Setting Up the Dell™ DR Series System as a CIFS or VTL Backup Target on CommVault Simpana

Dell Engineering
June 2015

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release
March 2014	Updated for missed DR replication step.
April 2015	Added VTL Content for v3.2 Release
July 2015	Added content for configuring an iSCSI target on Linux

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2015 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

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

Trademarks used in this text:

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

Table of contents

1 Installing and configuring the DR Series system for use with CommVault Simpana 5

1.1 CommVault Simpana software prerequisites 5

1.2 Installing and configuring the DR Series system 5

2 Configuring CIFS and NFS containers for CommVault Simpana 9

2.1 Creating containers in the DR Series system 9

2.2 Adding the target container(s) to CommVault Simpana 12

2.2 Setting up a single system environment (DR Series system as NFS disk library) 14

2.3 Setting up a replicated system environment 16

2.4 Using the continuous data replicator to replicate client data to a DR Series container 24

3 Configuring VTL for CommVault Simpana 36

3.1 Creating and configuring iSCSI target container(s) for CommVault Simpana 36

3.1.1 Create the iSCSI VTL container for CommVault Simpana 36

3.1.2 Configure the iSCSI Target - Windows 38

3.1.3 Configure CommVault to use the newly created iSCSI VTL 44

3.2 Creating and configuring NDMP target container(s) for CommVault Simpana 56

3.2.1 Create the NDMP VTL container for CommVault Simpana 56

3.2.2 Configure CommVault to use the newly created NDMP VTL 58

4 Setting up the DR Series system cleaner 83

5 Monitoring deduplication, compression, and performance 84

A VTL configuration guidelines 85

A.1 Managing VTL protocol accounts and credentials 85

A.1.1 iSCSI account details and management 85

A.1.2 NDMP account details and management 86

A.2 VTL default account summary table 86

A.3 Managing VTL media and space use 87

A.3.1 General performance guidelines for DMA configuration 87

A.3.2 Physical space sizing and planning 87

A.3.3 Logical VTL geometry and media sizing 88

A.3.4 Media retention and grouping 89

A.3.5 VTL media count guidelines 89

A.3.6 Adding the VTL media to the container 90
A.3.7 Updating CommVault to identify newly added VTL media 91
A.3.8 Space reclamation 94
B Glossary 100

Executive summary

This document provides information about how to set up the Dell DR Series system to run Virtual Synthetic Backup on CommVault Simpana 10. 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 CommVault Simpana screenshots used in this document may vary slightly, depending on the DR Series system firmware version and Simpana version you are using.

1 Installing and configuring the DR Series system for use with CommVault Simpana

1.1 CommVault Simpana software prerequisites

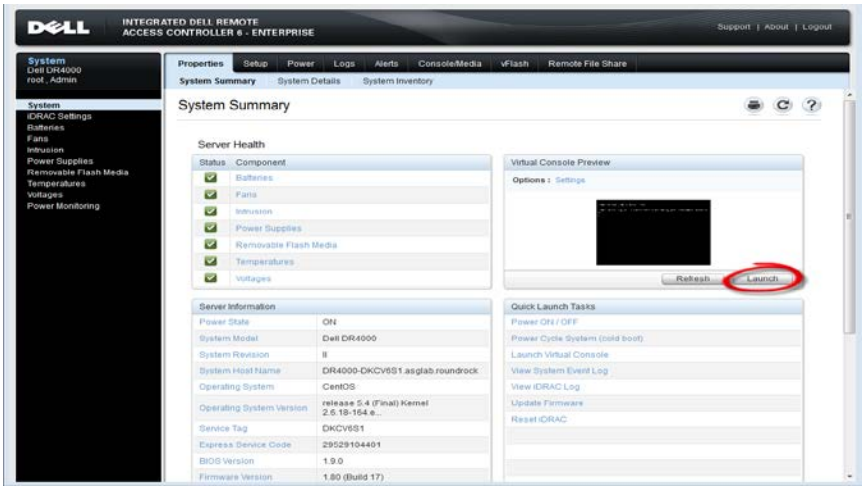
This guide applies to versions of CommVault Simpana version 10 and later. The screenshots used in this document may vary slightly, depending on the version of the software you are using.

For CommVault version 10, there are patch requirements to add support for NDMP VTL. Refer to the CommVault documentation for more information 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 more information about using the iDRAC connection and initializing the DR Series system.

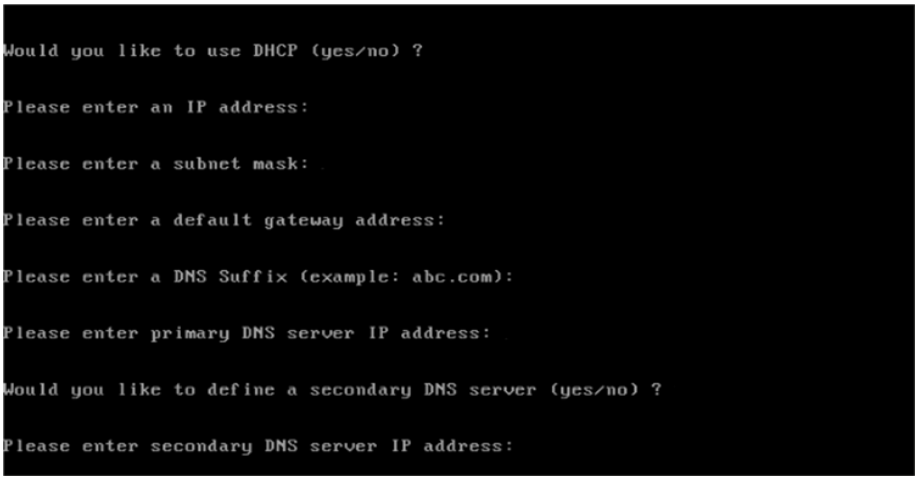
2. Log on to iDRAC using the default address **192.168.0.120**, or the IP address that is assigned to the iDRAC interface. Use the user name and password: "**root/calvin**".



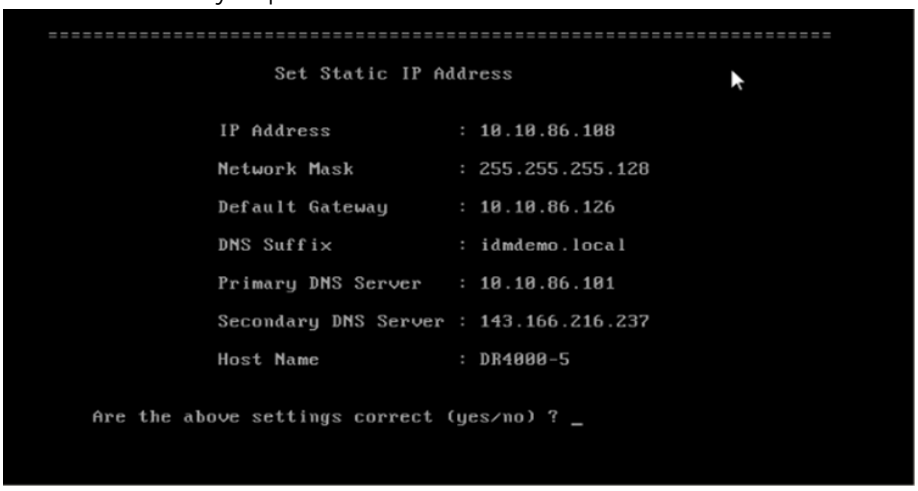
3. Launch the virtual console.

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).

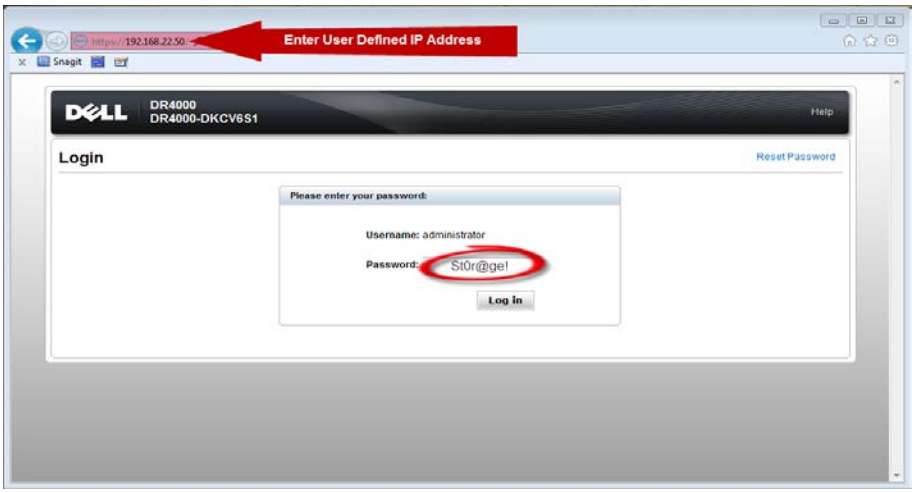
5. Set the user-defined networking preferences.



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



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

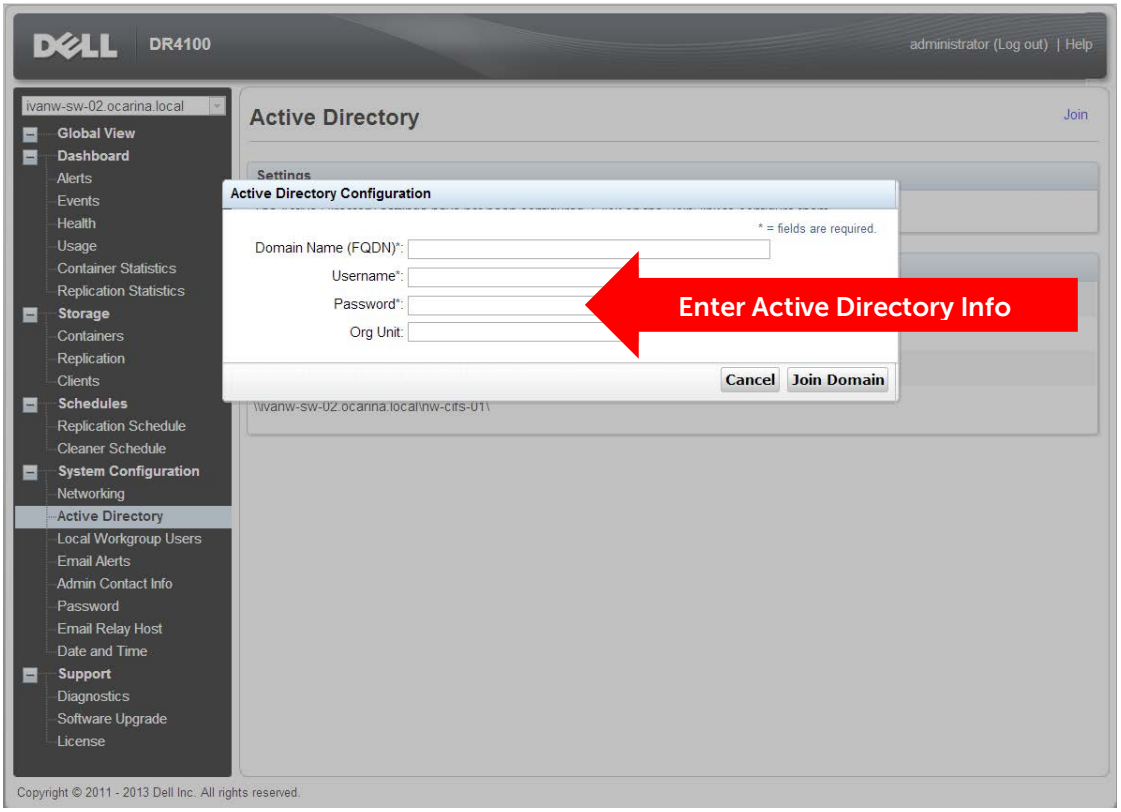


8. Join the DR Series system into the Active Directory domain.

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

a. Select **Active Directory** from the left navigation area of the DR Series system GUI.

b. Enter your Active Directory credentials.

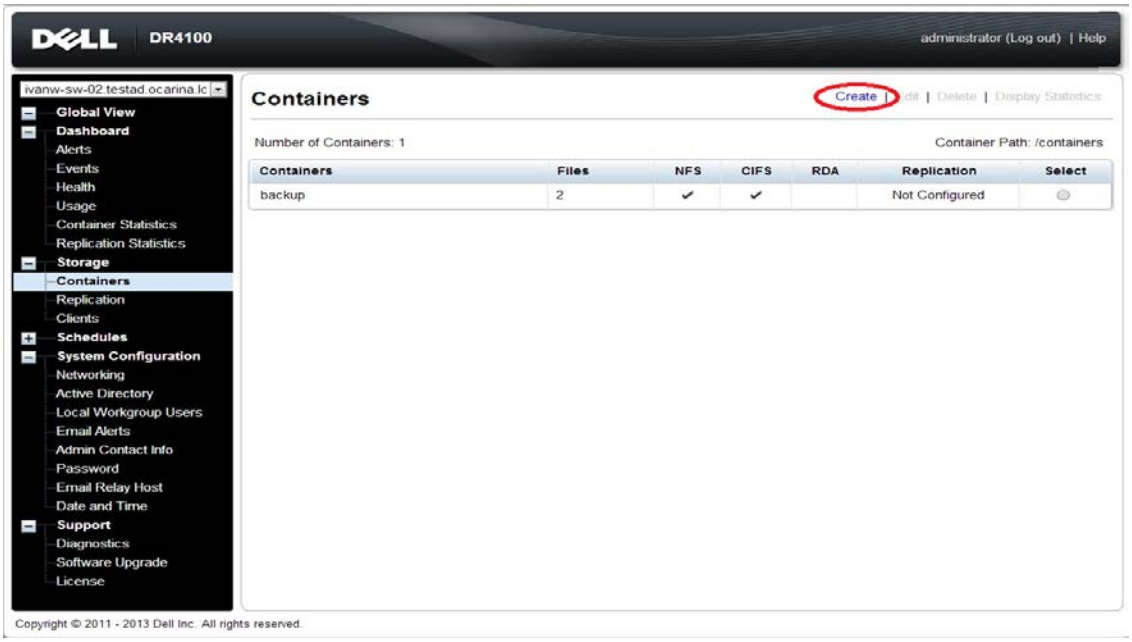


2 Configuring CIFS and NFS containers for CommVault Simpana

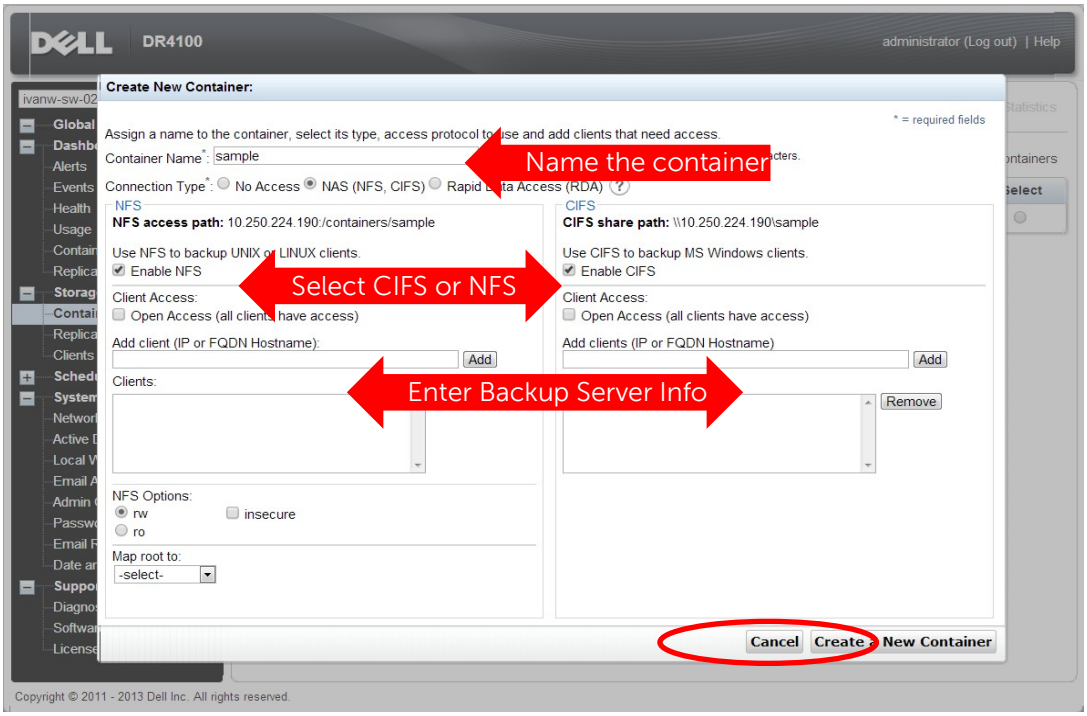
2.1 Creating containers in the DR Series system

For this procedure, you will need to create and mount the container.

