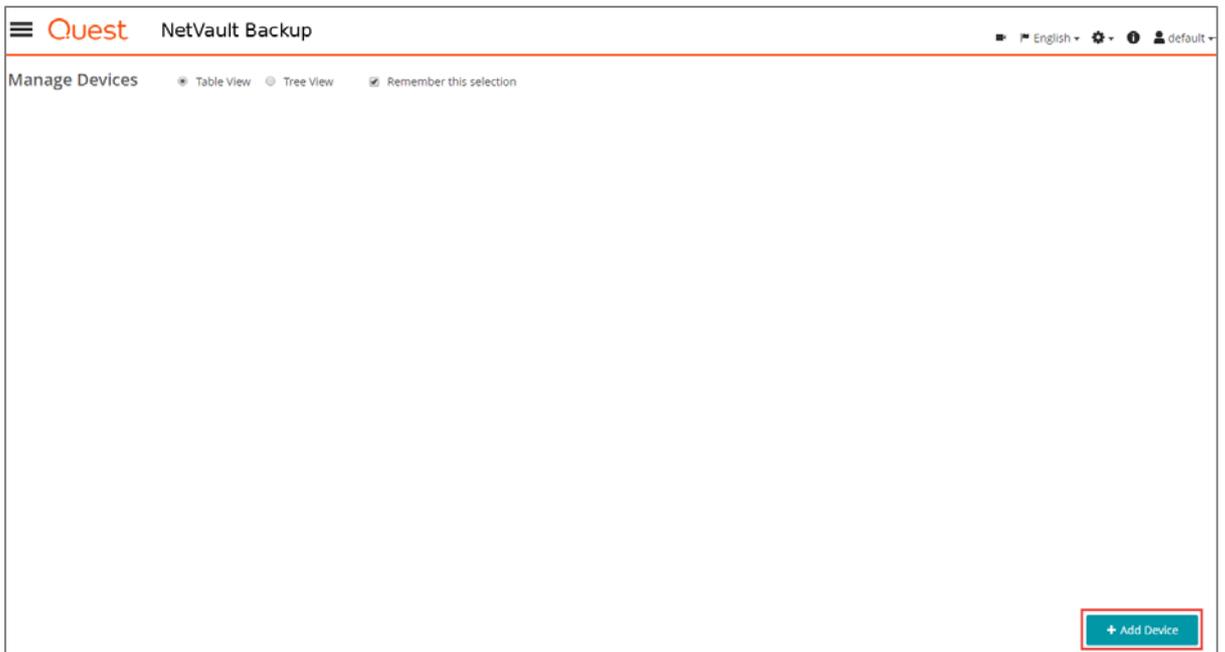
- 1 Open the NetVault: Backup Web Console.



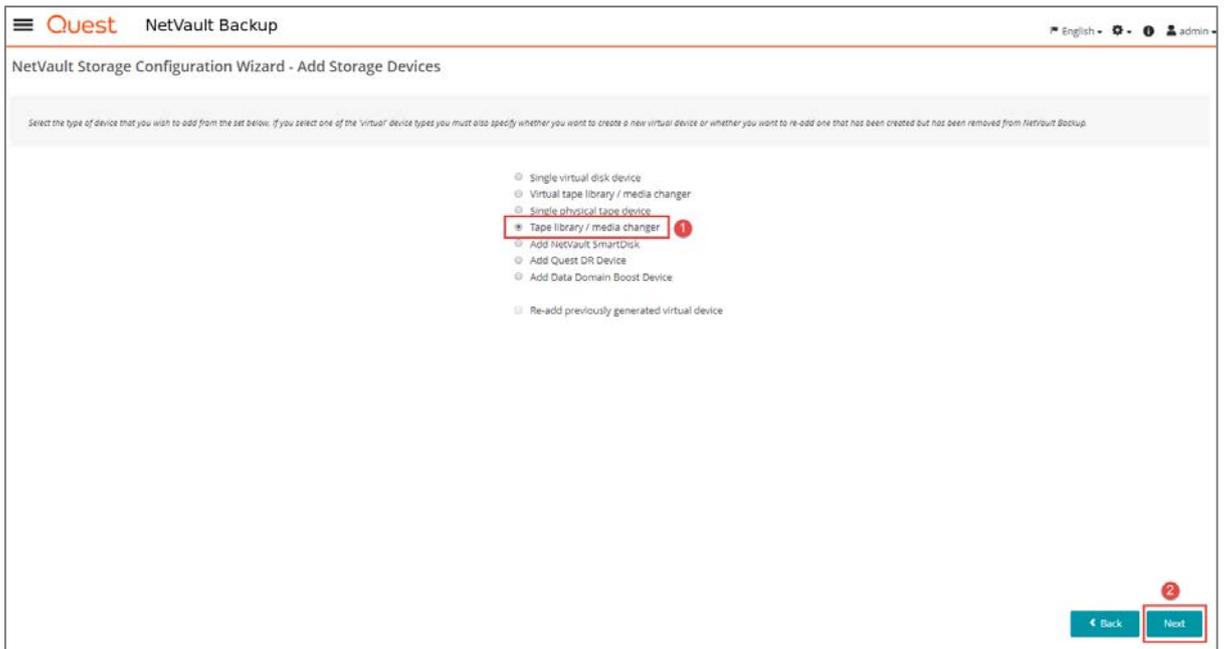
- 2 Add the DR VTL container to NetVault: Backup by opening the menu drawer ① and selecting the Manage Devices wizard ②.



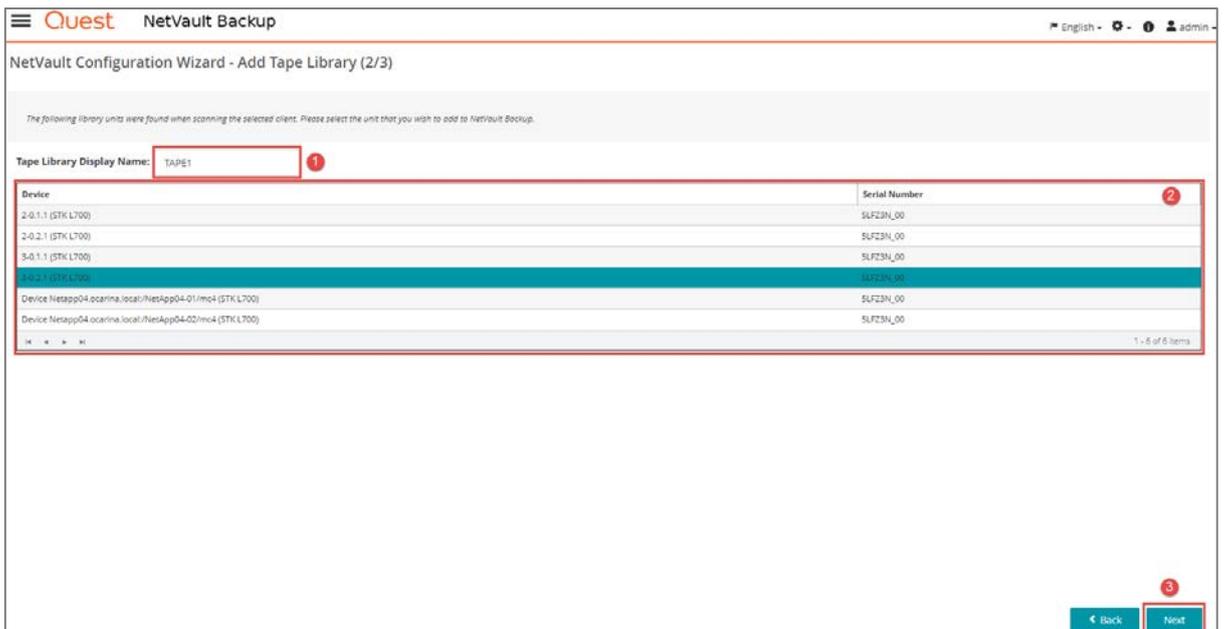
3 Click the **Add Device** button.



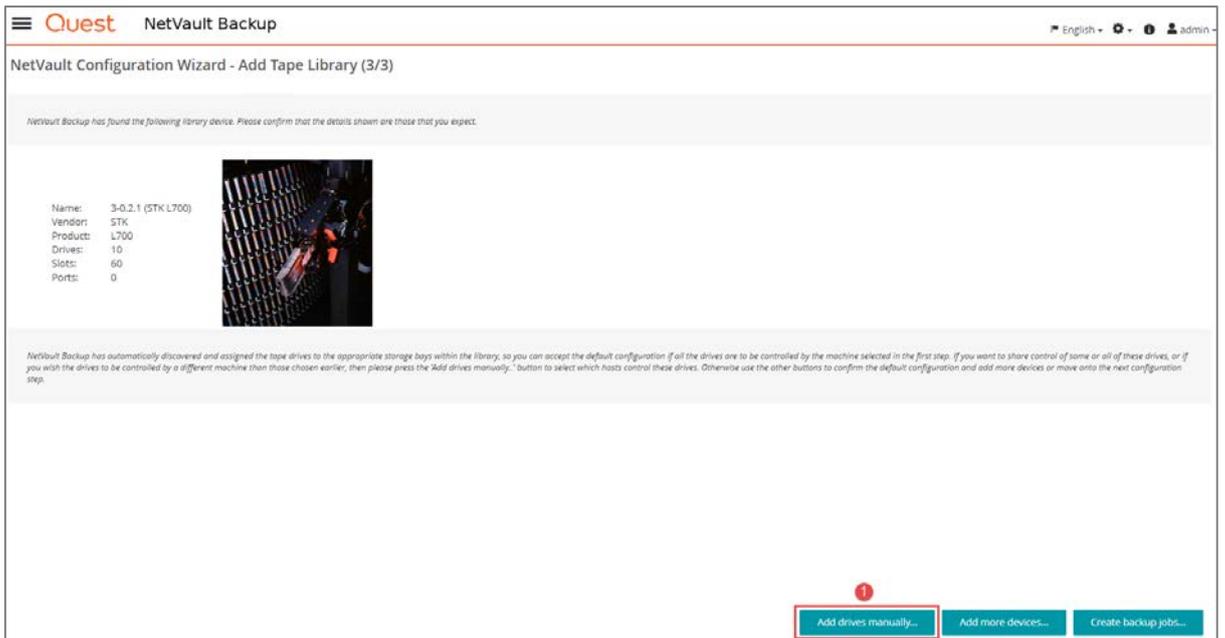
4 Select the Add Tape Library/ media changer ❶ and click the **Next** button ❷.



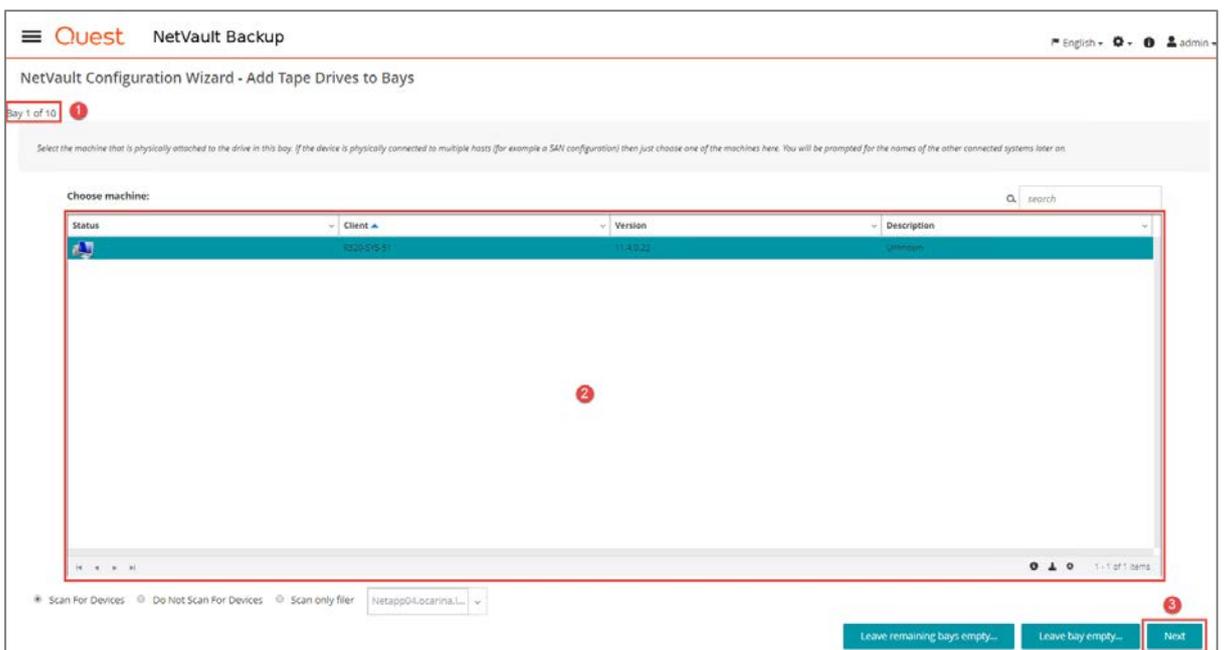
- 5 Provide a name for the VTL 1, select the VTL changer path intended to control the changer LUN 2 and then click **Next** on the lower right 3,