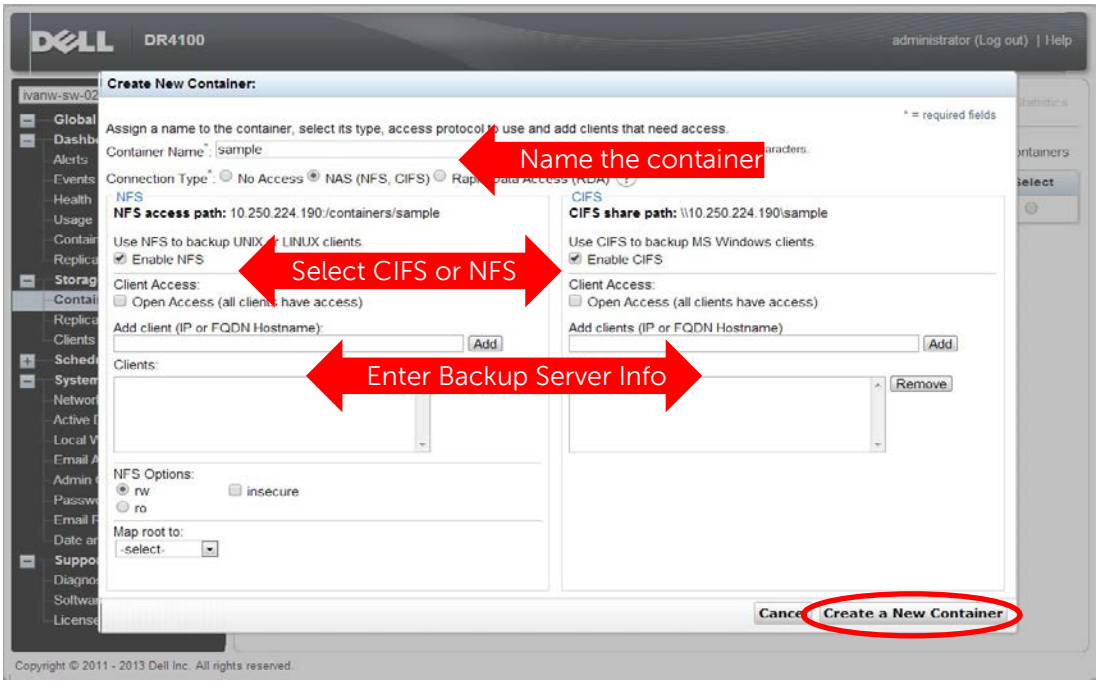
1. Select **Containers** in the left navigation area of the DR Series system GUI, and then click **Create** at the top of the page.



2. Enter a **Container Name**, and select the **Enable CIFS** or **Enable NFS** check box as appropriate. (CommVault Simpana supports both CIFS and NFS protocols.)

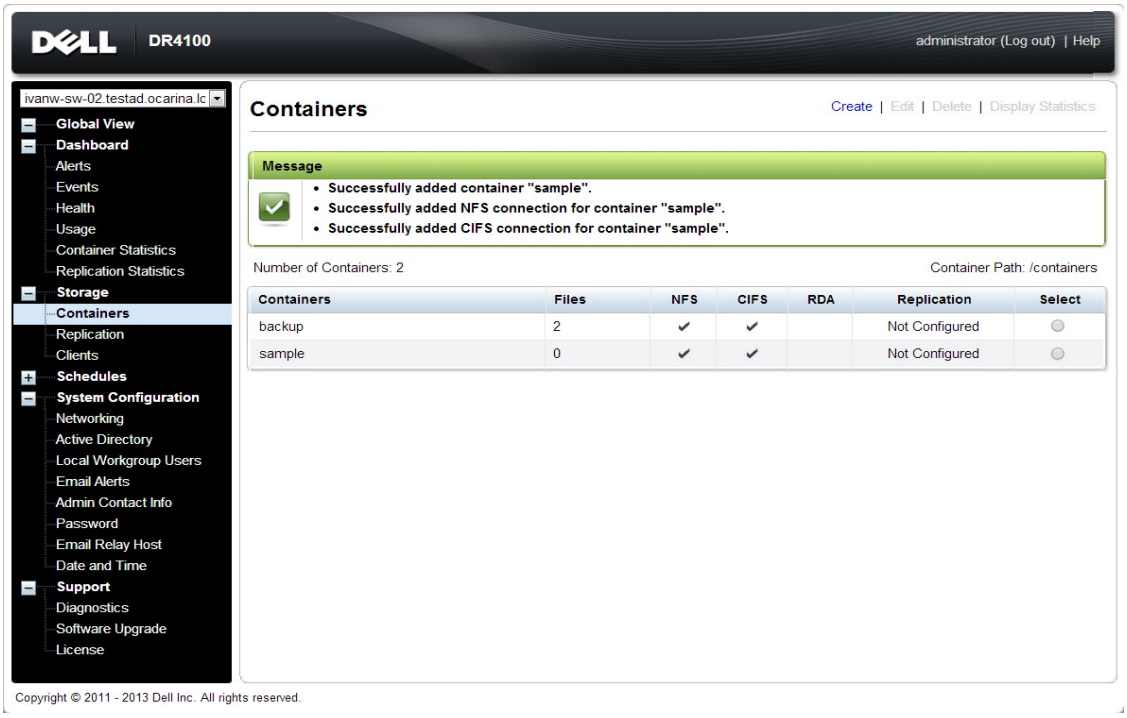


3. Select the preferred client access credentials.

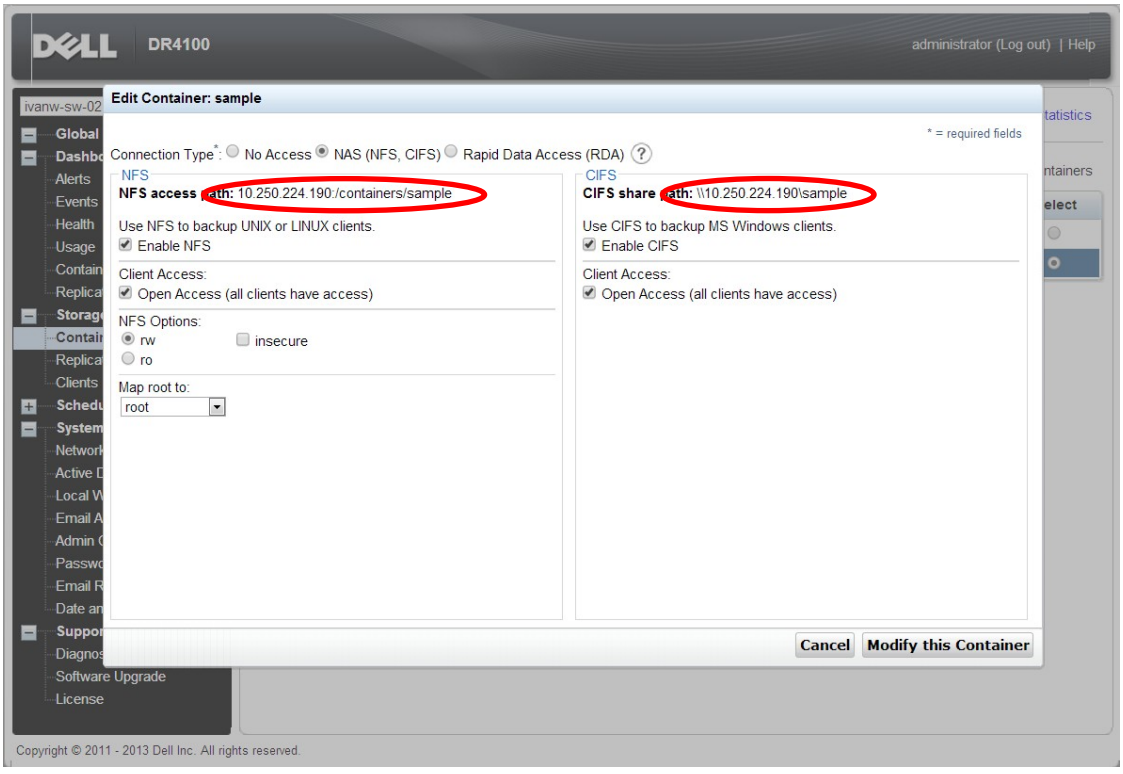


Note: For improved security, Dell recommends adding IP addresses for the following: Backup console (CommVault Server, CommVault Media Agents). (Not all environments will have all components)

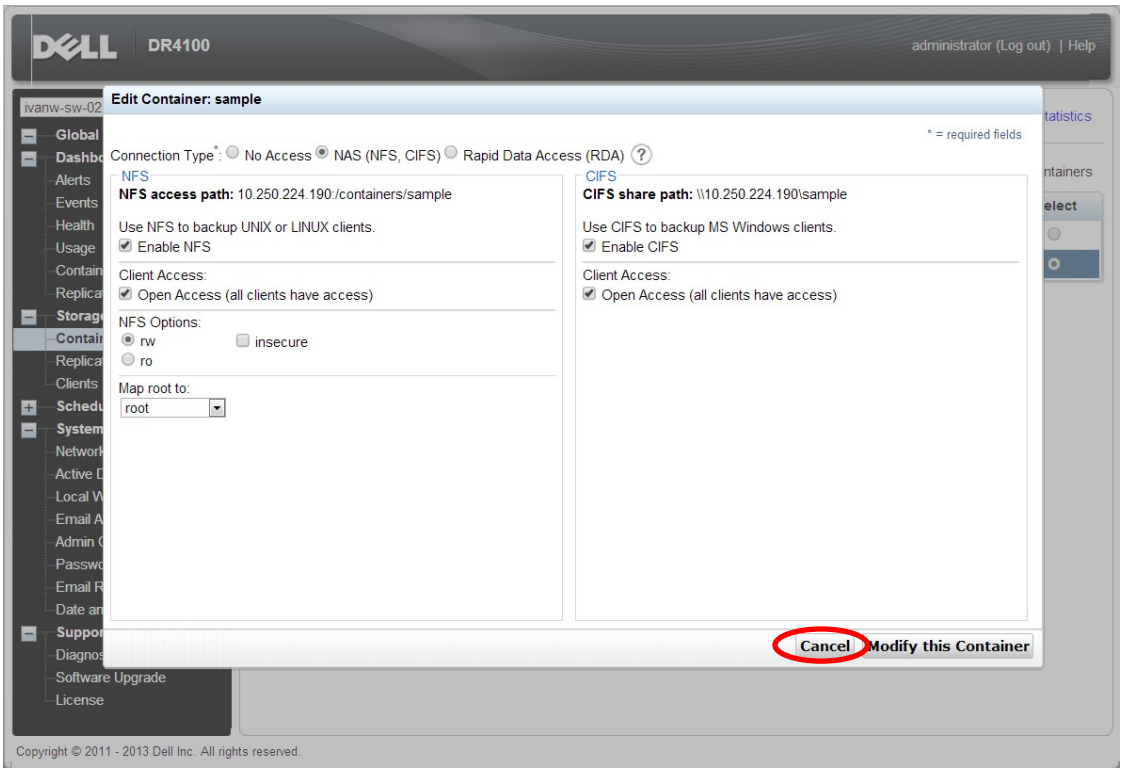
4. Click **Create a New Container**. Confirm that the container is added.



5. Select the container and click **Edit**. Note down the container share/export path, which will be used later as the Disk Library for CommVault Simpana.

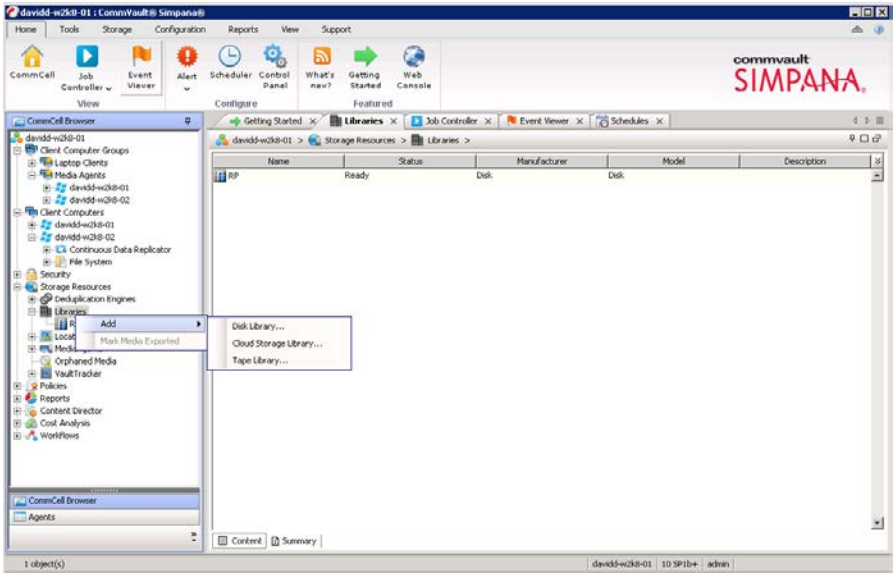


7. Click **Cancel** to exit.

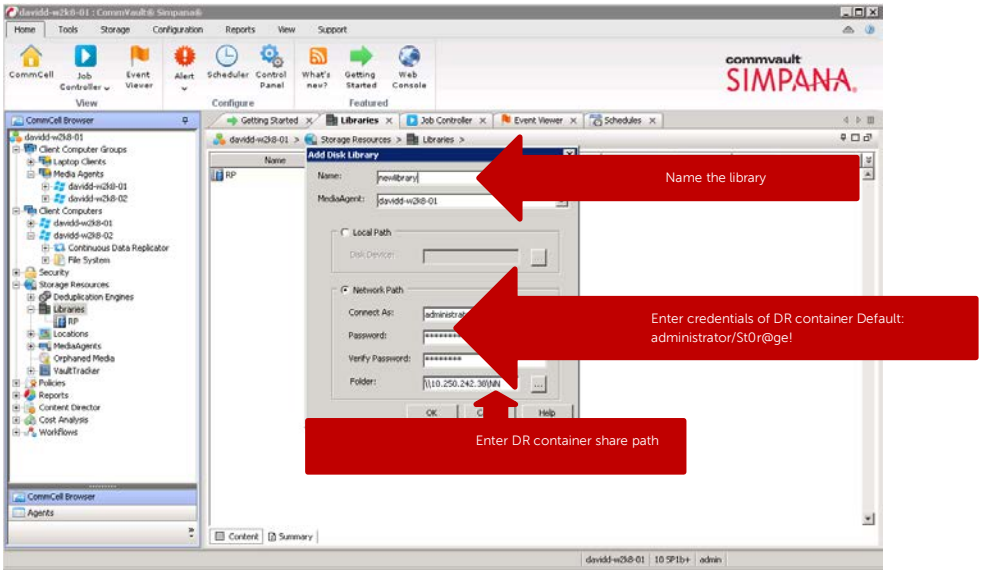


2.2 Adding the target container(s) to CommVault Simpana

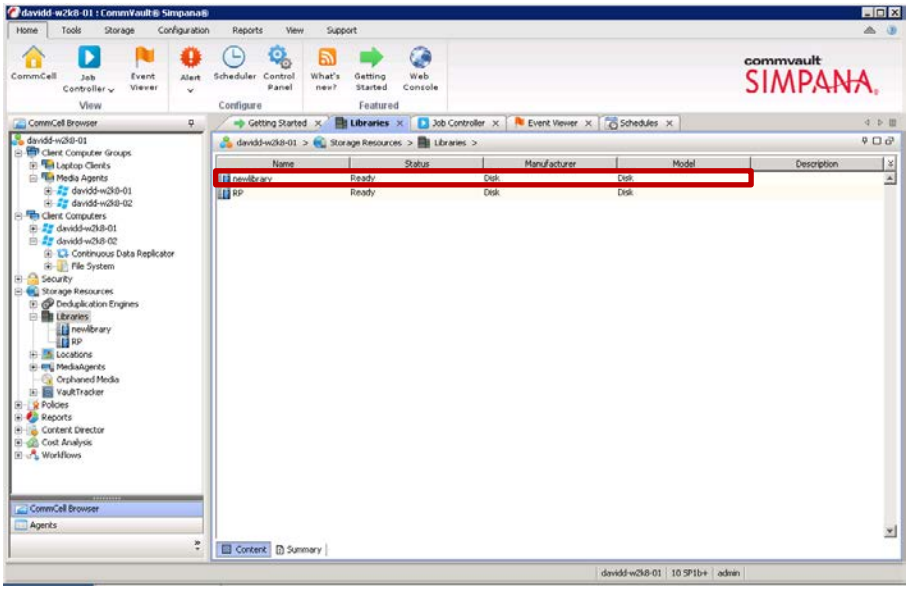
1. Open the **Simpana Administrative Console**, expand **Storage Resources**, right-click **Libraries**, and select **Add** –> **DiskLibrary...**



2. In the **Add Disk Library** window, enter a name for the Disk Library and the information about the DR Series system container, and click **OK**.

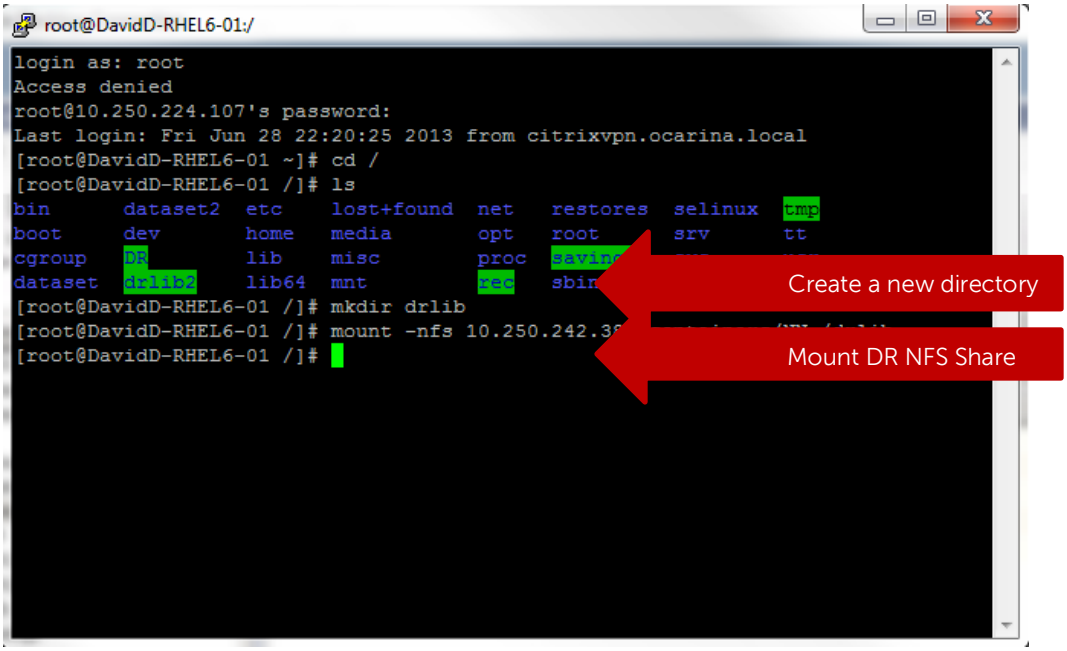


3. Confirm that the library is created, and that the status is **Ready**.

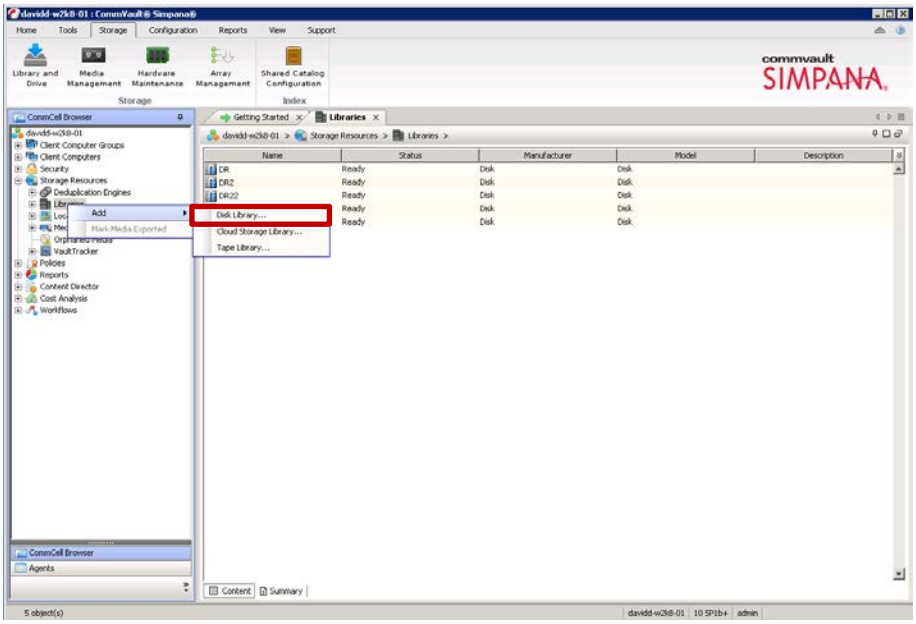


2.2 Setting up a single system environment (DR Series system as NFS disk library)

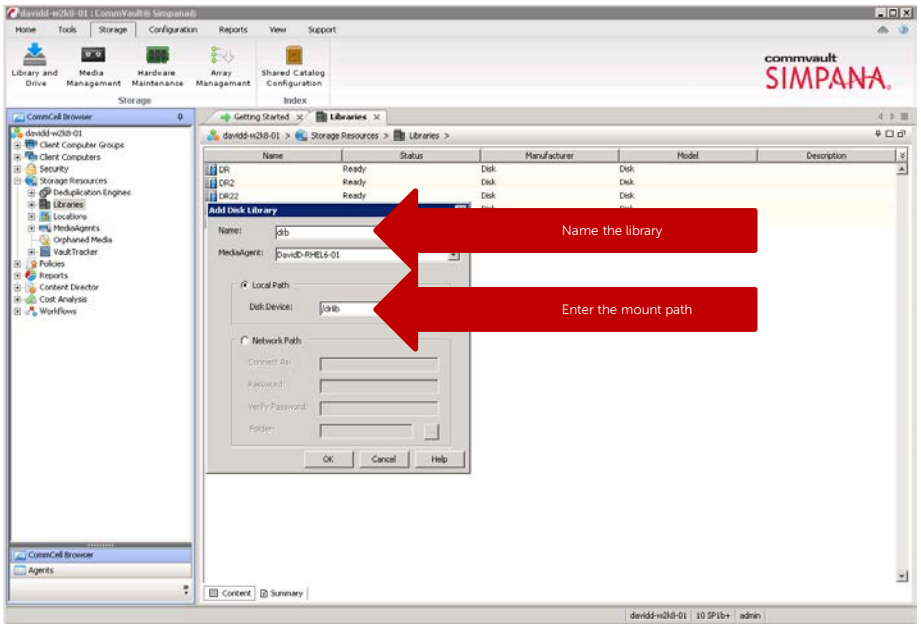
1. Mount the DR container NFS export onto a Unix/Linux Media Agent.



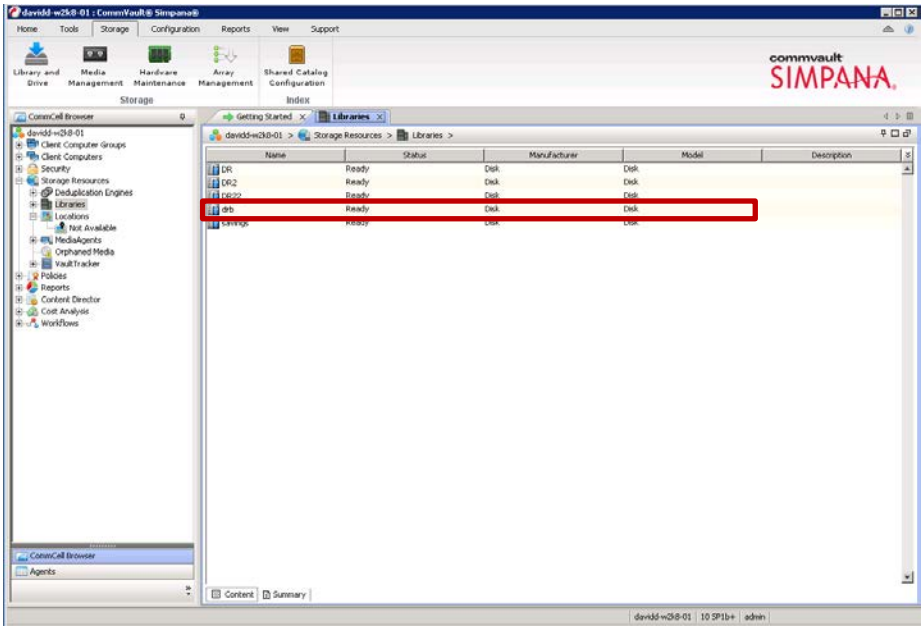
2. Open the **Simpana Administrative Console**, expand **Storage Resources**, right-click **Libraries**, and select **Add** –> **DiskLibrary...**



3. In the **Add Disk Library** window, enter the name for the **Disk Library** and the mount path of DR container export, and click **OK**.



4. Confirm that the library is created, and the **Status** is **Ready**.

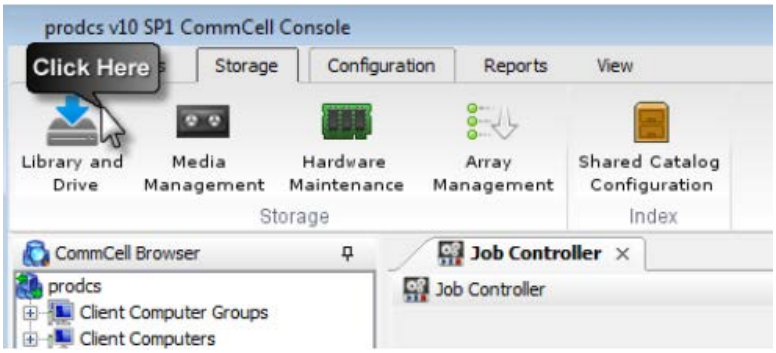


2.3 Setting up a replicated system environment

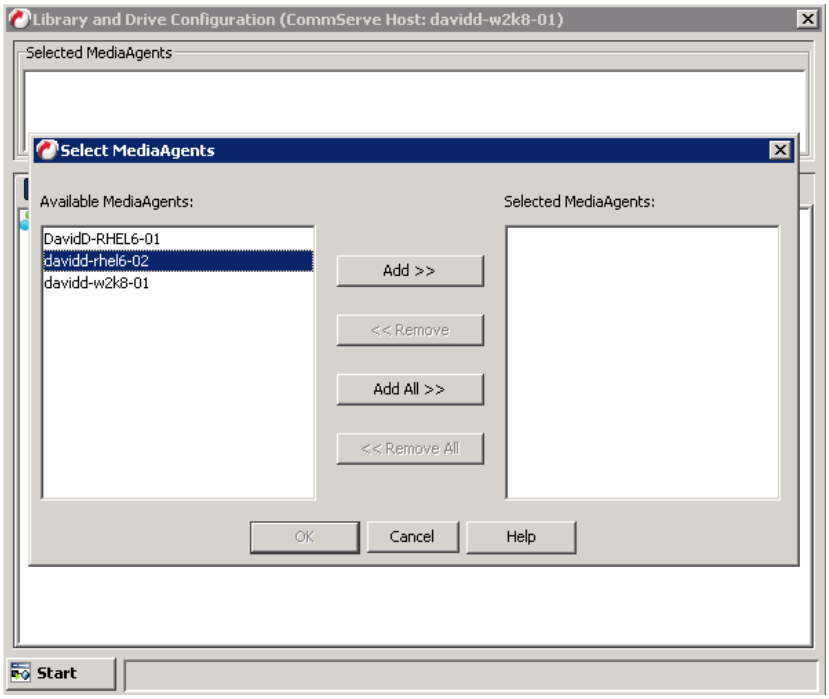
The replicated system environment includes a minimum of two DR Series systems that are connected to two different Media Agents. For more details, please refer to the CommVault documentation:

http://documentation.commvault.com/hds/v10/article?p=features/remote_office/remote_office_how_to.htm

1. On **CommCell Console**, click **Storage** then **Library and Drive**.



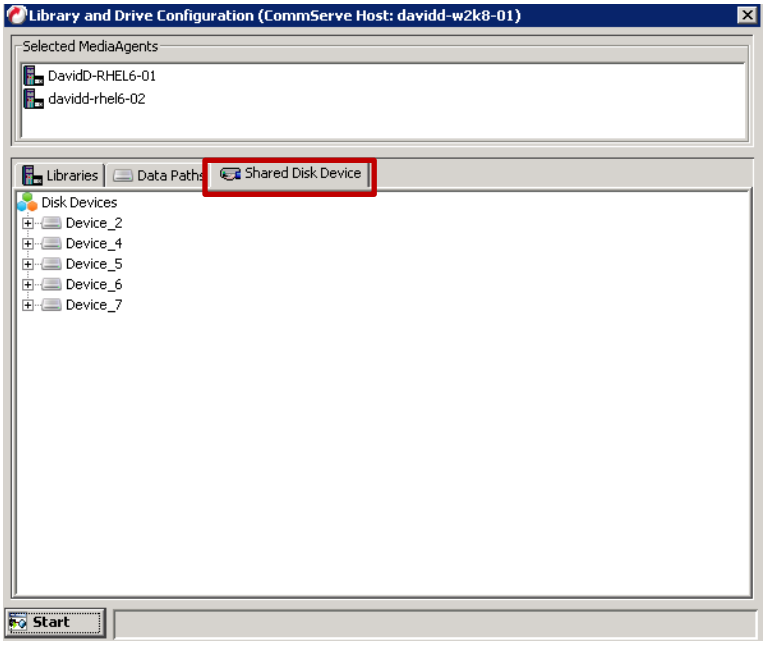
2. Select all the MediaAgent(s) that will participate in replication, click **Add** to add to **Selected MediaAgents**, and then click **OK**.