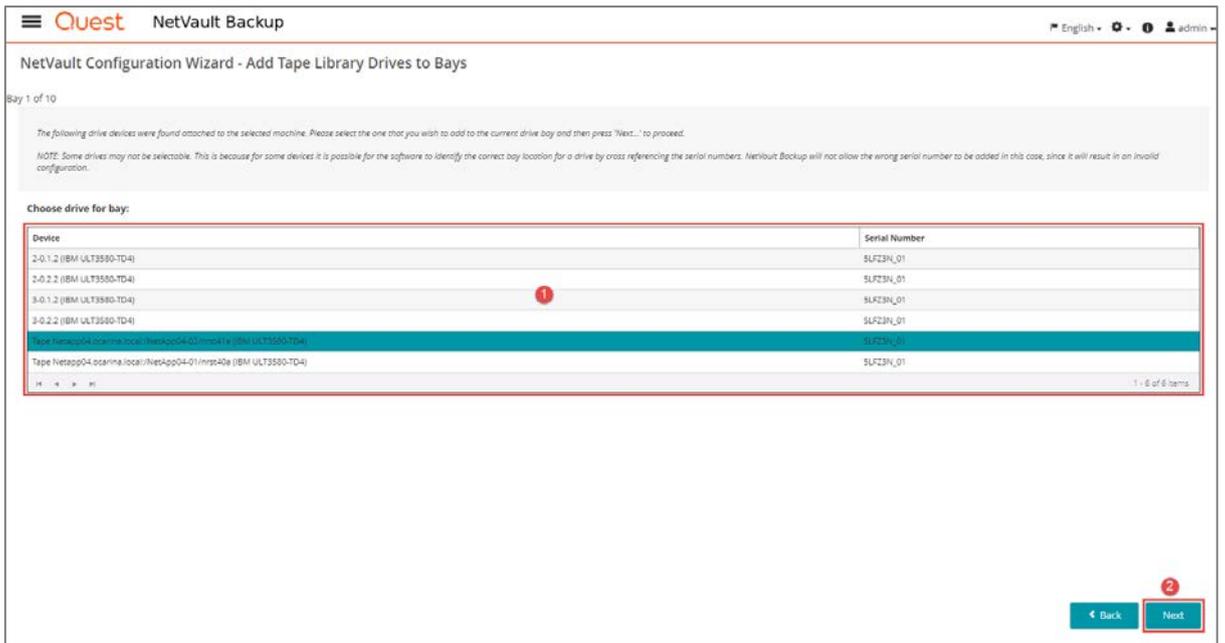
- 6 When the tape library scan is complete, click the **Add drives manually** 1 button to continue to add the library for LAN-Free access.



7 For each Drive Bay ① displayed, select the first of the nodes ② to be added as shared and click Next ③.



8 Select the Primary path for the drive LUN ① displayed, click Next ②.

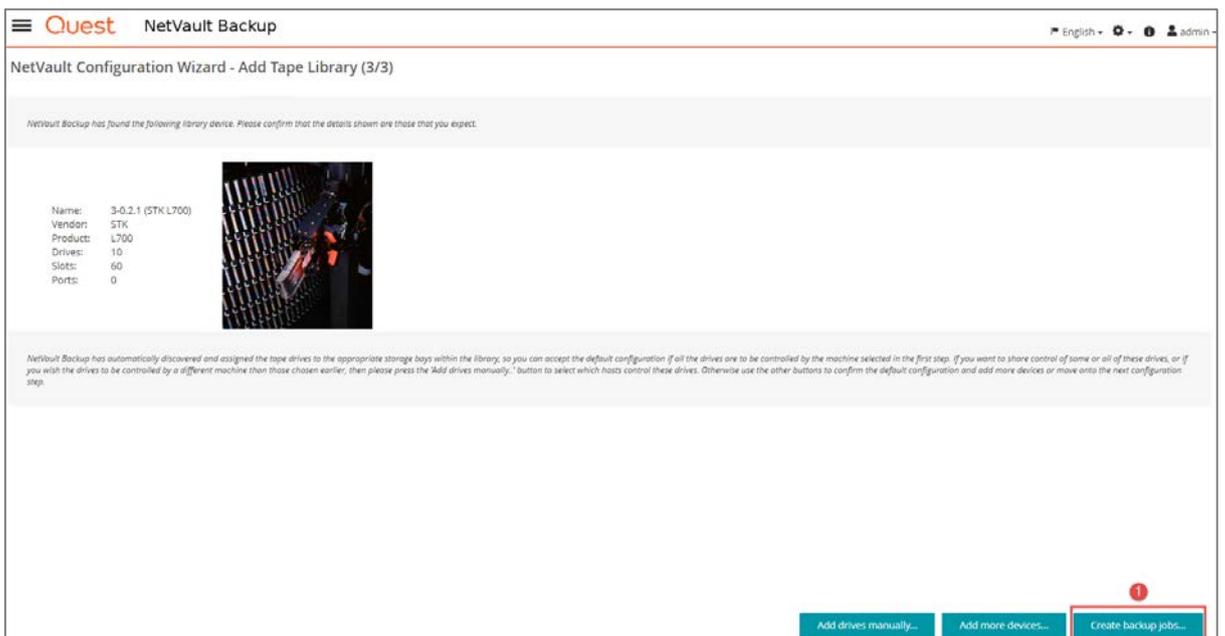


9 Select the client systems that are to share the tape drive LUNs ①, click the **Next** ② button.

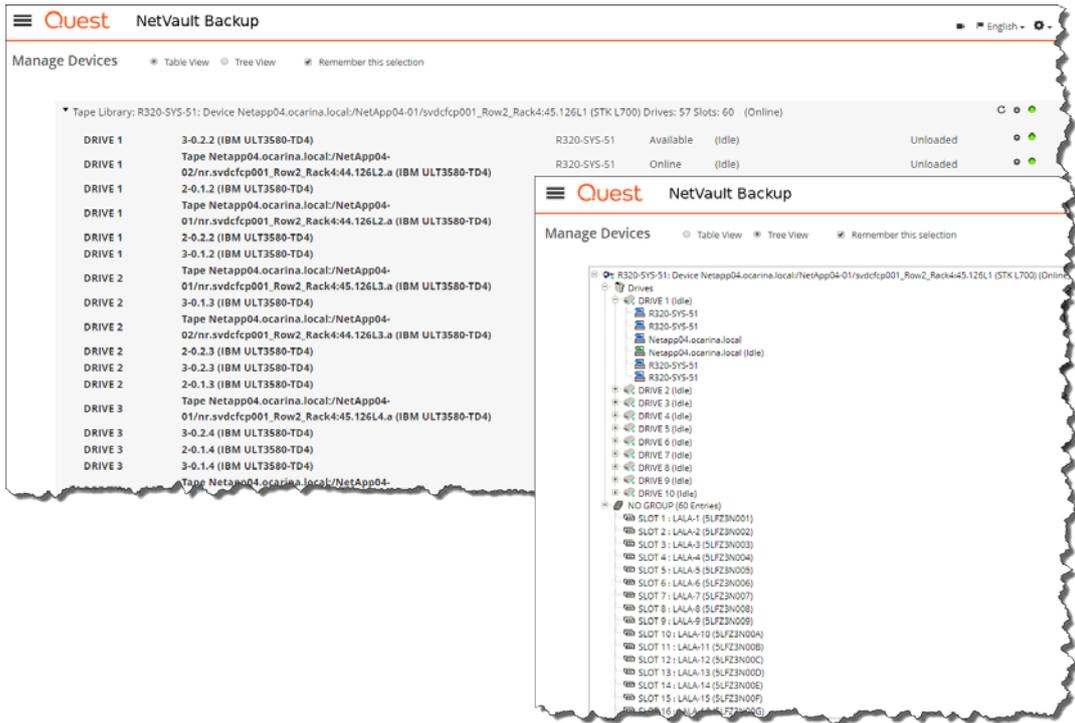


10 Repeat this process for the remaining drive bays and click the **Next** button to complete.

11 When the tape library scan is complete, click the **Create Backup job** ① button to commit the library. The VTL should show up ready for use.



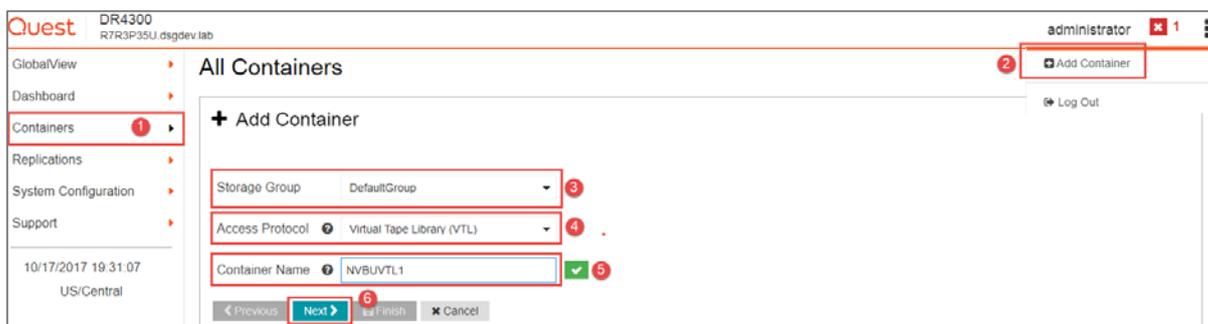
12 The LAN-Free VTL Configuration is now ready for use.



Configuring the DR Series as a iSCSI VTL target for NetVault: Backup

Creating and configuring iSCSI target containers for NetVault: Backup

- 1 Select Containers in the left navigation area of the DR Series system GUI (1), and then select the Action Menu in the upper right corner. Click the Add Container option at the top of the menu (2). Enter a Container Name (3), and select **Virtual Tape Library (VTL)** from the Access Protocol drop down menu (4). Provide a name for the container (5) then click next (6).



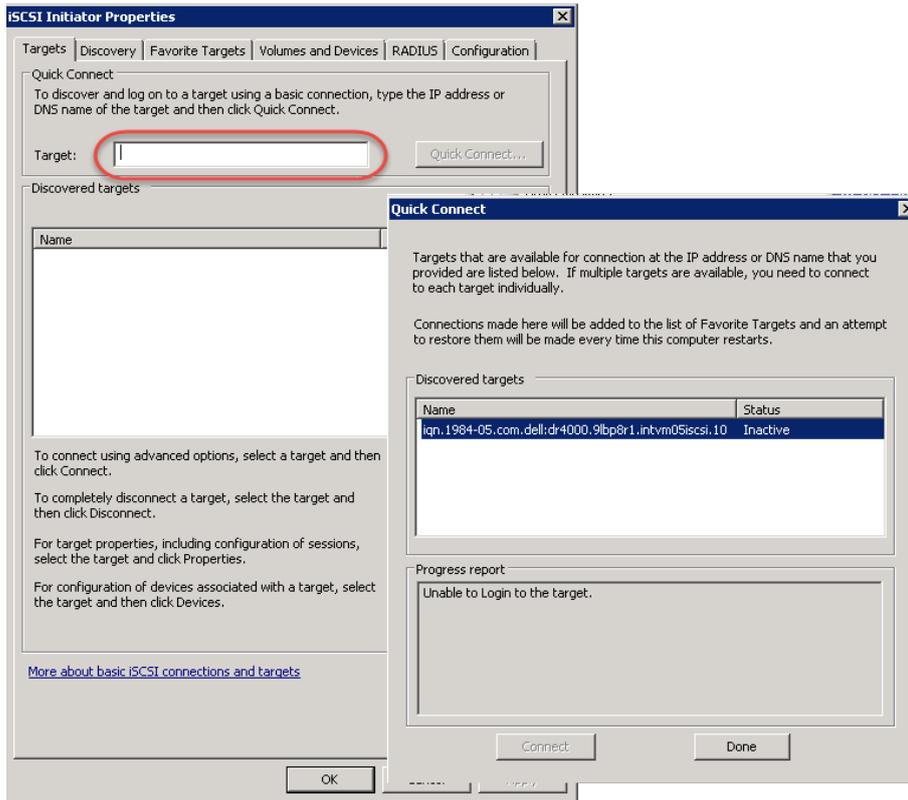
- 2 When prompted select the **STK L700** Robot Model (1). Select the Tape Size (2), the **iSCSI VTL** Access Protocol (3) and number of drives. Specify the DMA Access Control by providing the storage node or media node IP Address or FQDN (4). For NetVault, you must also specify **Auto** (5) as the **Marker Type**. Click Next (6).