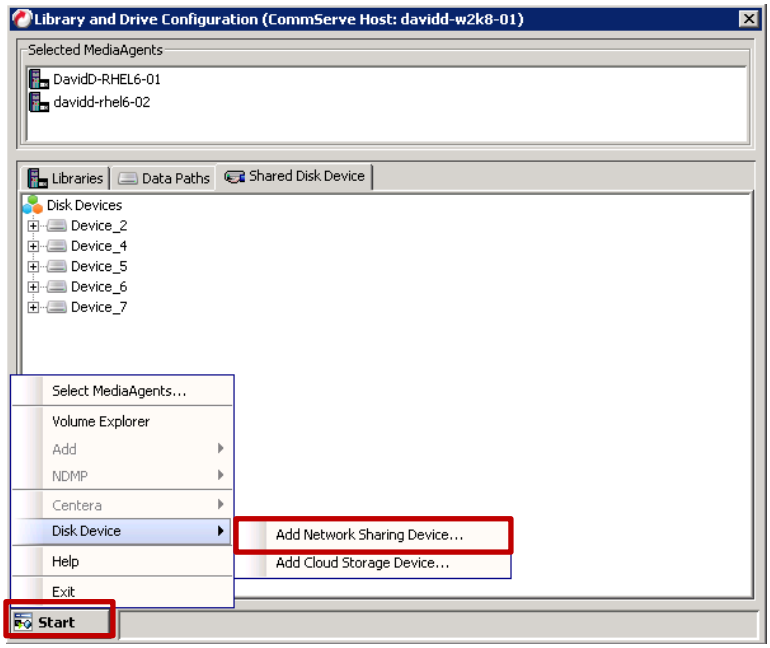
Note: To configure a shared library, make sure you select all the MediaAgents that share that library.

3. Click **OK** to continue.

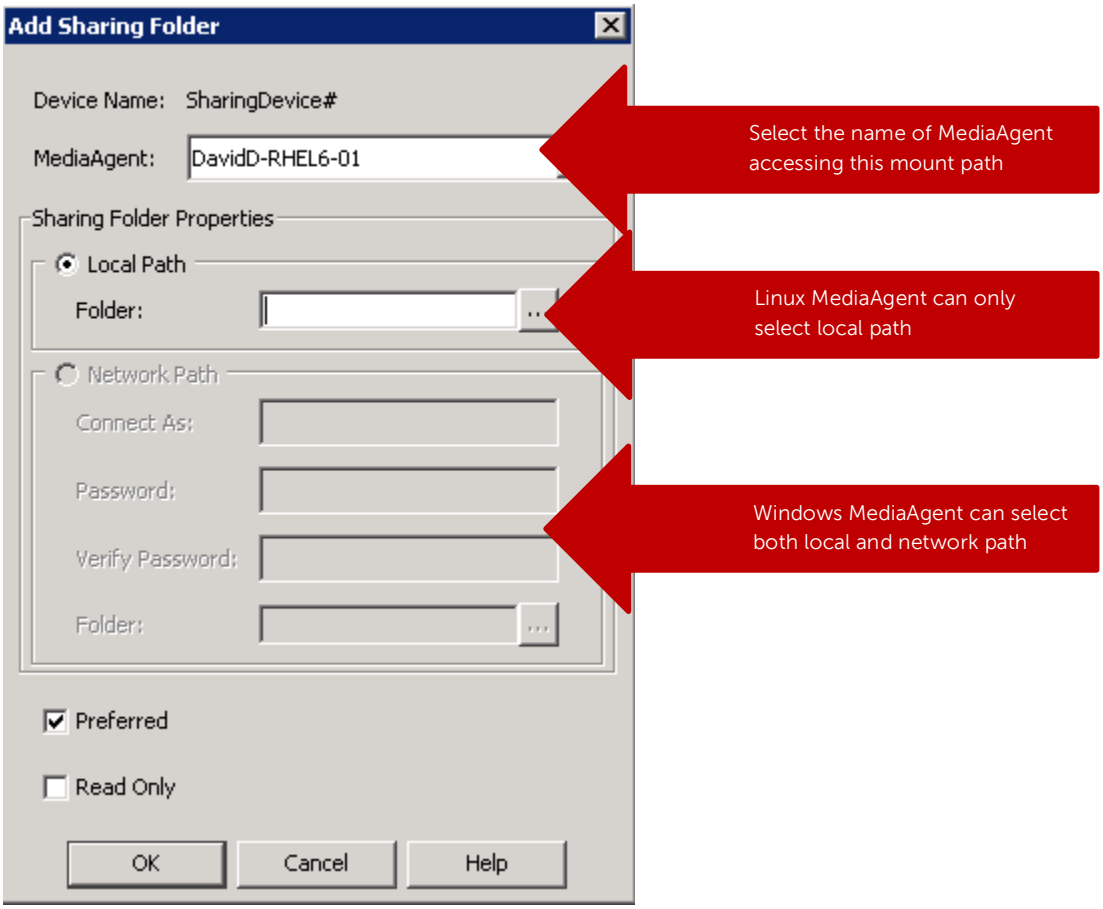
4. Click the **Shared Disk Device** tab.



5. Click **Start**, and select **Disk Device** > **Add Network Sharing Device...**

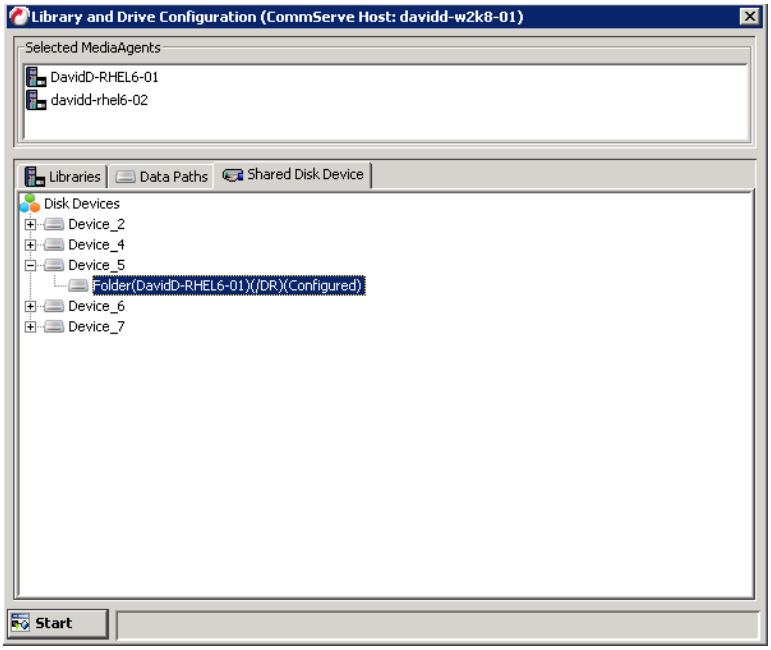


6. In the **Add Sharing Folder** dialog box, enter the source DR container share/export information and then click **OK**.

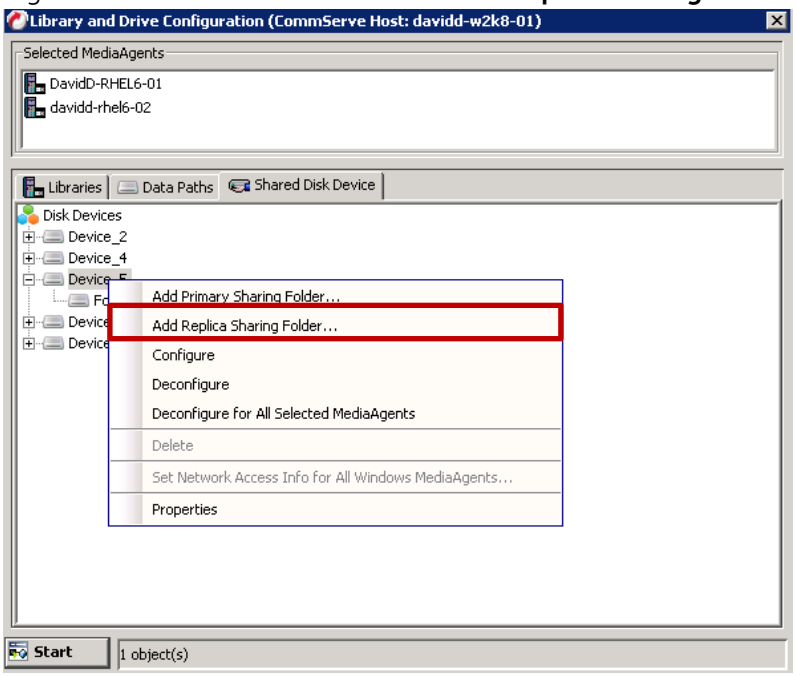


Note: This Device is the replication source. Device information is based on which protocol the container is exposed to the MediaAgents.

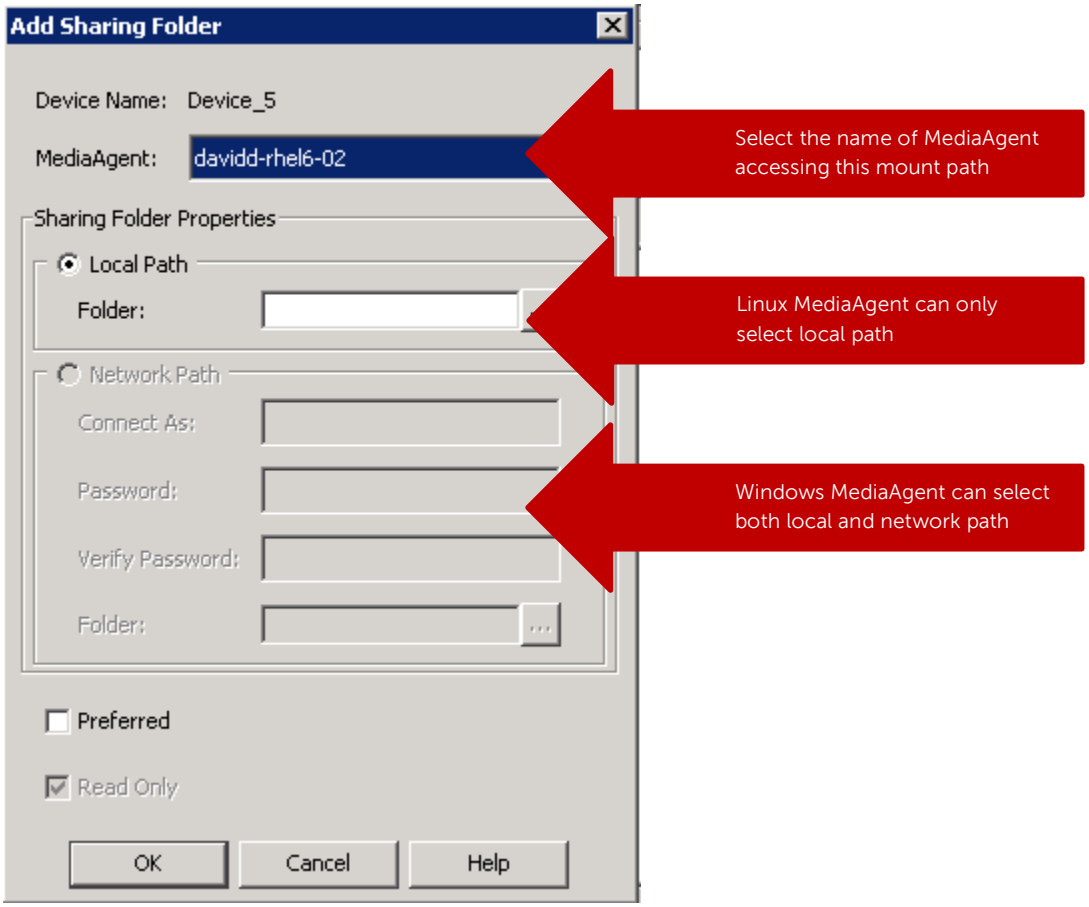
7. The system displays the device information with the **MediaAgent** that can access the device in **Library and Drive Configuration** window.



8. Right-click the device and then click **Add Replica Sharing Folder**.

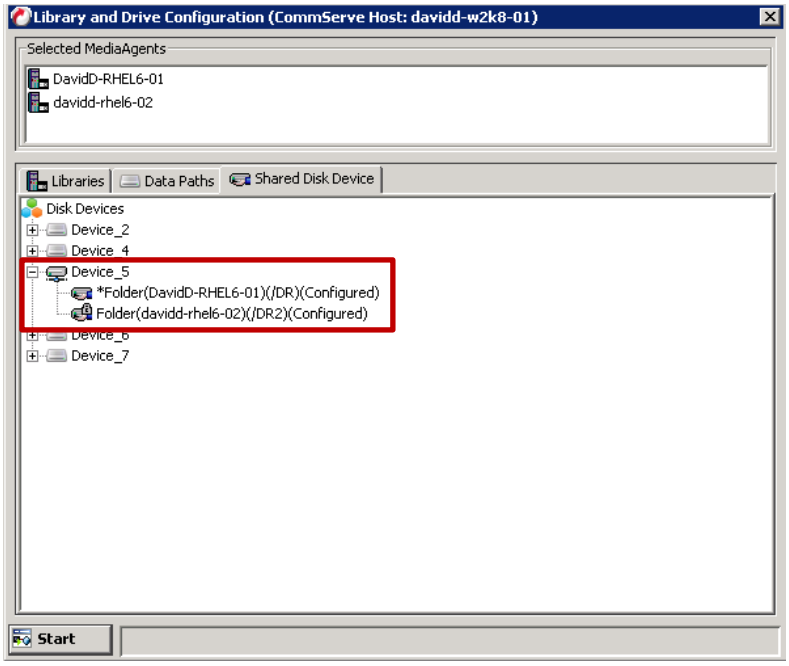


9. In the **Add Sharing Folder** dialog box, enter the target DR container share/export information and then click **OK**.

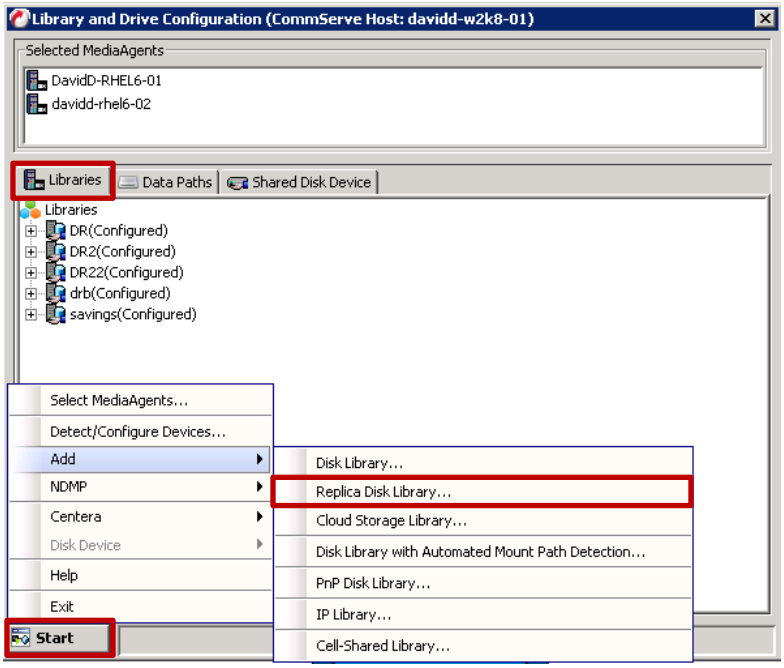


Note: This Device is the destination of the replication. Device information is based on which protocol the container is exposed to the MediaAgents.

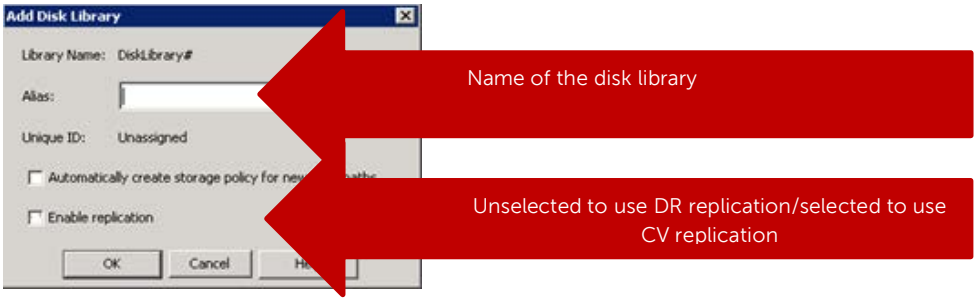
10. The system displays the device information with which MediaAgent can access the device in the **Library and Drive Configuration** window.



11. On the **Libraries** tab, click the **Start** menu, and select **Add** -> **Replica Disk Library**.



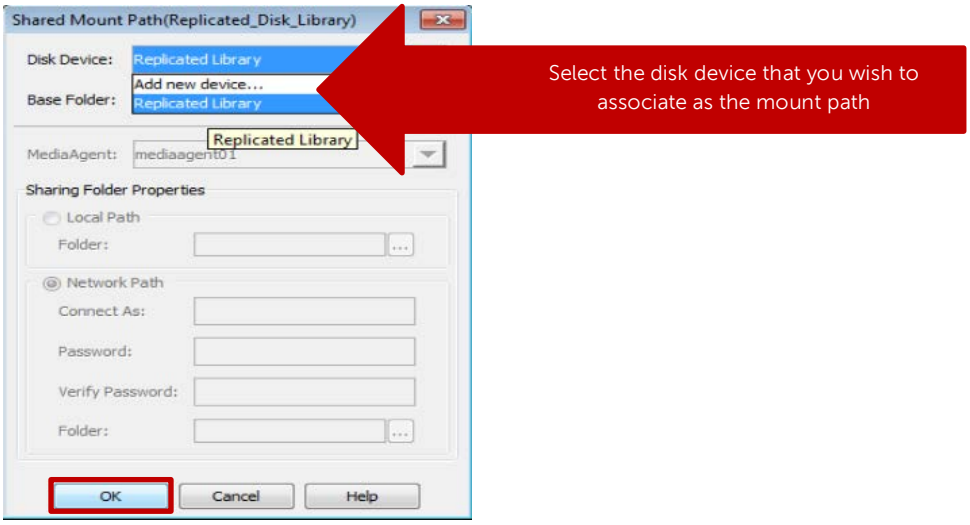
12. In the Add Disk Library dialog box, enter the **Alias** and clear the **Enable replication** checkbox.



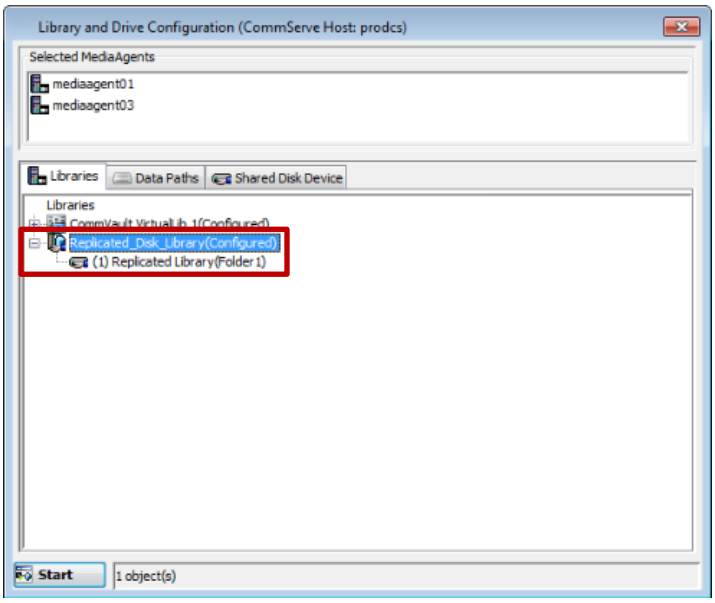
NOTE: **Enabling Replication**:

- For the Disk Library Replication solution, select this option to use ContinuousDataReplicator to replicate data between the source (shared folder added in Step 7) and the destination (shared folder added in Step 10) mount paths. Leave this option unselected if you do not want CommVault to manage replication between the two DR Series systems.
- Selecting this option will automatically create a new replication set and a replication pair under ContinuousDataReplicator, when a mount path is added to this library. These replication sets and replication pairs can be monitored from the CommCell Console. It is highly recommended not to change the default settings of the replication sets, or delete the replication sets when the replication is in progress.
- If this option is selected, make sure to install the ContinuousDataReplicator package on the source and the destination computers before adding mount path to this library. Click **OK**.

13. In the **Share Mount Path** dialog box, select the device configured in step 5-10, which has two sharing folders on both the replication source an replication target, and then click **OK**.



14. Verify the disk library is configured.



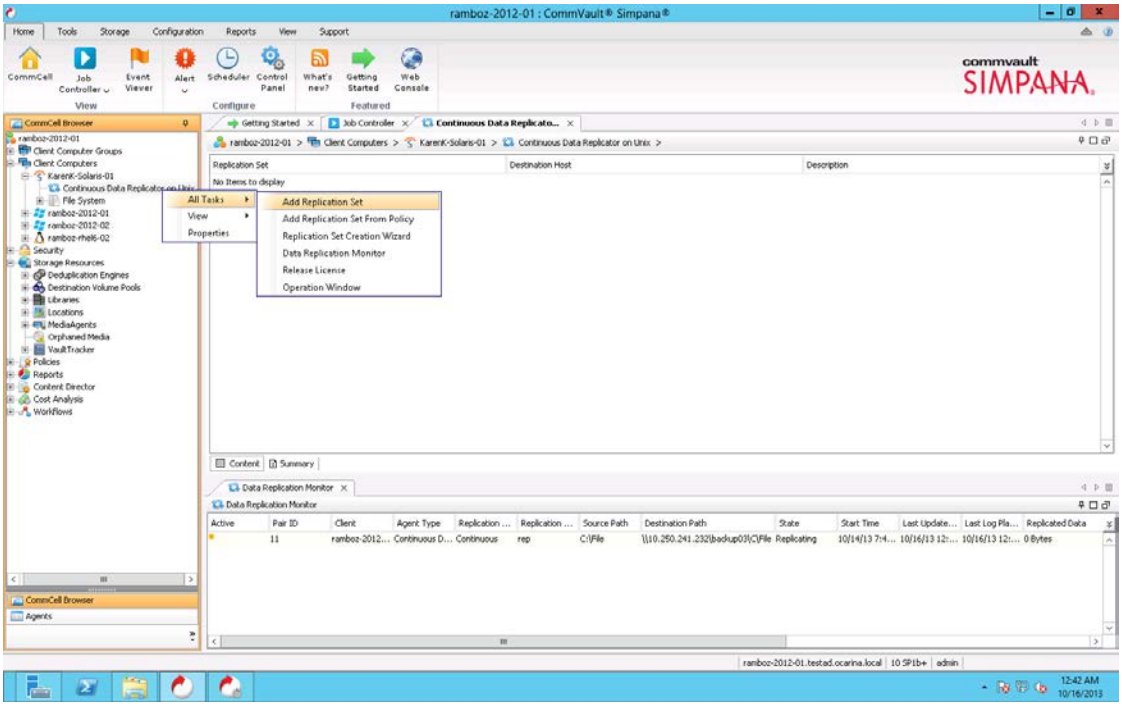
2.4 Using the continuous data replicator to replicate client data to a DR Series container

ContinuousDataReplicator (CDR) replicates data from a source computer to a destination computer, with both computers supporting the same network transfer protocol.

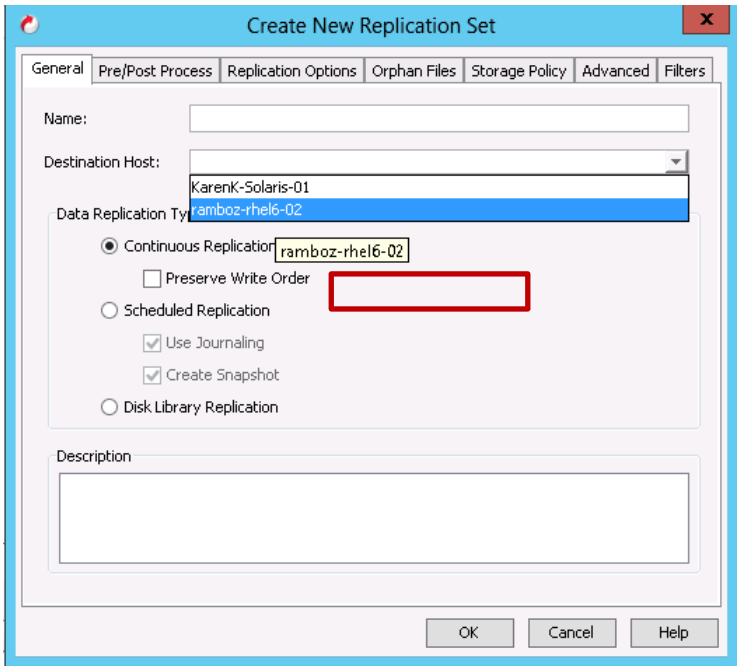
In this configuration, CDR replicates between a client and a DR Series system container. The CDR package should be installed on both media agents associated with this configuration. For more details, refer to the CommVault documentation:

http://documentation.commvault.com/commvault/release_10_0_0/books_online_1/english_us/prod_info/flr.htm

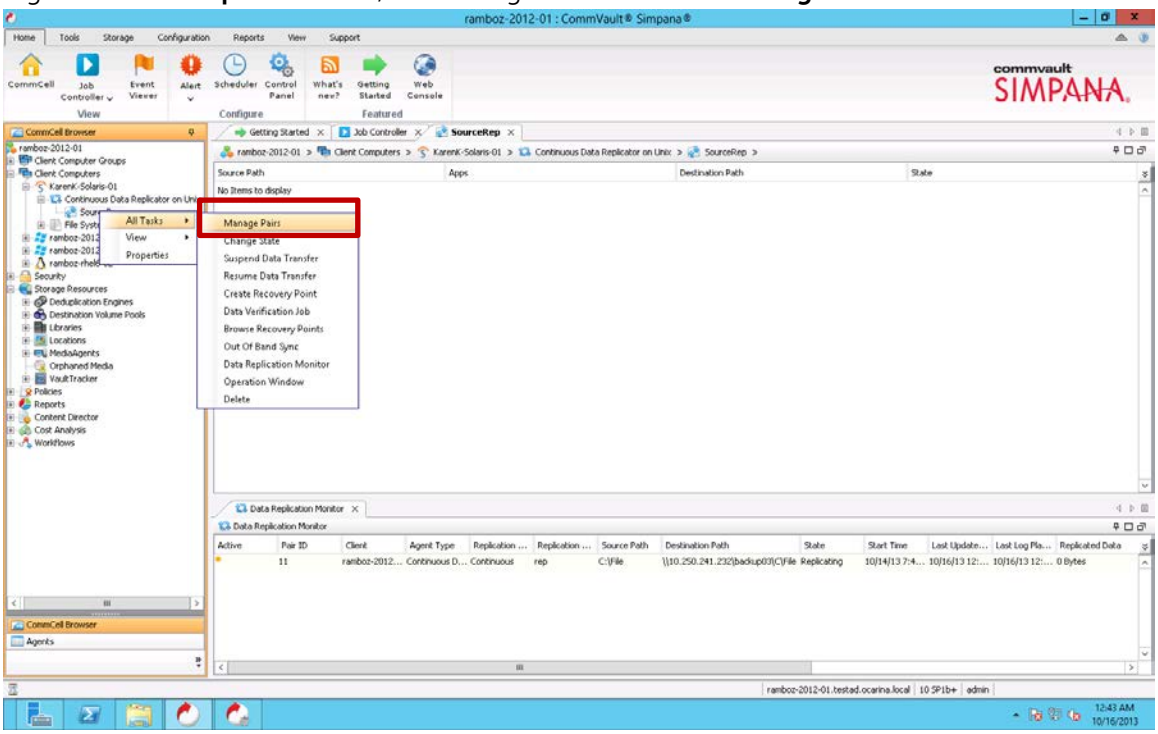
1. From **CommCell Console**, pick the client that a dataset needs to be replicated to the DR Series system. Right-click and select **Continuous Data Replicator** -> **All Tasks** -> **Add Replication Set**.