- 3 Finalize VTL creation by clicking **Save**.

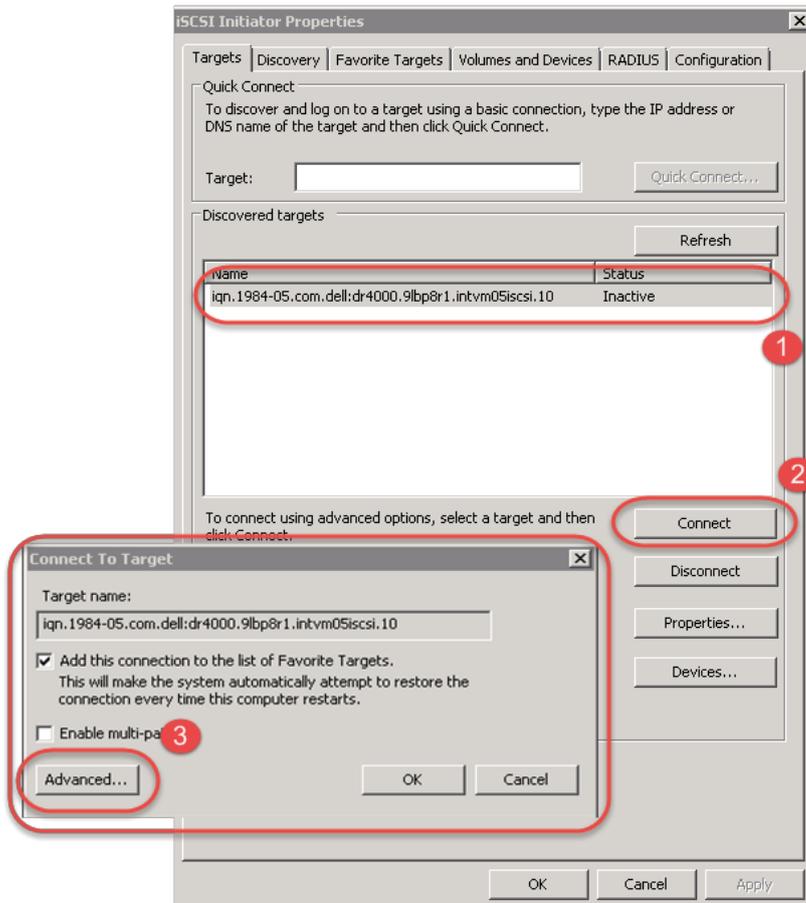
Verifying initiators are connected to the iSCSI VTL container for use with NetVault: Backup

Configuring the iSCSI target – Windows

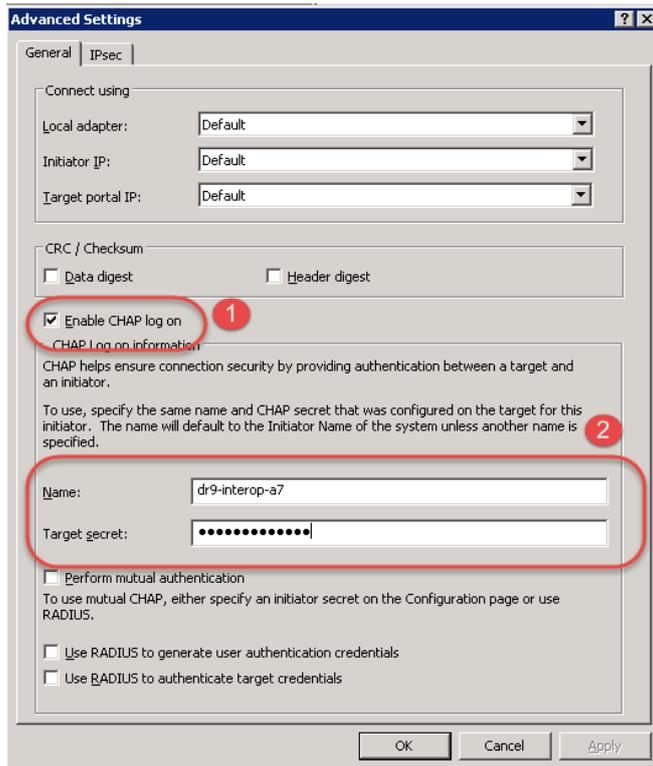
- 1 Configure the iSCSI Initiator Software for Windows by providing the IP or FQDN of the DR Series system in the Quick Connect **Target** field.
- 2 Click **Quick Connection** to open the Quick Connect dialog box, which indicates a connection was made but is set as inactive.



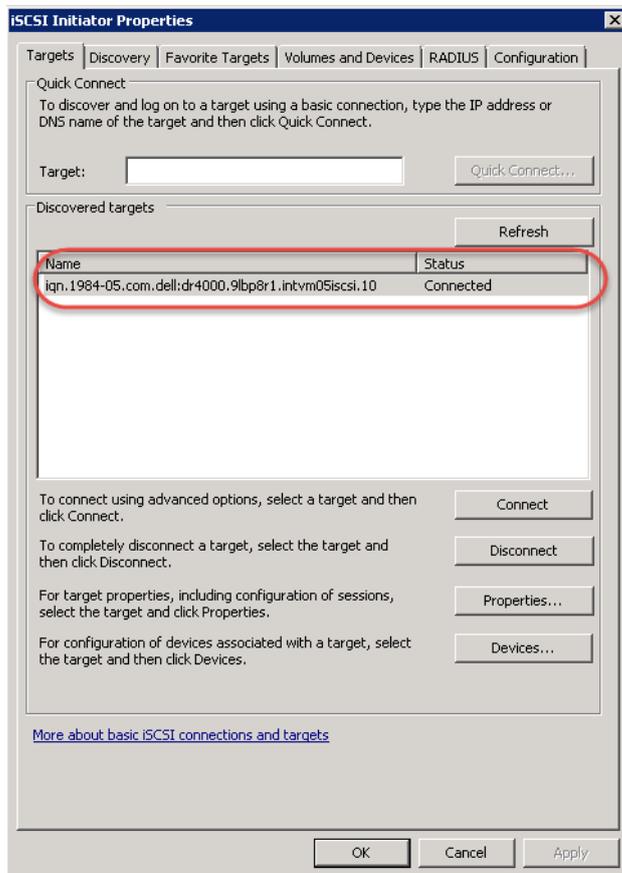
- 3 Close the dialog box and proceed by selecting the newly discovered target. This target will have an Inactive Status as it requires authentication parameters to be provided for iSCSI logon.
- 4 Select the Target from the list, click the **Connect** button, and then in the Connect To Target dialog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



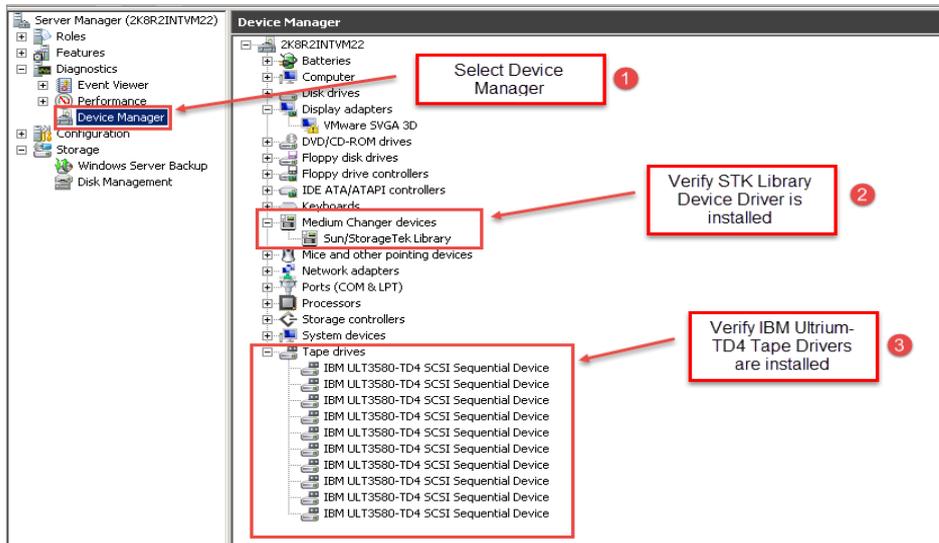
- 5 In Advanced Settings, select to **Enable CHAP log on** and enter the User Name and Target Secret / Password.
- 6 Click **OK** and refer to VTL configuration guidelines chapter of this document for more information about accounts and credentials.



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



- 7 Open the Server Manager Snap-in and verify that the newly connected devices show up in the Device Manager.
- 8 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, for example, StorageTek Library Drivers.

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.

- 1 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
```

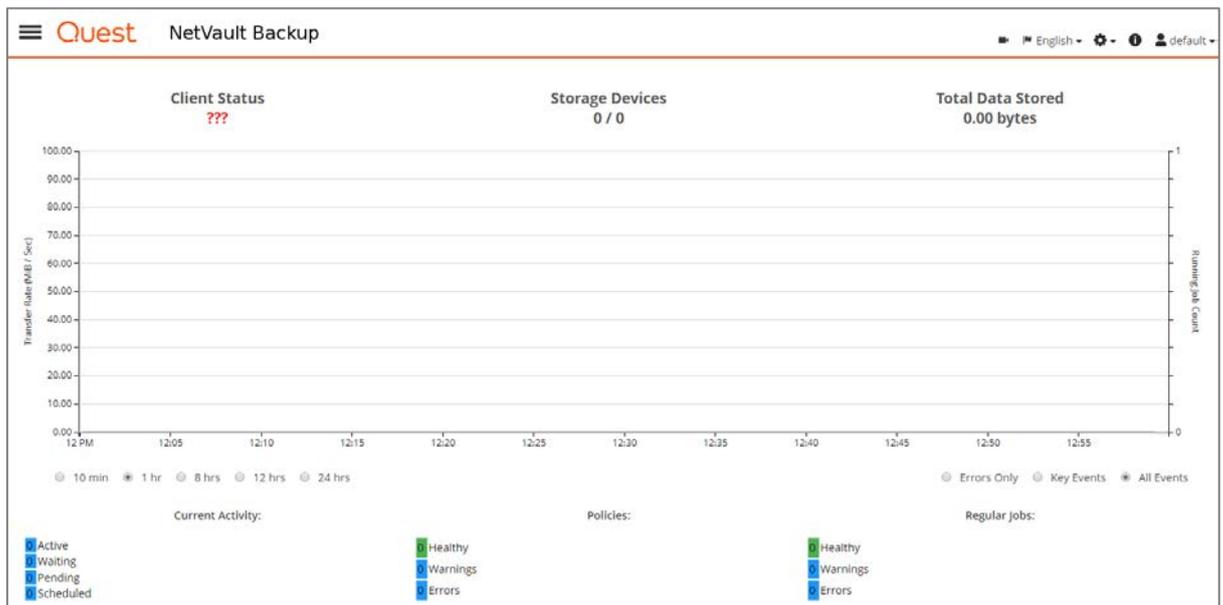
For example:

```
iscsiadm -m session = tcp: [8] 10.8.230.108:3260,1 iqn.1984-05.com.dell:dr4000.3071067.interoprhel52nl.30
```

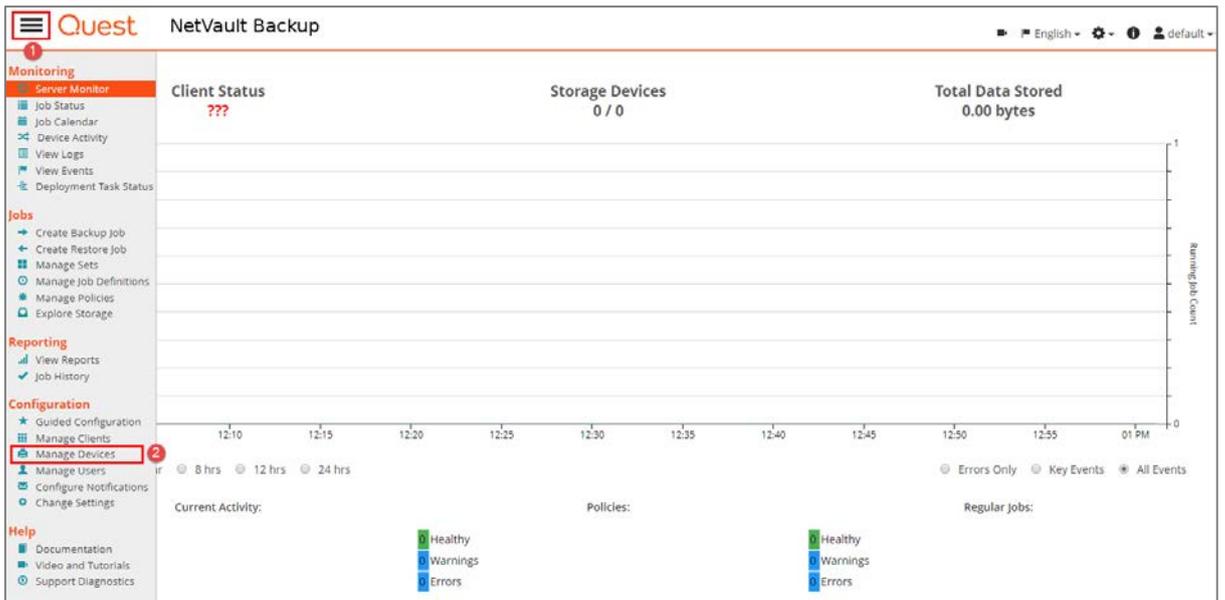
- 5 Review dmesg or /var/log/messages for details about the tape devices created upon adding the DR Series system iSCSI VTL.

Configuring NetVault: Backup to use the newly created iSCSI VTL – Automatic Library Detection

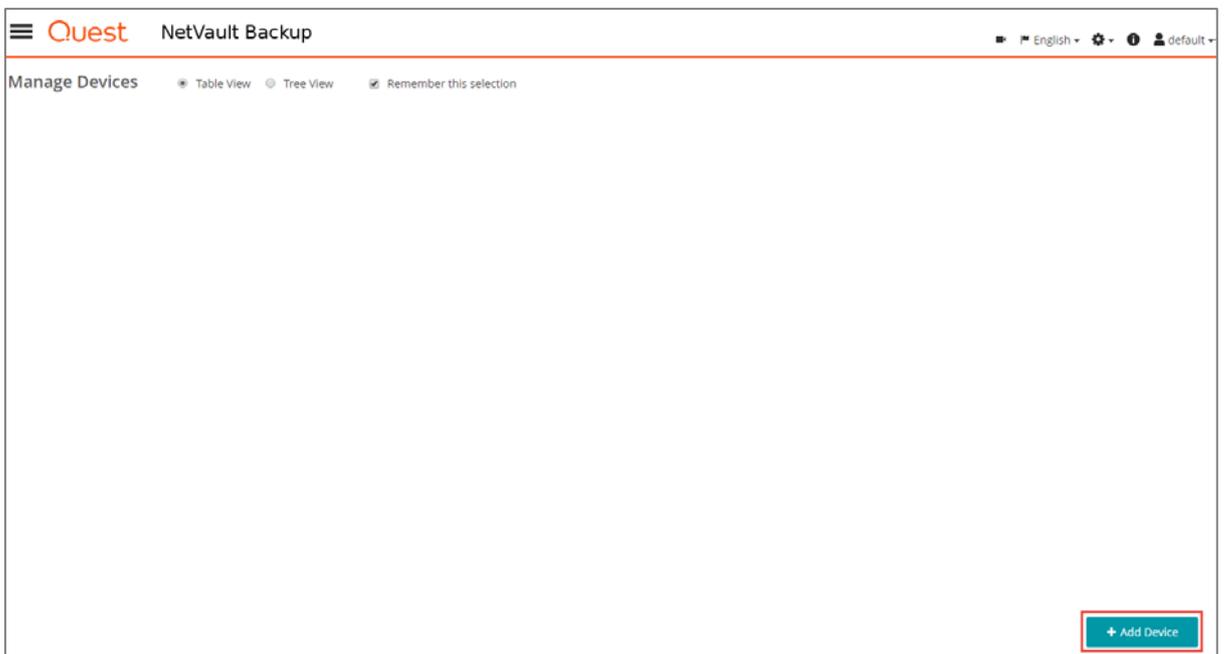
- 1 Open the NetVault: Backup Web Console.



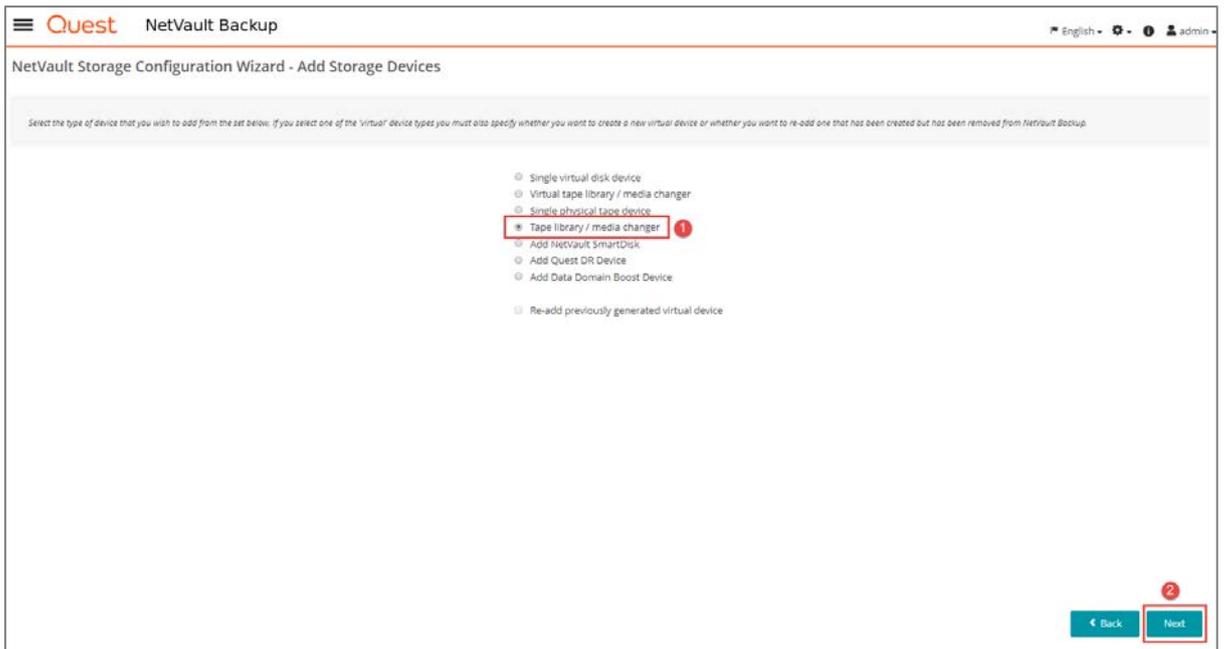
- 2 Add the DR VTL container to NetVault: Backup by opening the menu drawer ❶ and selecting the Manage Devices wizard ❷.



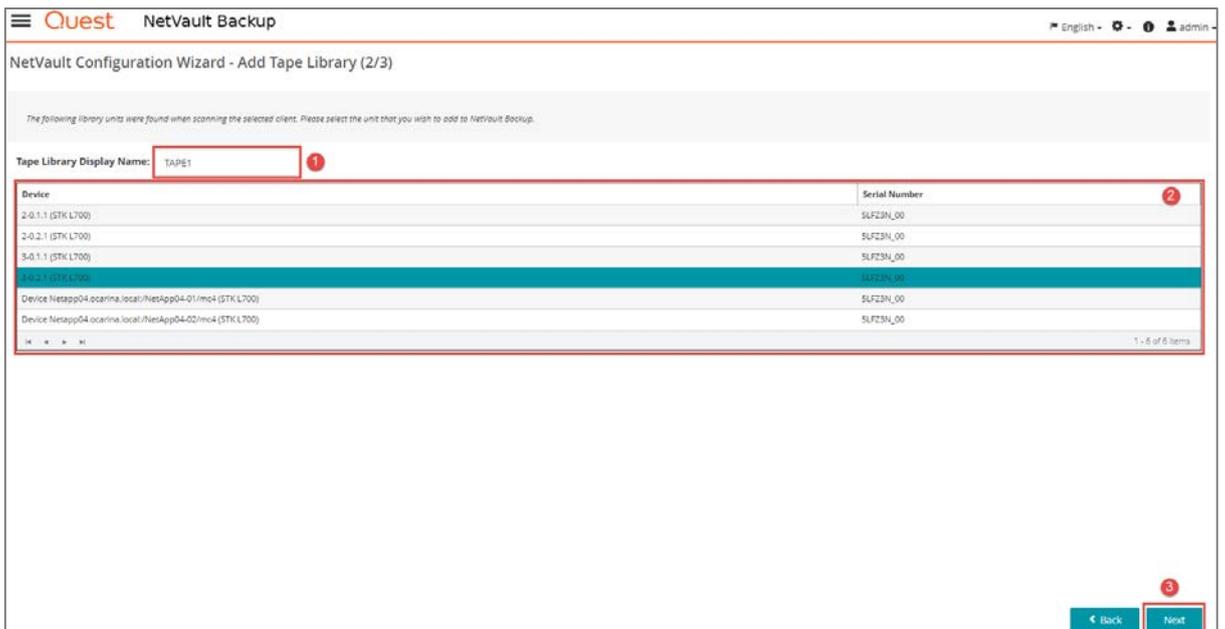
3 Select the Add Device button.



4 Select the Add Tape Library/ media changer ① and hit the next button ② on the lower right.



- 5 Provide a name for the VTL ①, select the VTL changer path intended to control the changer LUN ② and then click **Next** on the lower right ③,



- 6 When the tape library scan has been completed, click the **Create Backup job** ① button to commit the library. The VTL should show up ready for use.

Quest NetVault Backup English - [gear] [info] [admin]

NetVault Configuration Wizard - Add Tape Library (3/3)

NetVault Backup has found the following library device. Please confirm that the details shown are those that you expect.

Name:	3-0.2.1 (STK L700)
Vendor:	STK
Product:	L700
Drives:	10
Slots:	60
Ports:	0



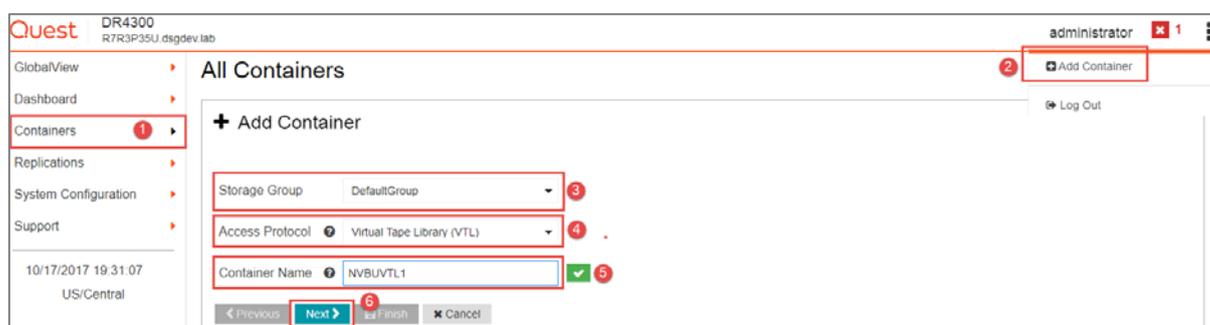
NetVault Backup has automatically discovered and assigned the tape drives to the appropriate storage bays within the library, so you can accept the default configuration if all the drives are to be controlled by the machine selected in the first step. If you want to share control of some or all of these drives, or if you wish the drives to be controlled by a different machine than those chosen earlier, then please press the "Add drives manually..." button to select which hosts control these drives. Otherwise use the other buttons to confirm the default configuration and add more devices or move onto the next configuration step.

Add drives manually... Add more devices... Create backup jobs...

Configuring the DR Series as a NDMP VTL target for NetVault: Backup

Creating and configuring NDMP target containers for NetVault: Backup

- 1 Select Containers in the left navigation area of the DR Series system GUI (1), and then select the Action Menu in the upper right corner. Click the Add Container option at the top of the menu (2). Enter a Container Name (3), and select **Virtual Tape Library (VTL)** from the Access Protocol drop down menu (4). Provide a name for the container (5) then click next (6).

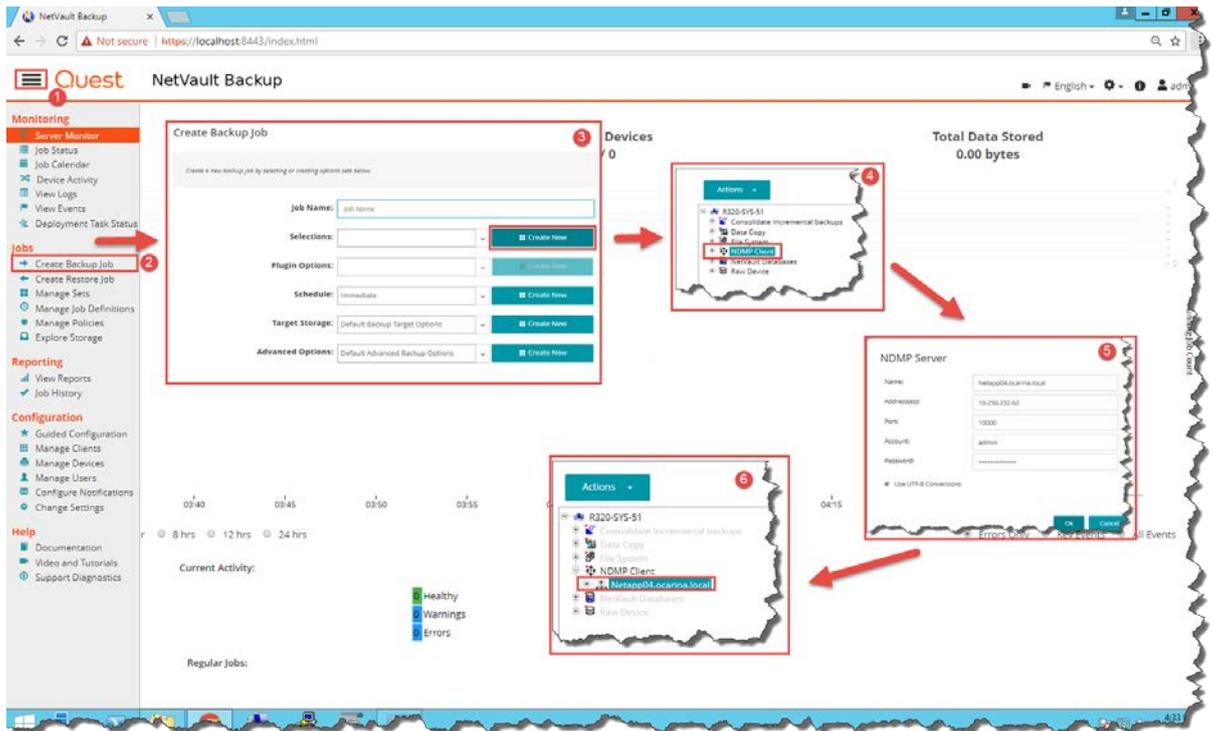


- 2 When prompted select the **STK L700** Robot Model (1). Select the Tape Size (2), the **NDMP VTL** Access Protocol (3) and number of drives. Specify the DMA Access Control by providing the storage node or media node IP Address or FQDN (4). For NetVault, you must also specify **Auto** (5) as the **Marker Type**. Click Next (6).

- Finalize VTL creation by clicking **Save**.

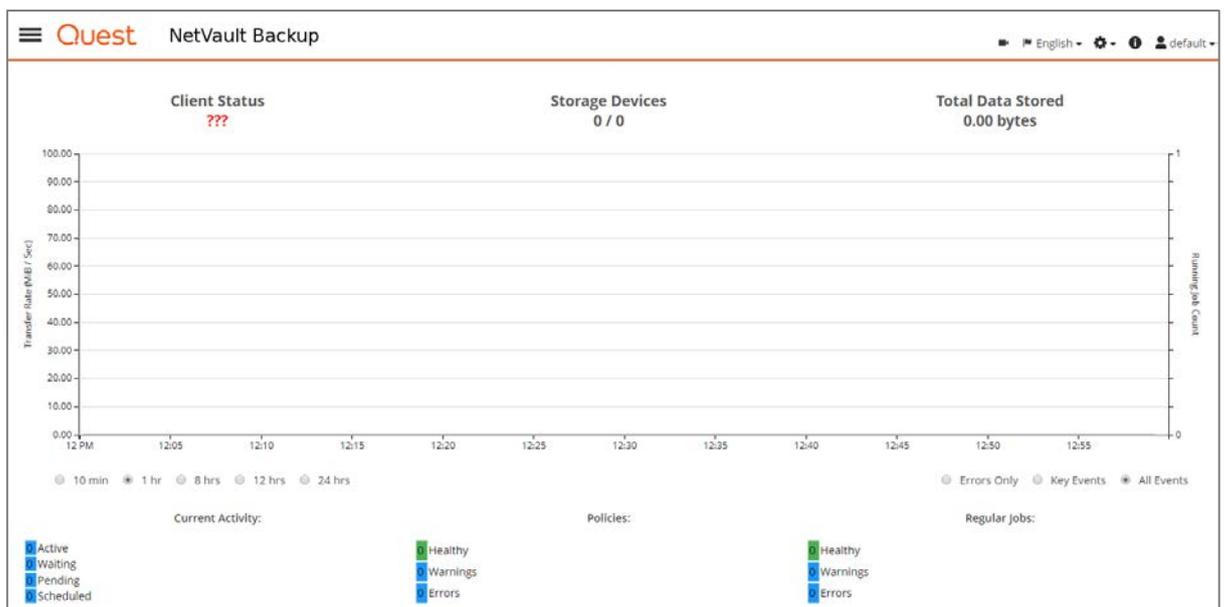
Configuring the DR Series NDMP service with NetVault: Backup

- Open the NetVault: Backup Web Console.
- From the Main Menu ❶ Navigate to the Create Backup Job submenu ❷ and select to Create New Selection Set ❸. Select the NDMP Plugin within the NetVault Create Selection Set navigation pane and Select to add a new NDMP Server node ❹. In the dialog box, enter the desired logical name of the node, the IP address or FQDN and DR the NDMP credentials ❺. Provide the logon credentials for the ndmp user account on the DR Series system. Verify that the DR Appliance is added to the NetVault: Backup Server and is ready for access ❻.

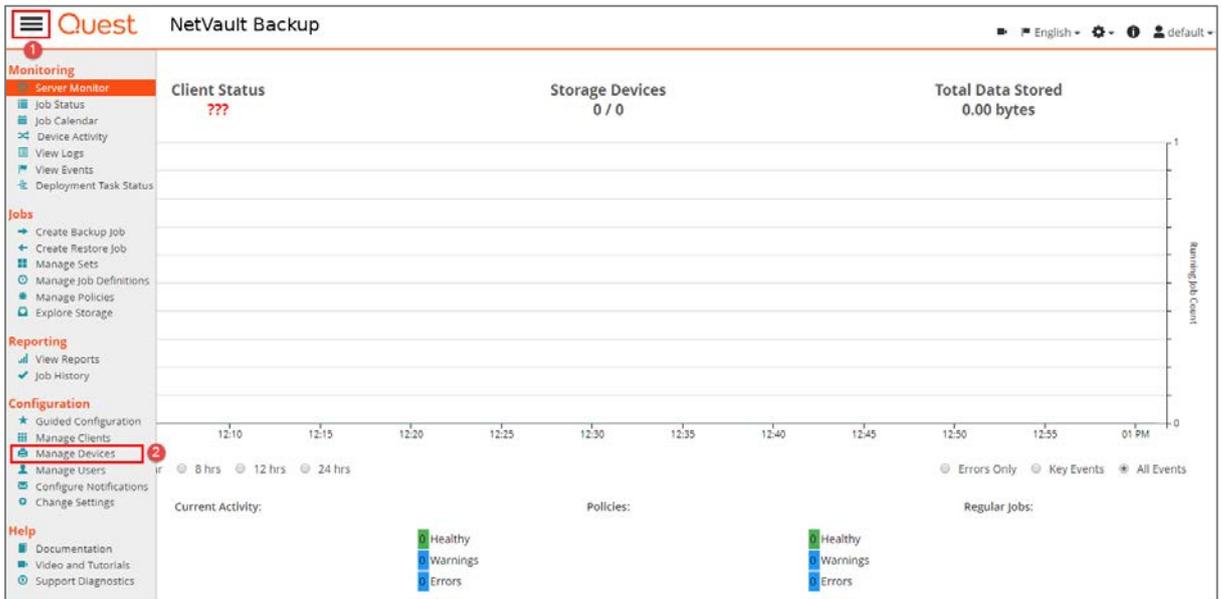


Configuring NetVault: Backup to use the newly created NDMP VTL – Automatic Library Detection

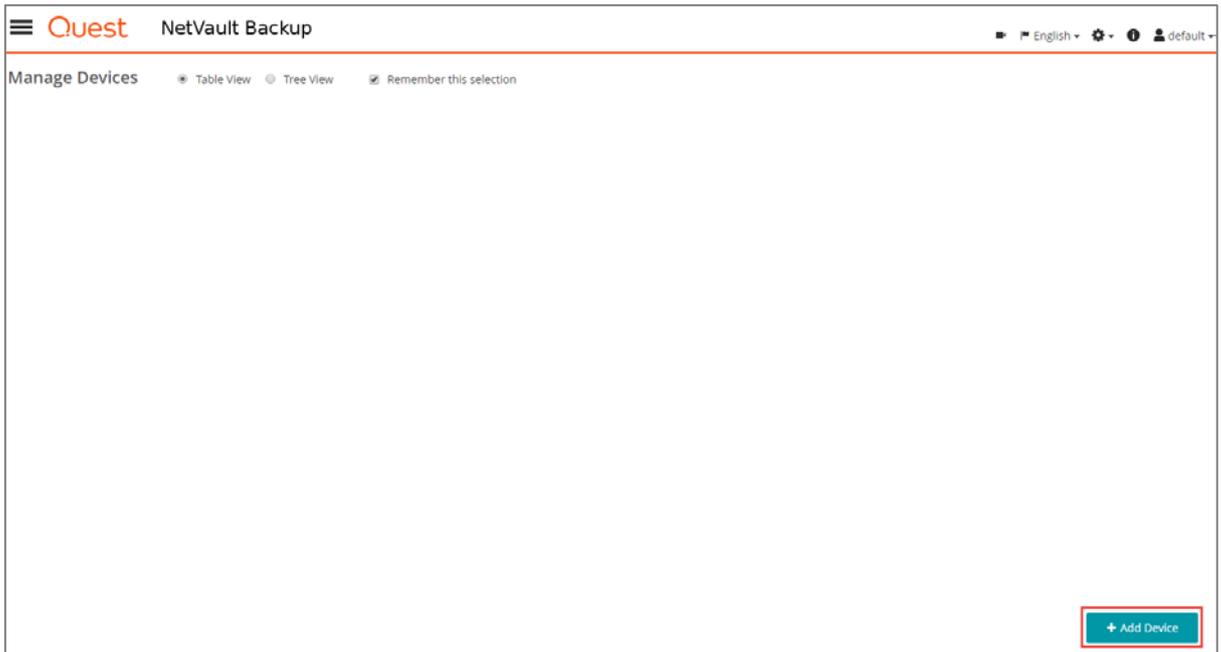
- 1 Open the NetVault: Backup Web Console.



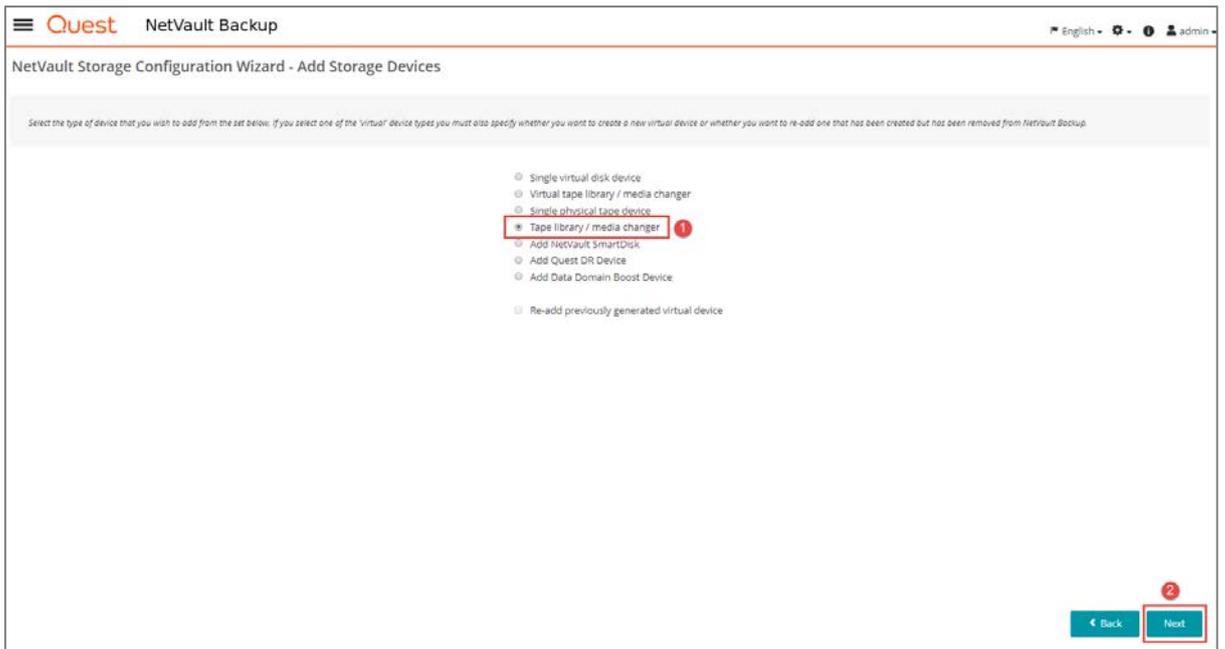
- 2 Add the DR VTL container to NetVault: Backup by opening the menu drawer ① and selecting the Manage Devices wizard ②.



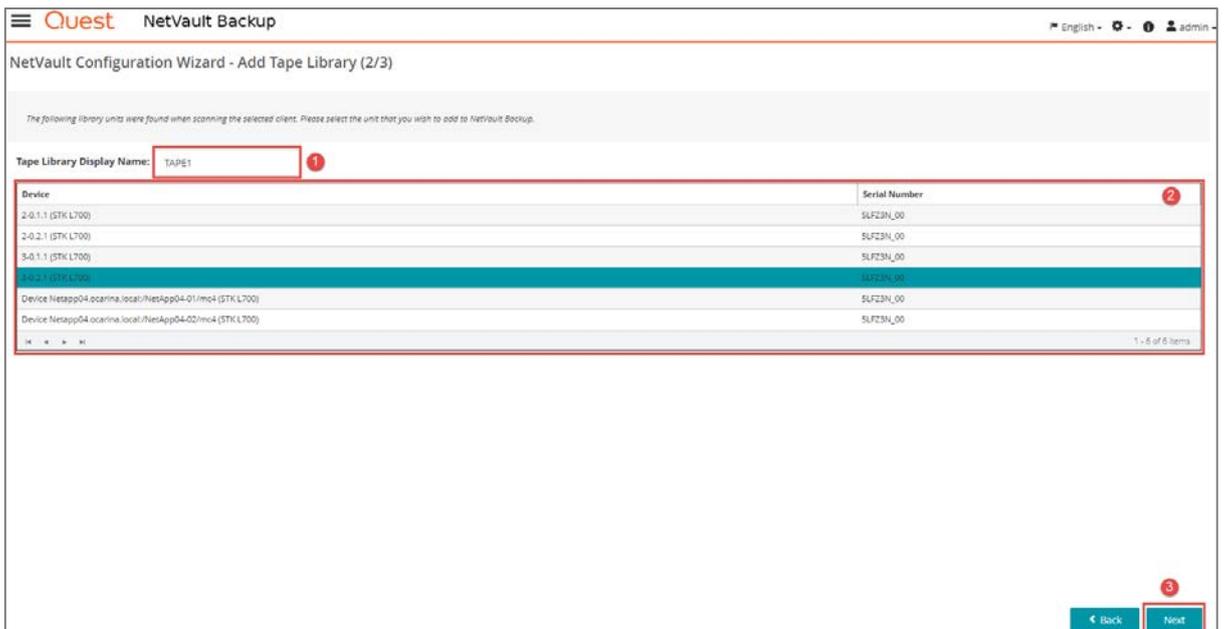
- 3 Select the Add Device button.



- 4 Select the Add Tape Library/ media changer ① and hit the next button ② on the lower right.



- 5 Provide a name for the VTL 1, select the VTL changer path intended to control the changer LUN 2 and then click **Next** on the lower right 3,



- 6 When the tape library scan is complete, click the **Create Backup job** 1 button to commit the library. The VTL should show up ready for use.

Quest NetVault Backup English - [gear] [info] [admin]

NetVault Configuration Wizard - Add Tape Library (3/3)

NetVault Backup has found the following library device. Please confirm that the details shown are those that you expect.

Name:	3-0.2.1 (STK L700)
Vendor:	STK
Product:	L700
Drives:	10
Slots:	60
Ports:	0



NetVault Backup has automatically discovered and assigned the tape drives to the appropriate storage bays within the library, so you can accept the default configuration if all the drives are to be controlled by the machine selected in the first step. If you want to share control of some or all of these drives, or if you wish the drives to be controlled by a different machine than those chosen earlier, then please press the "Add drives manually..." button to select which hosts control these drives. Otherwise use the other buttons to confirm the default configuration and add more devices or move onto the next configuration step.

Add drives manually... Add more devices... Create backup jobs...

Using VTL replication

Leveraging the VTL replication feature allows for native data replication between up to two or three DR Series systems. This replication occurs at the tape level insuring restorability even if the replication is not completely in-sync.

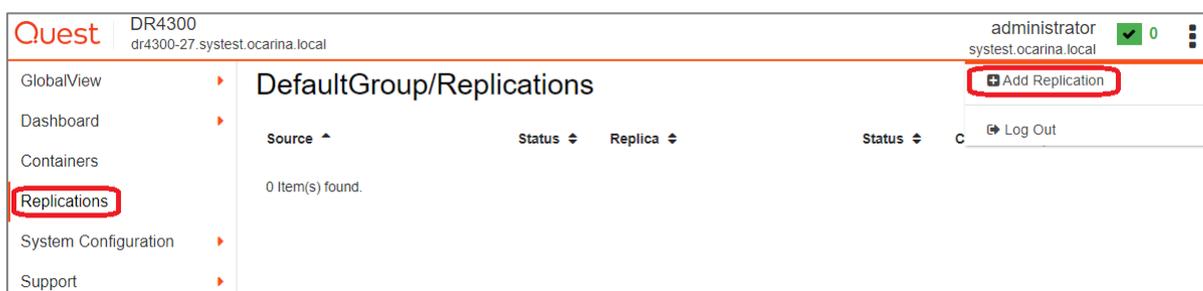
Configuring the DR Series system for VTL replication

Native VTL Replication must occur between two DR systems; but, optionally, can be configured for up to three systems. The primary VTL is referred to as the Source, the first replication target is referred to the Replica Target. The optional second replication target is referred to as the Replica Cascade.

Prerequisites:

- Both the Source, Replica Target, and Replica Cascade VTL should be created. Follow the corresponding Configure VTL section of this guide if assistance is needed in creating VTL's.
- The Source, Replica Target, and Replica Cascade VTLs need to be of the same Tape Size.

- 1 On the DR web GUI of the Replication Source system select Replications, then click the Action Menu in the upper right and click Add Replication.



- 2 In the resulting wizard select Replica only if only two DR systems are replicating. If a Replication Cascade is desired select Replica & Cascade. Once finished click Next.

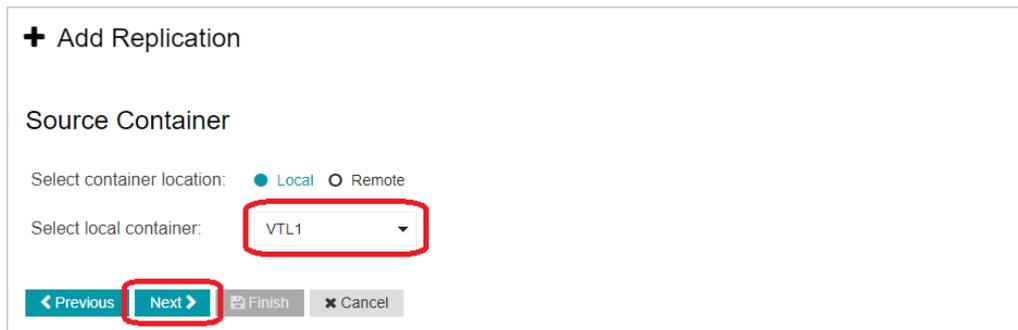


+ Add Replication

Choose replication type: Replica only Replica & Cascade

< Previous **Next >** Finish Cancel

- 3 Select the Select local container dropdown and click on the source replication VTL name. Click Next to proceed.



+ Add Replication

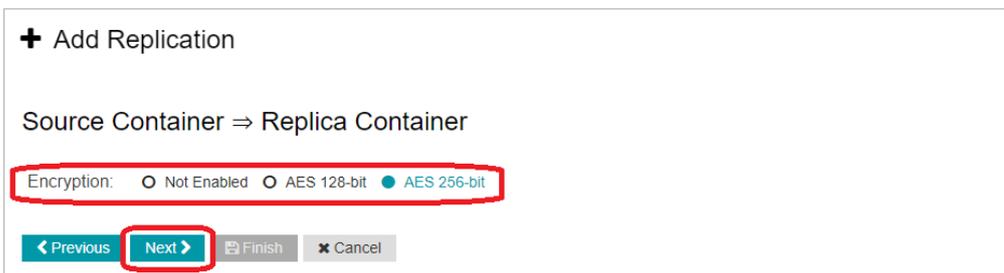
Source Container

Select container location: Local Remote

Select local container: VTL1

< Previous **Next >** Finish Cancel

- 4 In the Encryption option select either 128-bit or 256-bit AES encryption if desired. If this is not needed leave the "Not Enabled" option selected, then click Next.



+ Add Replication

Source Container => Replica Container

Encryption: Not Enabled AES 128-bit AES 256-bit

< Previous **Next >** Finish Cancel

- 5 Enter the Username and Password with the corresponding information from the Replica target. Enter the Fully Qualified Domain Name or IP address of the Replica Target in the Remote Systems field. Click the Retrieve Remote Container(s) button and the Select remote container drop down menu should populate. Select the Select remote container drop down and click the Replica Target VLT name from the list. Once finished click Next.



NOTE: The default Username is administrator with a default password of St0r@ge!

+ Add Replication

Replica Container

Select container location: Local Remote

Username:

Password:

Remote system:

Select remote container:



NOTE: If a Replica Cascade is being configured the next screen will look exactly like Step 5. Fill in the Username, Password, Remote system, and Select Remote Container fields as they pertain to the Replica Cascade VTL target.

- The next wizard screen is a summary of the configuration. Click Finish to apply the configuration

+ Add Replication

Summary

Source Container

Location: **local**

Name: **VTL1**

Source Container ⇒ Replica Container

Encryption: **AES 256-bit**

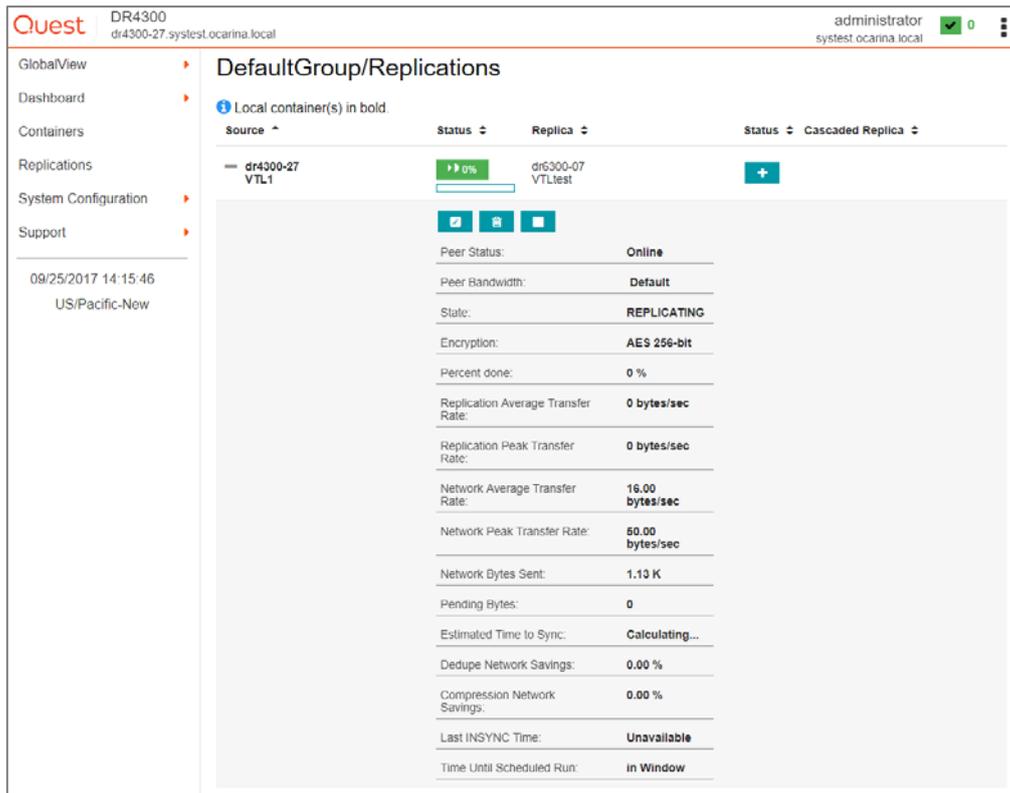
Replica Container

Location: **remote**

Remote System: **dr6300-07.systest.ocarina.local**

name: **VTLtest**

- After a few moments, the replication should appear on the Replications page. Monitor replication status by clicking the + icon to the left of the replication in question.



Restoring from a replica or replica cascade

Before attempting to restore from replication, it is important to understand how NetVault: Backup handles tape backups. All tapes have a barcode, a MID and a logical label, which are stored in the NetVault:Backup database with a matching Media Object. If the barcode were to change the MID would not match what is assigned to the logical media label. It should also be noted in the examples we use a iSCSI library. The steps are the same no matter the protocol type, the only change is the access protocol used on the replica library. Also if the FC protocol is used some switch zoning may be needed.