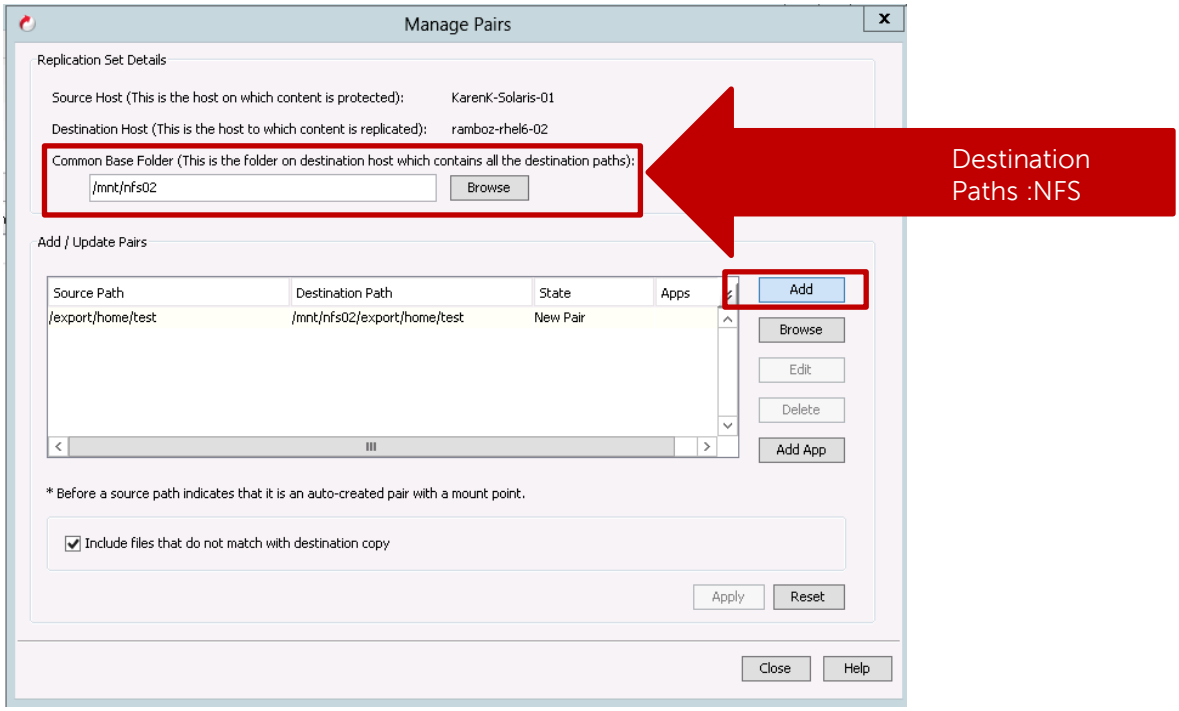
2. In the **Create New Replication Set** window, enter the **Name** for the Replication Set, and select **Destination Host** from the dropdown list. This is the client machine that has the DR container mounted (CIFS or NFS). Click **OK**.



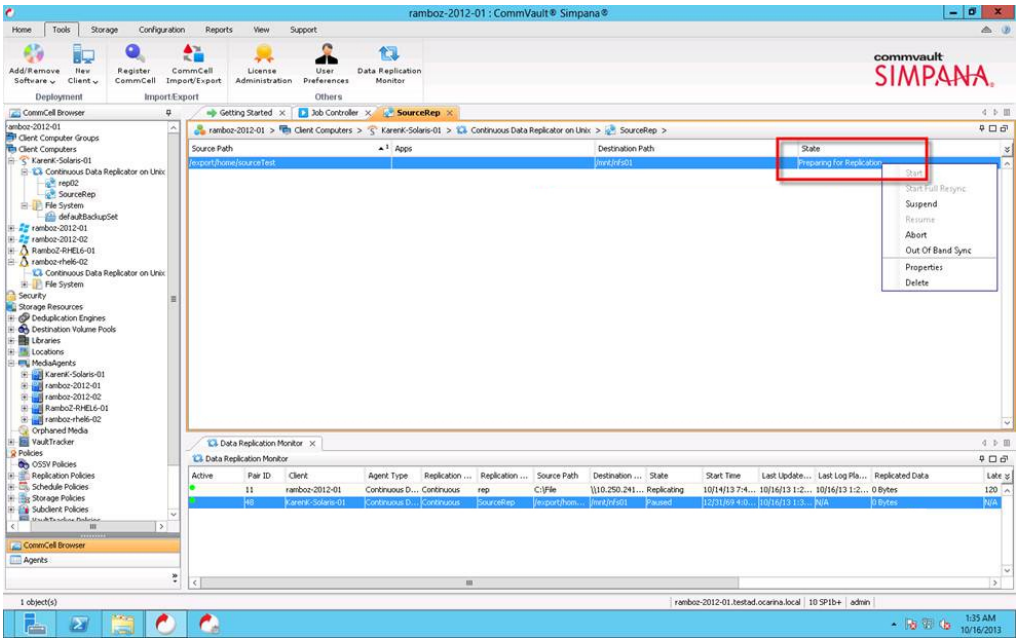
3. Right-click the **Replication Set**, and then go to **All Tasks** -> **Manage Pairs**.



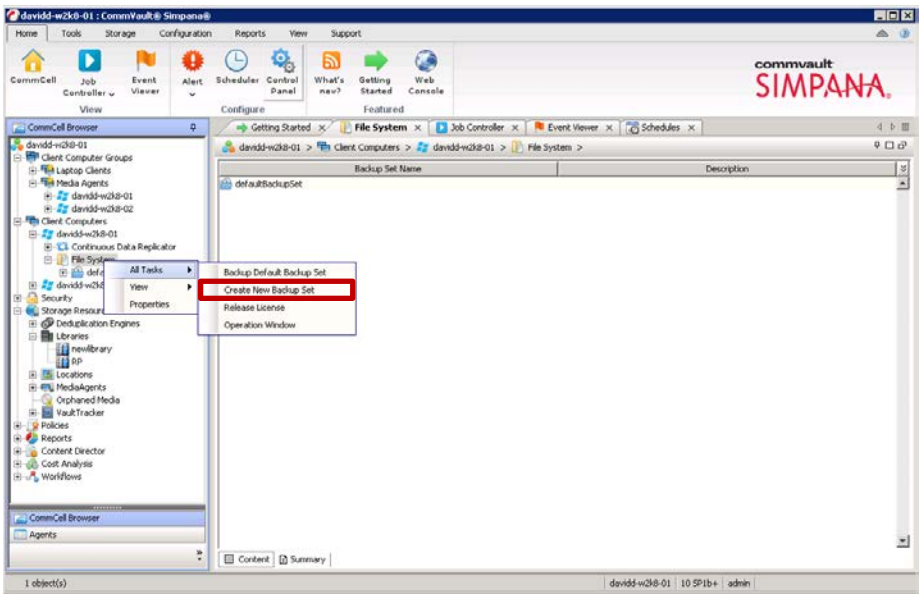
4. For **Common Base Folder**, enter the path pointing to the DR container share/export. Click **Add**-> select the Destination Path and click **Close**.



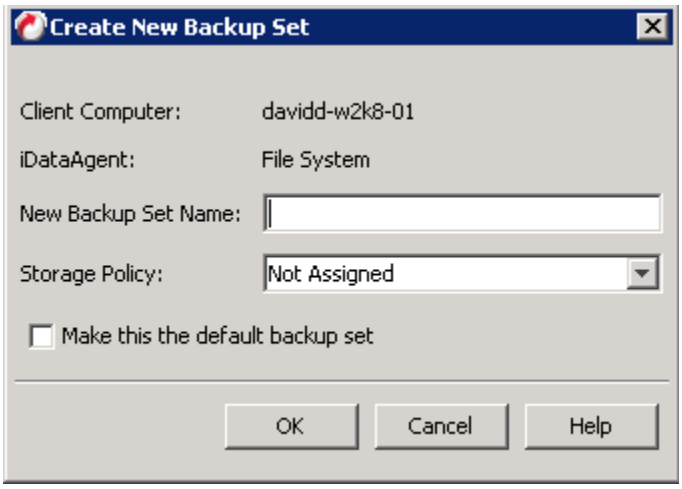
5. Right-click the managed pairs under the replication set. Select **Start/Start Full Resync** and monitor the **State**.



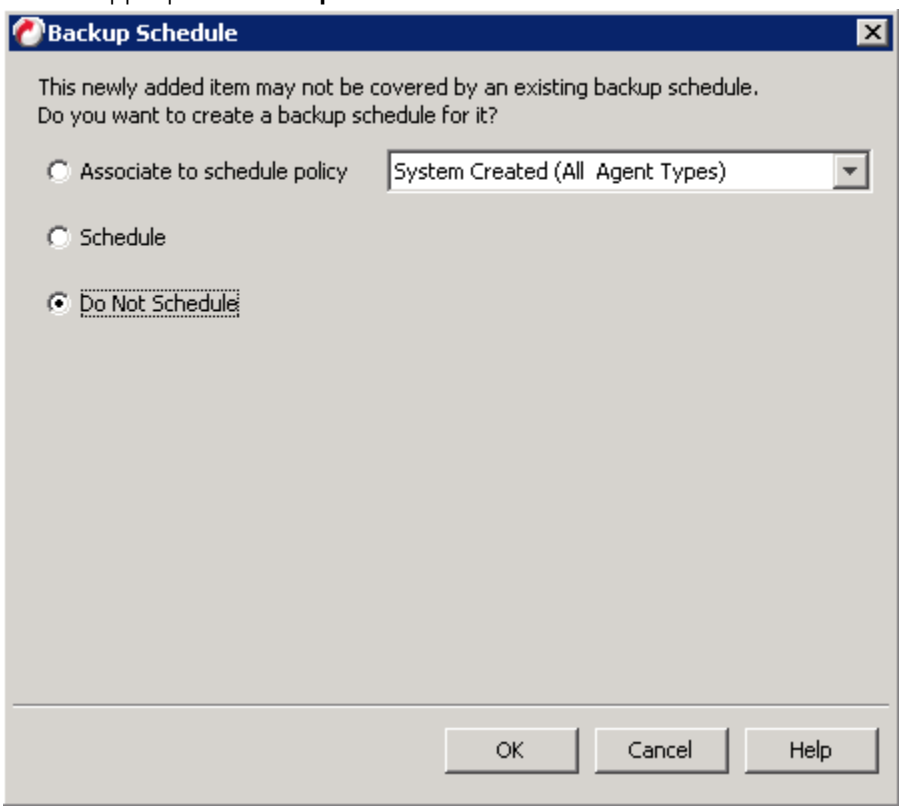
6. Expand the client to be backed up, right-click the target iDataAgent, and then select **All Tasks** –> **Create New Backup Set**.



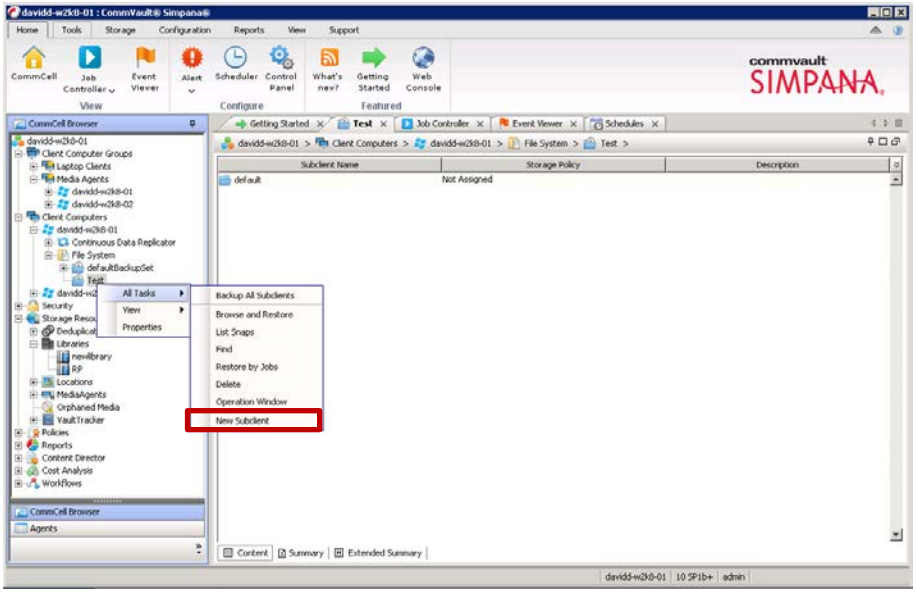
7. Enter the New Backup Set Name.