NOTE: It is important to note that only fully in-sync tapes are available on the replica site. What is restorable is affected by how in-sync the containers are at point of failure.

Understanding re-serialization

When activating a Replica VTL for restore it is possible to reserialize the VTL. This operation temporarily changes the library serial number and the tape barcodes so that a DMA will see it as a completely new/independent Tape Library. This feature can optionally be used in NetVault: Backup but should only be used with restoring to a different NetVault: Backup Server which has not seen the library before. If VTL reserialization is done to the original NetVault: Backup instance, a catalog of the media will be required.

Possible restore situations

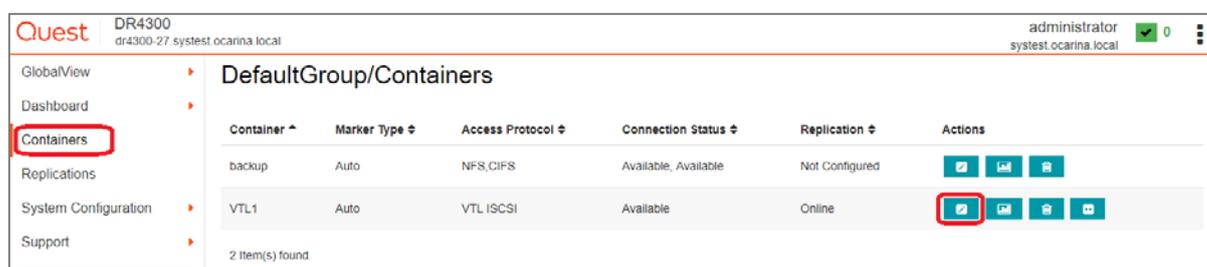
There are two general situations in which restores from replicated data would be performed.

- A restore to the original NetVault: Backup server, it is assumed the NetVault: Backup server database is intact.
 - In this example just the Primary Site DR or access to it might be down.
 - All the tapes will have barcodes that match what is stored in the NetVault: Backup database.
 - Reserialization is not needed.
- A restore to a new/temporary or alternative Netvault: Backup server in which case it is assumed the NetVault: Backup database is different.
 - A new/temporary NetVault: Backup install might be used to restore the original NetVault: Backup Database.
 - An independent NetVault: Backup server at a DR site is being used for restore at an offsite location.
 - Reserialization is not needed

Restoring from a replica VTL onto the original NetVault: Backup server

In this case, it is assumed that the NetVault: Backup database is intact. The barcodes of each tape will have a matching entry in a Media Database. Because of this, reserializing is not required. If reserialization occurs, an additional library would be added, but the tapes would not be in a Media Database. A catalog of the reserialized library would be required to restore these tapes. It is also assumed that the source DR is offline, and the VTL is no longer mounted to the Media Server.

- 1 First, you need to activate the VTL. This involves configuring it with a connection protocol and bringing the replica tape library online. In the DR Series system GUI navigate to the Containers page.
- 2 Click the  edit button on the Replica target VTL.



- 3 Select the VTL Access Protocol desired and fill in the IQN, FQDN, IP address, or port initiator WWN of the media server depending on which protocol is selected. Click Next, then click Save on the Summary Page.

Edit - VTL1

Robot Model Quest DR_L700 Dell DR_L700 STK L700

Tape Size 800GB

VTL Access Protocol FC NDMP iSCSI No Access

IQN, FQDN or IP Address

Marker Type

Add More Tapes (no. of tapes)



NOTE: Now that the Target VTL has an access protocol we need to activate it. This makes the Replica VTL readable

- Navigate to the Replications page, and then expand the replication in question to review its replication statistics. Check the Percent Done. If this is 100% In-Sync then click the  Activate button on the replication line.

Source	Status	Replica	Status	Cascaded Replica
dr6300-07 VTLtest		dr4300-27 VTL1		

Peer Status: Online

Peer Bandwidth: Default

State: INSYNC

Encryption: AES 256-bit

Percent done: 100 %

- In the window that comes up enter 00 as the re-serialization code for replica. This will insure the library has the same serial numbers and barcodes it did originally. If the VTL is in sync click Activate, if it is not in sync click Force Activate.

Activate VTL target Replica Container - VTL1

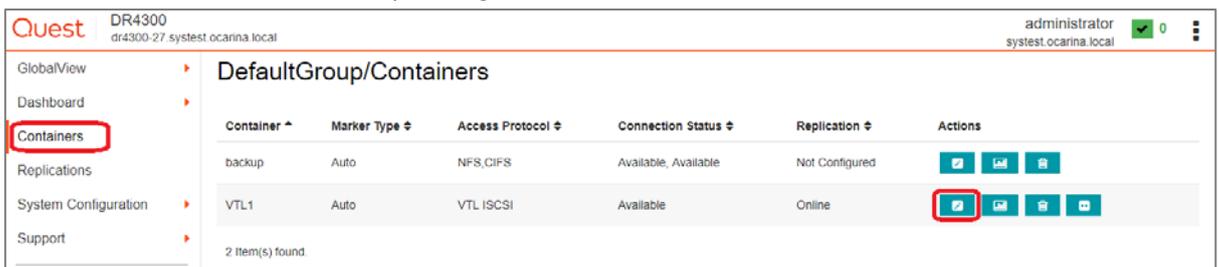
Reserialization code for replica:

- At this point the Library will be online and available. The next step is to connect the library to the NetVault: Backup Domain. Please reference sections specific to configuring your chosen protocol such as, Configuring the iSCSI Target in windows/linux and Verify the FC VTL is seen – Windows
- Once the VTL is seen by Windows, the Tape library will be seen by the NetVault: Backup server as well. Because barcodes match the NetVault: Backup Media Database, the library will not be useable again.

Restoring from a replica VTL on an alternative NetVault: Backup Server

In this case, it is not possible to assume the NetVault: Backup database is intact. The barcodes of each tape will not have an entry in a NetVault: Backup media database. Either way, the tapes need to be catalogued before a restore is possible. Reserialization is not necessary.