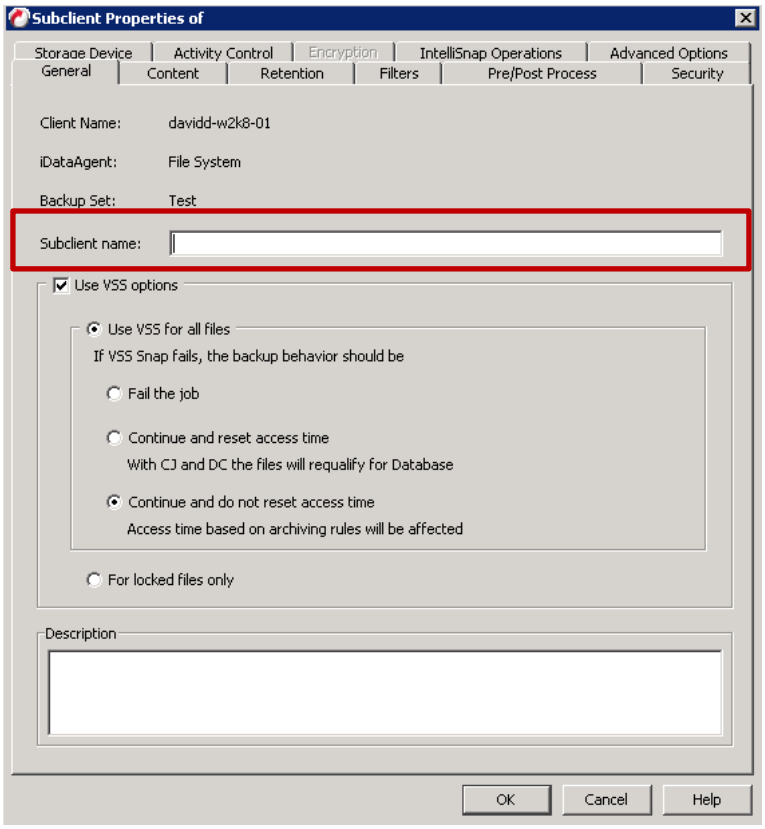
8. Set the appropriate **Backup Schedule**



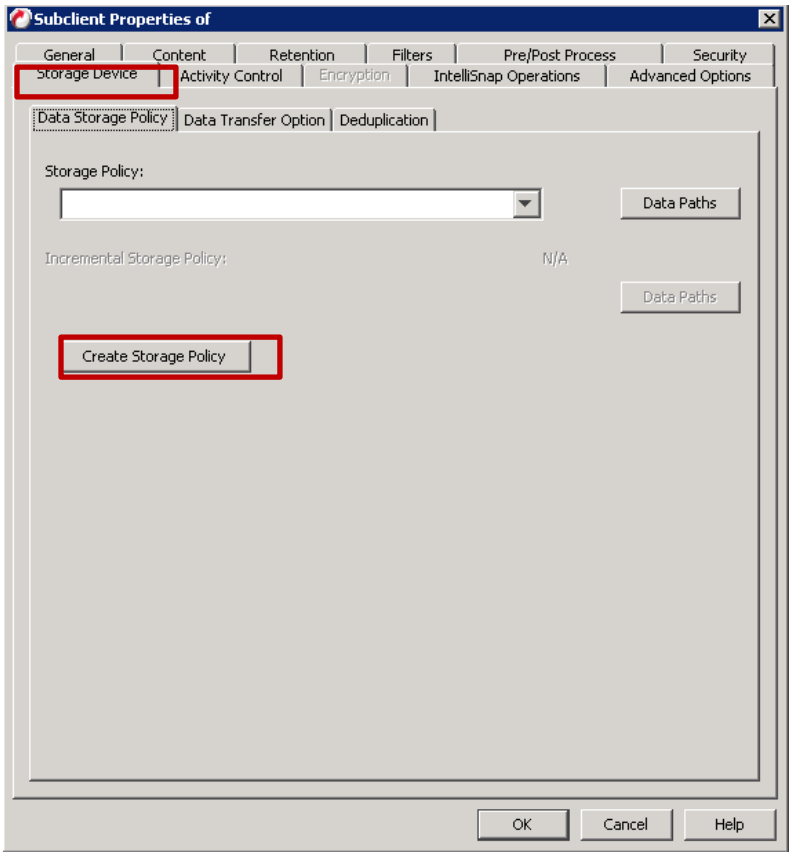
9. Right-click the newly created Backup Set, and select **All Tasks** -> **New Subclient**.



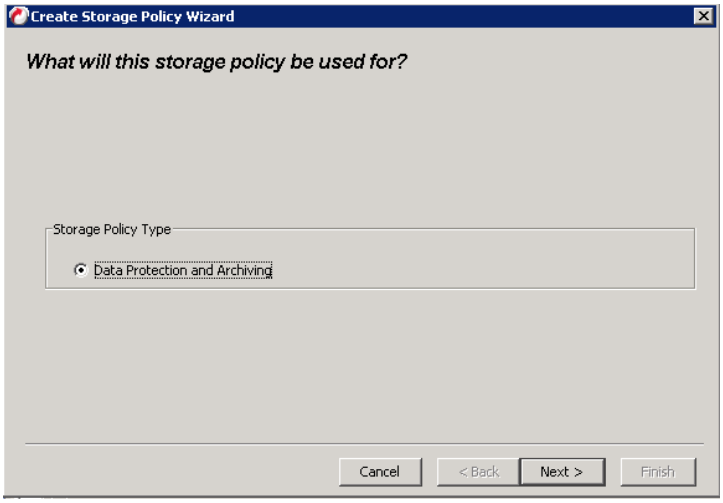
10. Enter the **Subclient name** on the **General** tab.



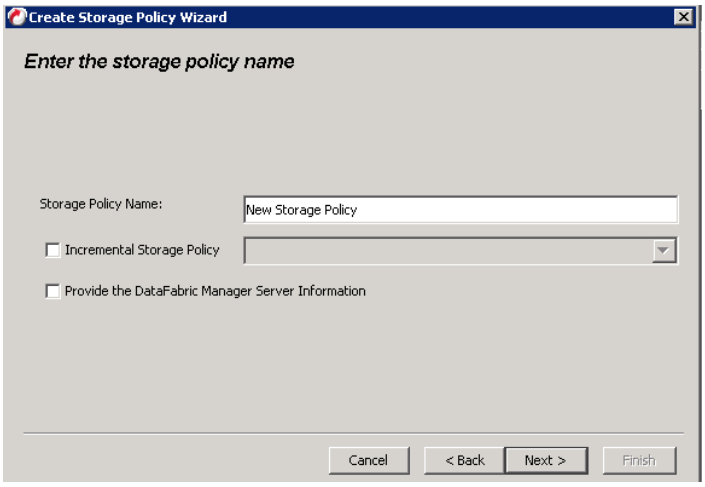
11. Select the Storage Device tab, and click **Create Storage Policy**.



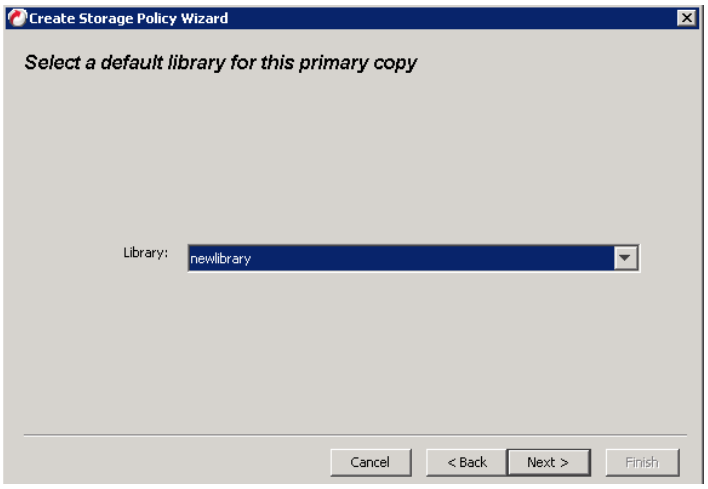
12. In the Create Storage Policy Wizard, select the Policy Type as **Data Protection and Archiving**.



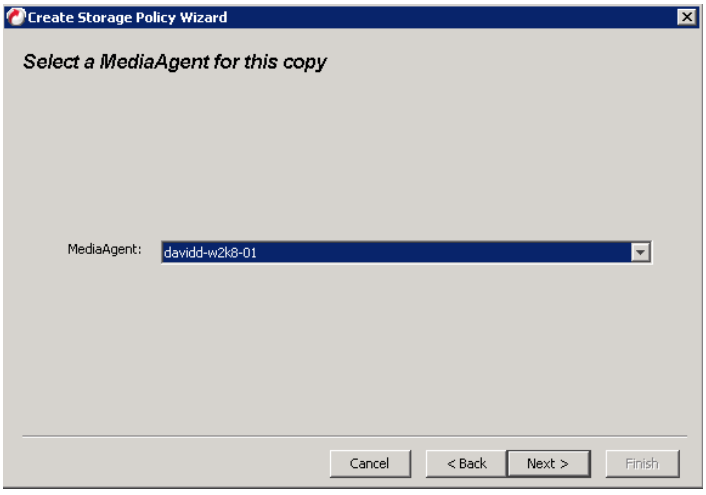
13. Enter the **Storage Policy Name**.



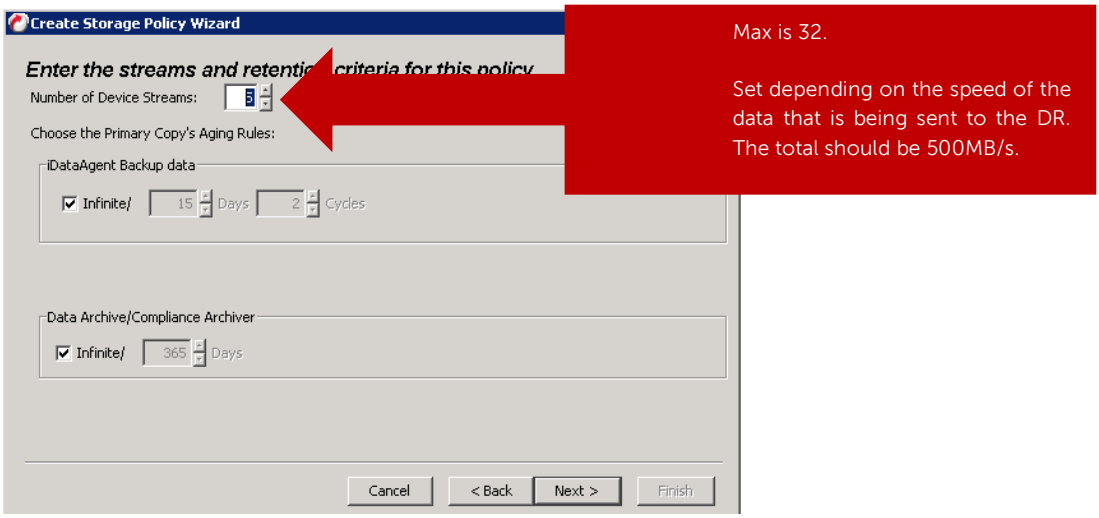
14. Select the DR disk library created in **Section 2** as the default library



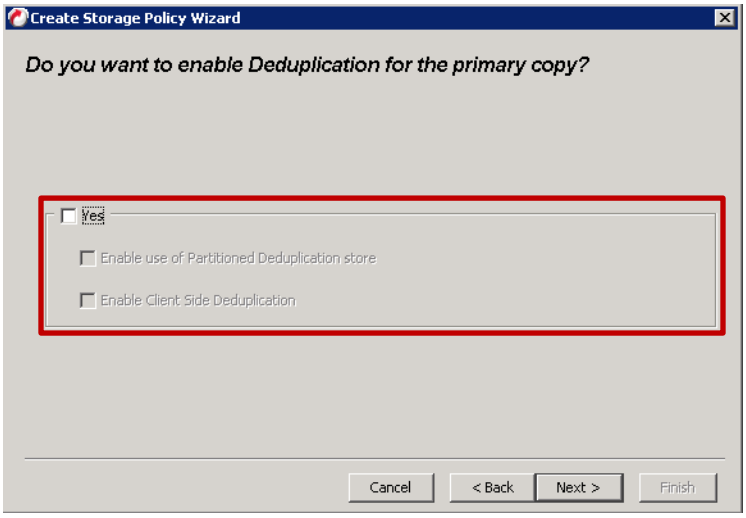
15. Select the MediaAgent.



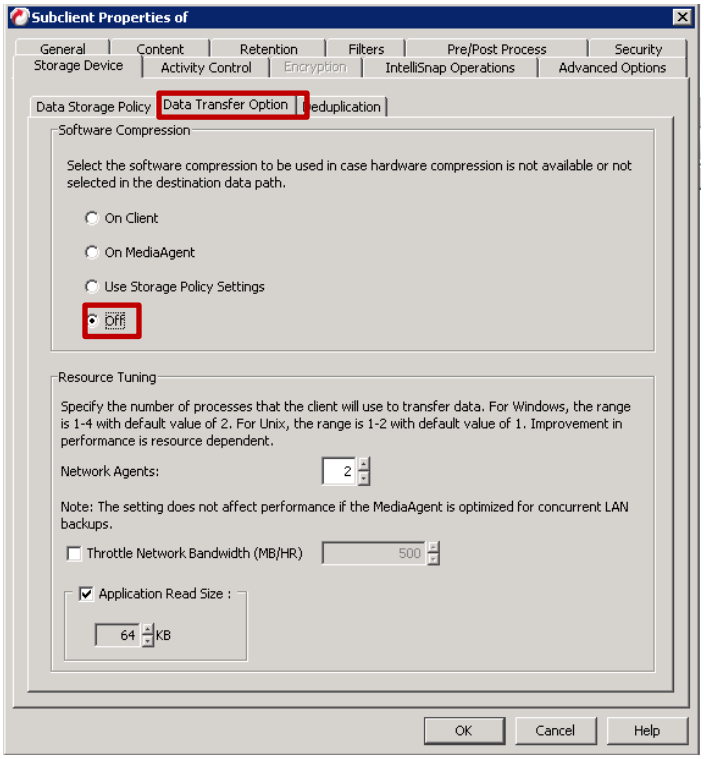
16. Enter the **Number of Device Streams** and retention policy.



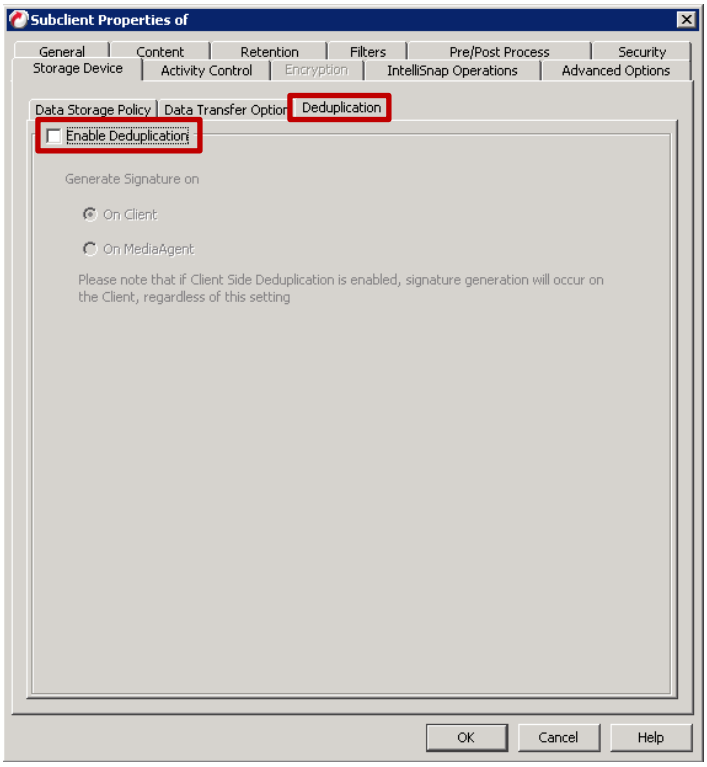
17. **Disable** deduplication for the primary copy.



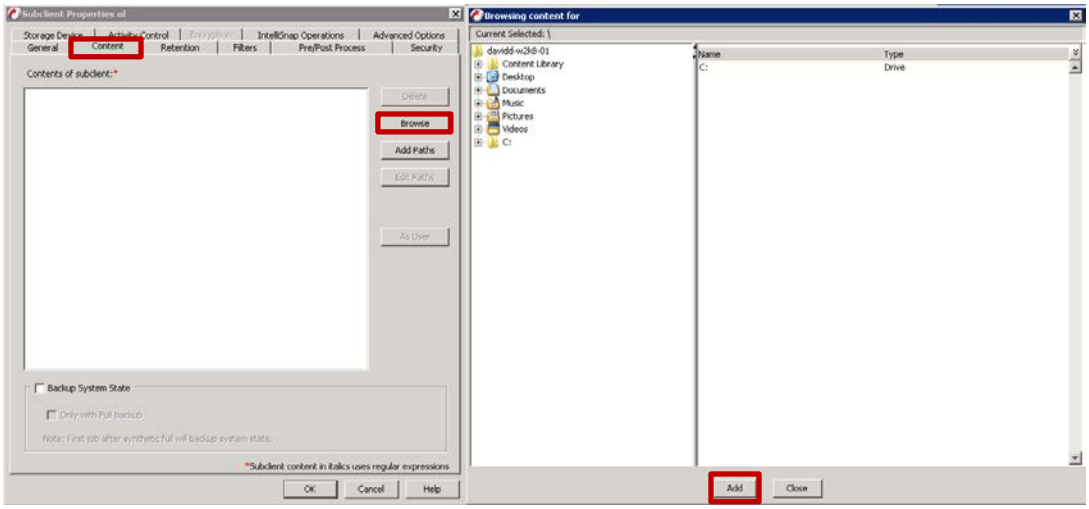
18. Click **Finish**.
19. Disable Software Compression under **Storage Device** > **Data Transfer Option**.