- You need to activate the VTL. This involves configuring it with a connection protocol and bringing the replica tape library online. In the DR Series system GUI, navigate to the Containers page.
- Click the  edit button on the Replica target VTL.



- Select the VTL Access Protocol needed, and enter the IQN, FQDN, IP address, or port initiator WWN of the media server depending on which protocol is selected. Click Next, and then click Save on the Summary Page.

Edit - VTL1

Robot Model: Quest DR_L700 Dell DR_L700 STK L700

Tape Size: 800GB

VTL Access Protocol: FC NDMP iSCSI No Access

IQN, FQDN or IP Address:

Marker Type: Auto

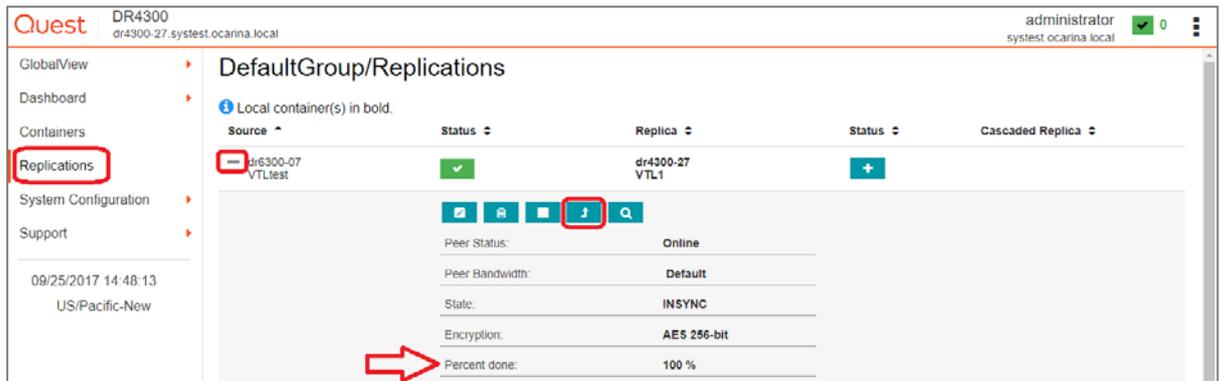
Add More Tapes (no. of tapes): Reached the max of tapes available

Navigation:

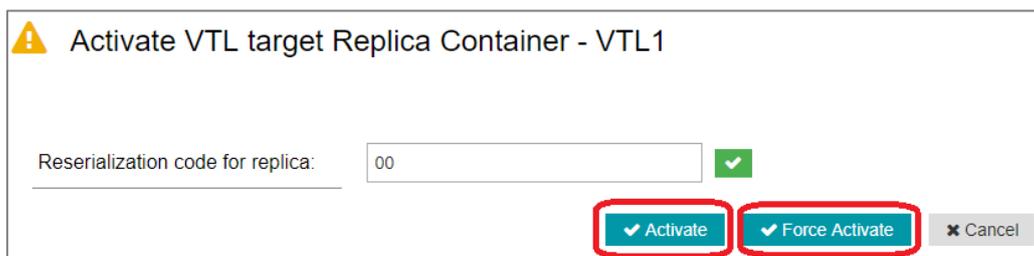


NOTE: Now that the Target VTL has an access protocol you need to activate it, which makes the Replica VTL readable.

- 4 Navigate to the Replications page, and then expand the replication to review replication statistics. Check the Percent Done. If this is 100% In-Sync then Click the  Activate button on the replication line.



- 5 In the window that comes up enter 00 for the re-serialization code for replica. This will insure the library has the same serial numbers and barcodes it did originally. If the VTL is in sync click Activate, if it is not in sync click Force Activate

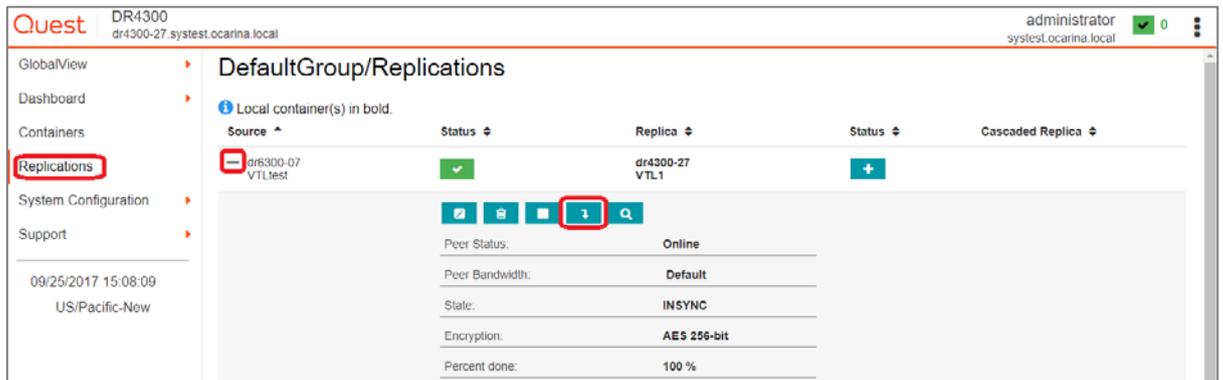


- 6 At this point, the Library will be online and available. The next step is to connect the library to the Media Server. Please reference sections specific to configuring your chosen protocol. I.E. Configuring the iSCSI Target in windows/linux and Verify the FC VTL is seen – Windows.
- 7 Once the VTL is seen by Windows, the tape library will need to be added to the NetVault: Backup server. This is because this library is new to this NetVault: Backup server. Please reference sections specific to configuration your chosen protocol. I.E. Configuring the DR Series iSCSI VTL in NetVault: Backup or Configuring the DR Series FC VTL in NetVault: Backup.
- 8 At this point, you will have a newly discovered Tape Library listed in NetVault: Backup. You need to run the inventory and catalog. This is done in the catalog section of the Tape Infrastructure section of the NetVault: Backup GUI.

Deactivating a replica VTL

Once all issues have been resolved make sure to disconnect your library and deactivate it. Then reconfigure replication as needed.

- 1 To deactivate a library in the DR Series system GUI, navigate to the Replications page. Expand the replication in question and click the  Deactivate button.



- 2 One the pop-up window click Yes.

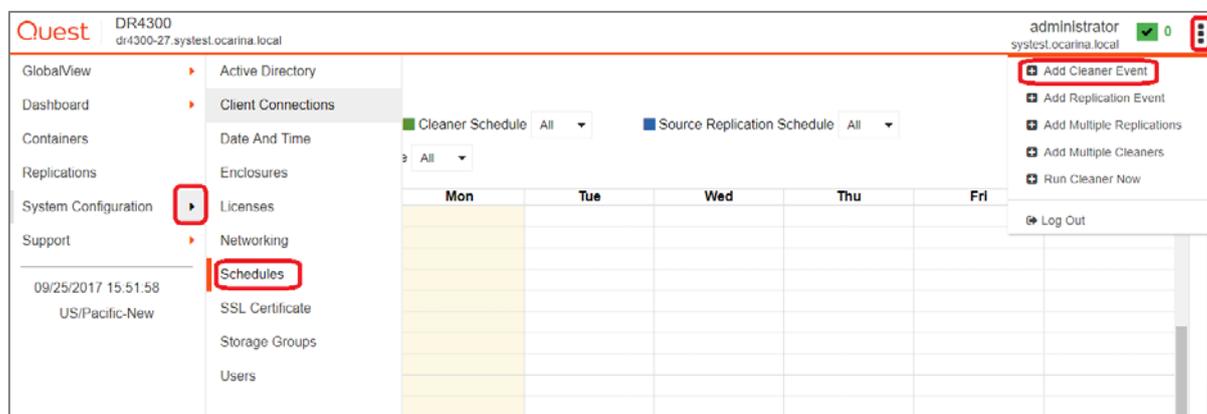


Setting up the DR Series system cleaner

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 system 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 example 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. Refer to the *DR Series Cleaner Best Practices* white paper for guidance on setting up the cleaner.

- 1 In the DR Series system GUI, click **System Configuration > Schedules**.
- 2 On the Action menu, click **Add Cleaner Event**.



- 3 Define the schedule and click **Save**.

New

Only one cleaner event is allowed per day.

Set event from start day: Sunday at: 01 : 00 to end day: Sunday at: 02 : 00

Save Cancel

The new cleaner event is displayed on the Schedules page.

Quest DR4300
dr4300-27.systest.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

09/25/2017 15:53:58
US/Pacific-New

Schedules

Cleaner status: **Done**

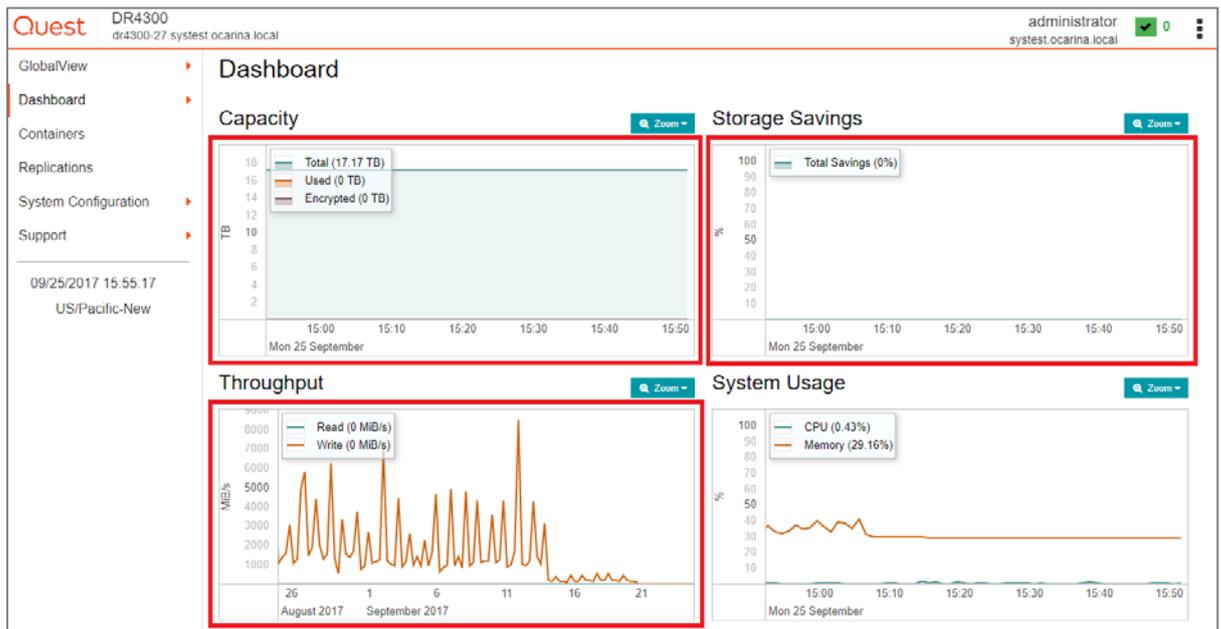
■ Cleaner Schedule All
 ■ Source Replication Schedule All
 ■ Target Replication Schedule All

	Sun	Mon	Tue	Wed	Thu
0:00					
1:00		1:00 - 2:00 Cleaner			
2:00					
3:00					

Monitoring deduplication, compression and performance

After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput in 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.

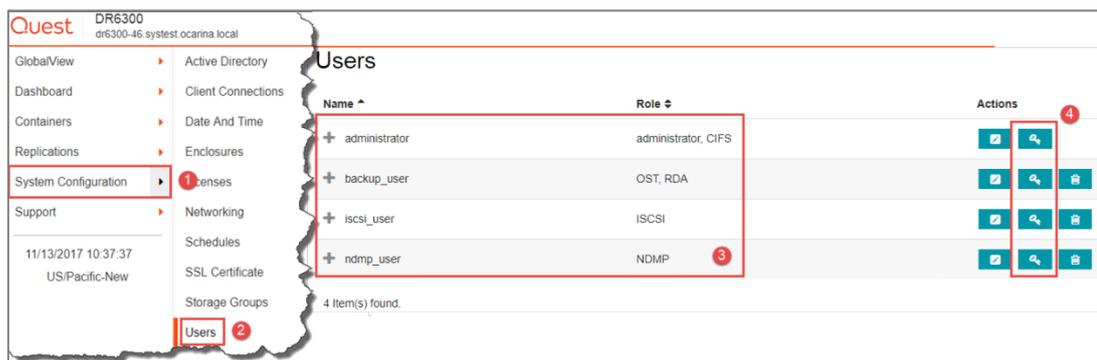


A - VTL configuration guidelines

Managing VTL protocol credentials

Setting the NDMP tape server credentials

The default NDMP password is “St0r@gel”. This can be modified by selecting the System Configuration menu ❶ and clicking Users ❷. On the Users ❸ page click the  icon ❹ on the `ndmp_user` line.



Alternatively, you can use the “`user --setpassword --name <user>`” CLI command to change the NDMP Tape Server Password setting. For example:

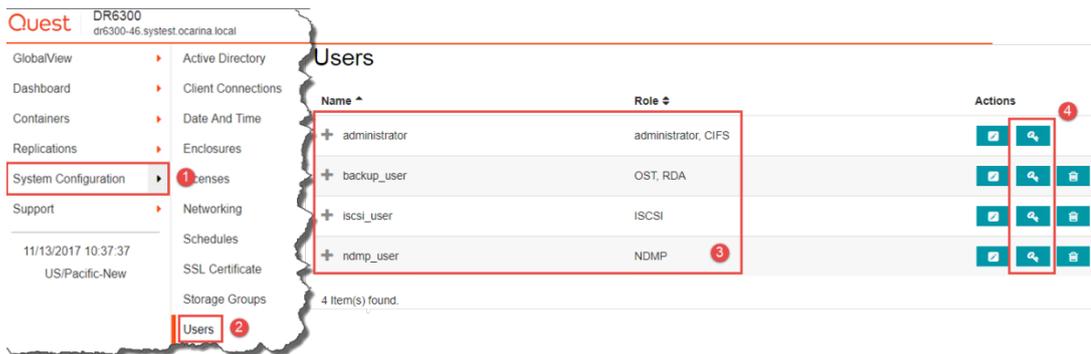
```
> user --setpassword --name ndmp_user  
Enter new password:  
Re-type password:  
Successfully updated User ndmp_user.
```

Setting the iSCSI target CHAP credentials

The default NDMP password is “St0r@geliscsi”. This can be modified by selecting the System Configuration menu ❶ and clicking Users ❷. On the Users ❸ page click the  icon ❹ on the `iscsi_user` line.



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



```

administrator@dr6300-46 > user --setpassword --name iscsi_user

Enter new password:

Re-type password:

WARNING: All existing iSCSI sessions will be terminated!

Do you want to continue? (yes/no) [n]? y

Successfully updated User iscsi_user.
  
```

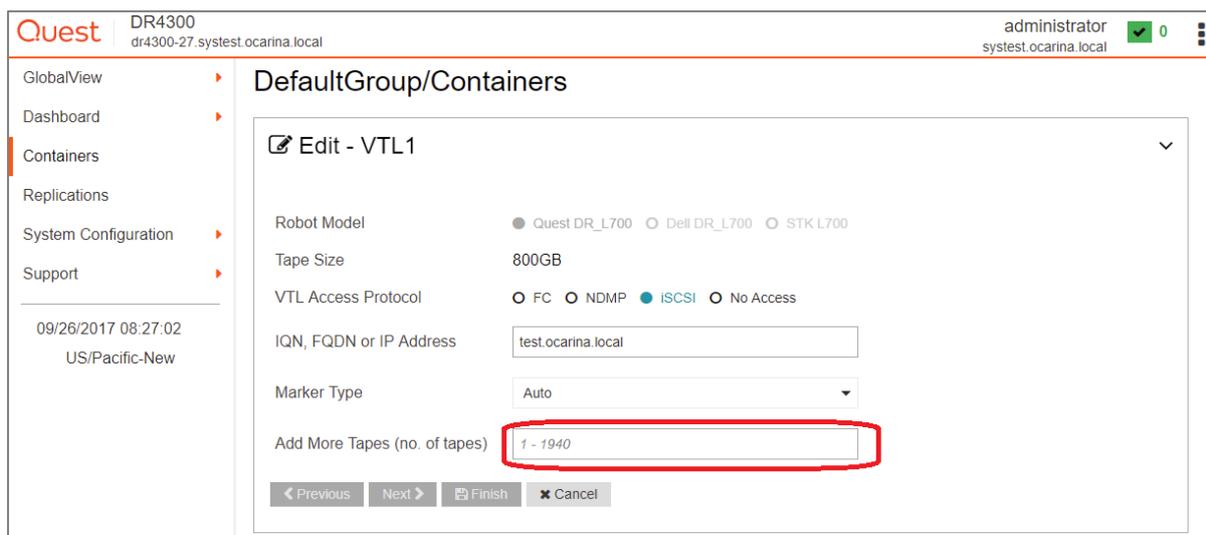
Managing VTL Media

Adding additional media to the VTL container



NOTE: With a VTL container, it is very easy to add additional tapes when required. It is recommended to add tapes in the increments of 50 and 100 to facilitate easy inventory from NetVault: Backup. Check the NetVault: Backup recommendations for the maximum number of tapes supported.

To add media to an existing VTL container Click the Containers menu, then click the  Edit Icon on the corresponding VTL. Use the resulting wizard field Add More Tape (no of Tape) to input the number of tapes to add to the VTL container and Click Next. On the view page click Save to finalize the change



Alternatively, you can use the “vtl –update_carts” cli command for this operation. For example:

```
> vtl -update_carts --name TEST_VTL_LALA -add -no_of_tapes 10
Created 10 cartridges
```

Managing VTL space use

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 Quest NetVault, Veritas BackupExec, Veritas 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.

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.

Logical VTL geometry and media size

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: 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		

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, 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.

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



IMPORTANT: With a VTL container, it is very easy to add additional tapes when required. We recommend adding tapes in the increments of 50 and 100 to facilitate easy inventory from NetVault: Backup. Check the NetVault: Backup recommendations for the maximum number of tapes supported.

Space reclamation

General guidelines

The DR Series Virtual Tape Library feature is presented to operating systems and data management applications alike as devices either through iSCSI, NDMP, or FC protocol connectivity. The DMA interfaces with the virtual tape library and all its underlying components including the drives and media through 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.



IMPORTANT: 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.