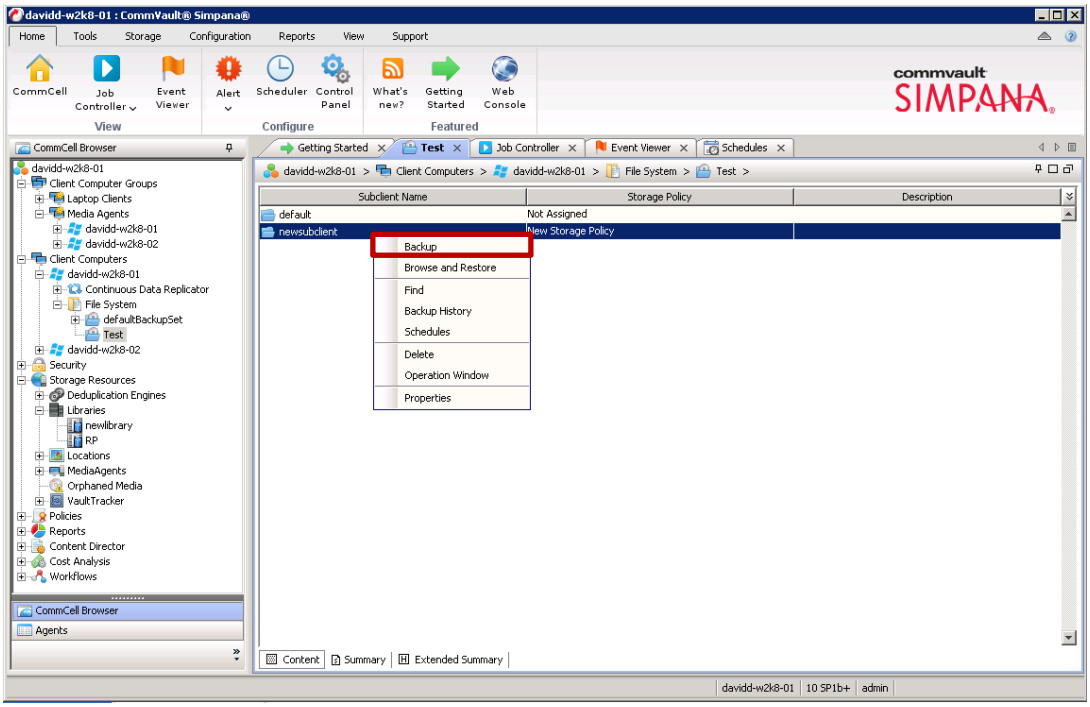
20. Clear the Enable Deduplication checkbox under **Storage Device** > **Deduplication**.



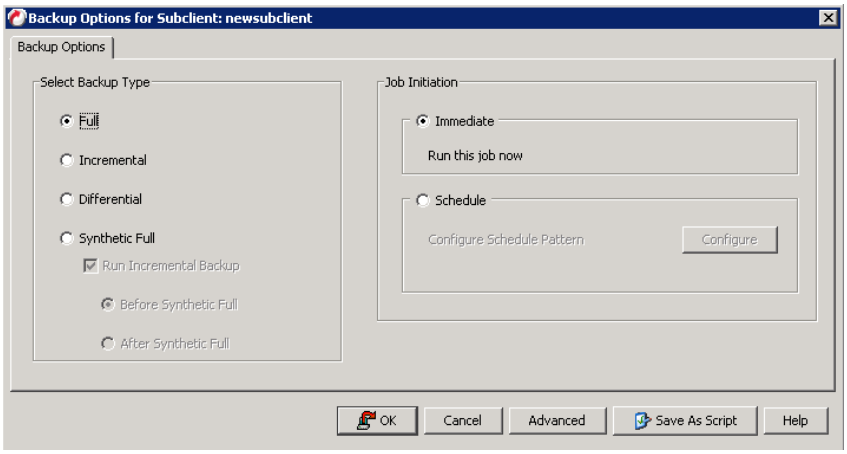
21. On the **Content** tab, select data for backup by clicking **Browse**.



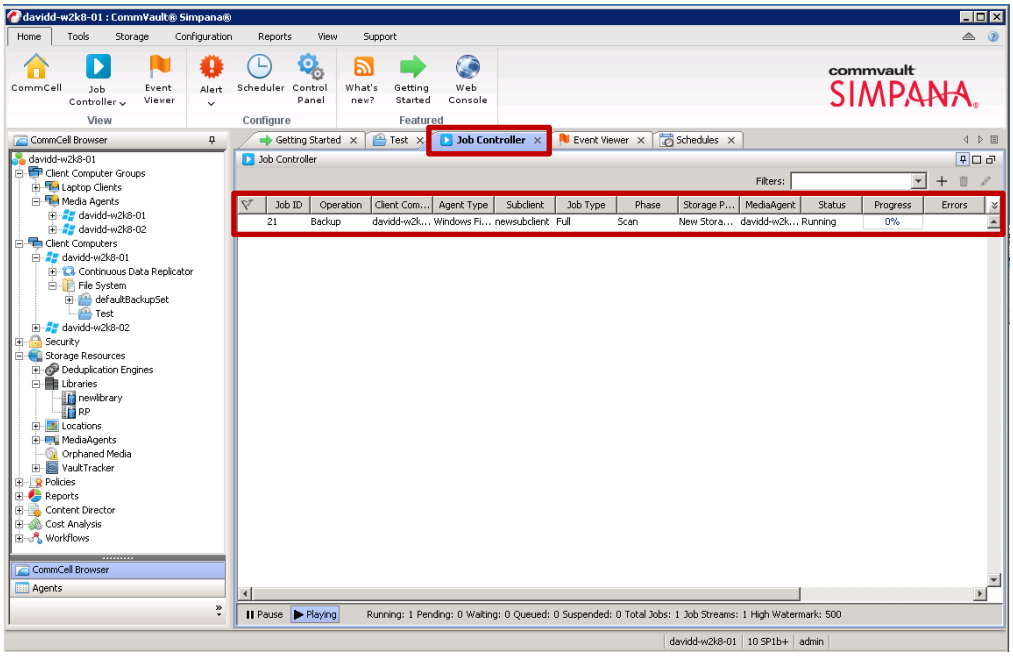
22. Right-click the newly created sub-client, and select **Backup**.



23. Make selection under **Select Backup Type** and click **OK**.



24. Navigate to **Job Controller** to monitor the job **Status**.



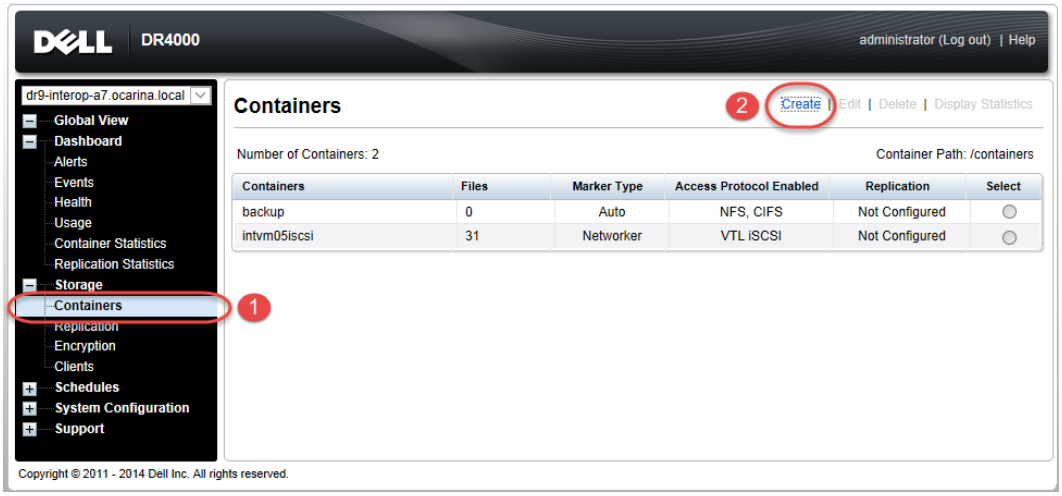
3 Configuring VTL for CommVault Simpana

3.1 Creating and configuring iSCSI target container(s) for CommVault Simpana

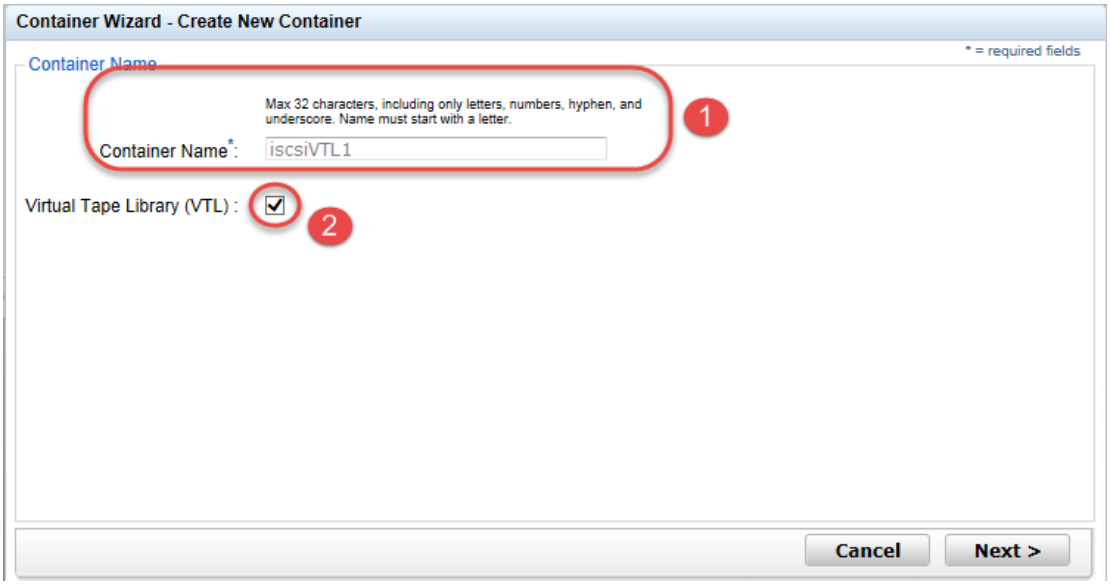
3.1.1 Creating the iSCSI VTL container for CommVault Simpana

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

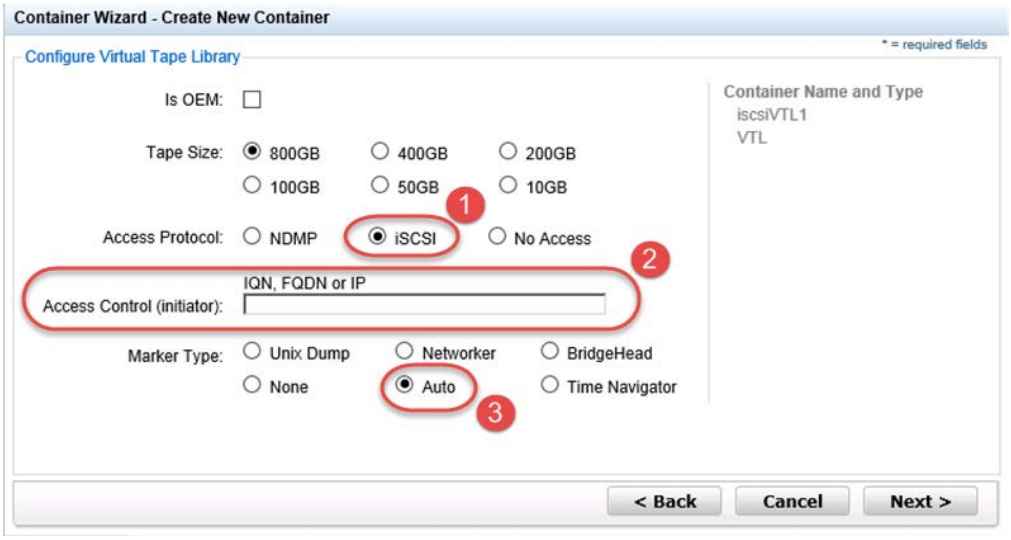
1. Select **Containers** in the left navigation area, and then click **Create** at the top of the page.



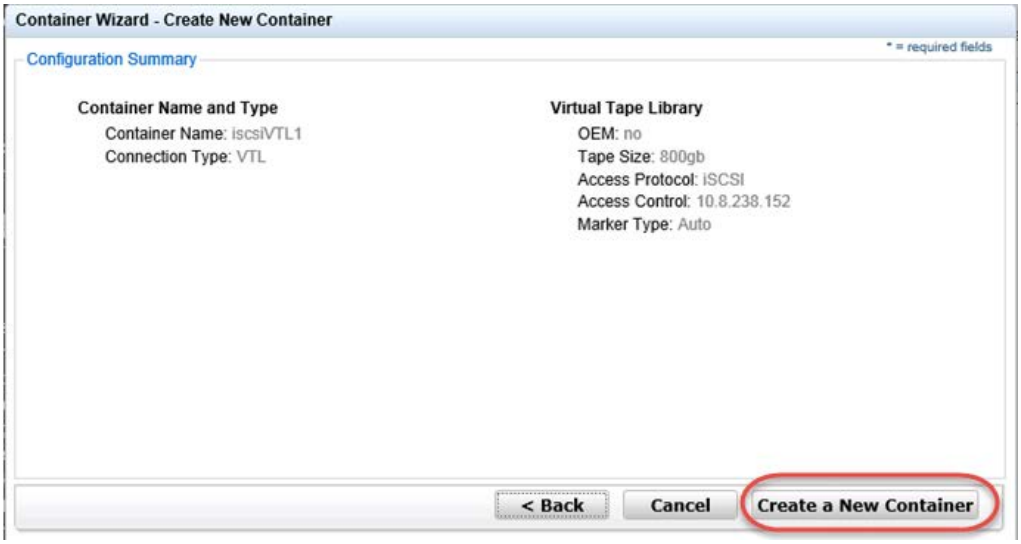
2. Enter a container name and select the **Virtual Tape Library (VTL)** container option.



3. Select the **iSCSI Access Protocol**. Specify the DMA **Access Control** by providing the storage node / media node IP Address, IQN or FQDN. Select the **Auto** Marker Type.

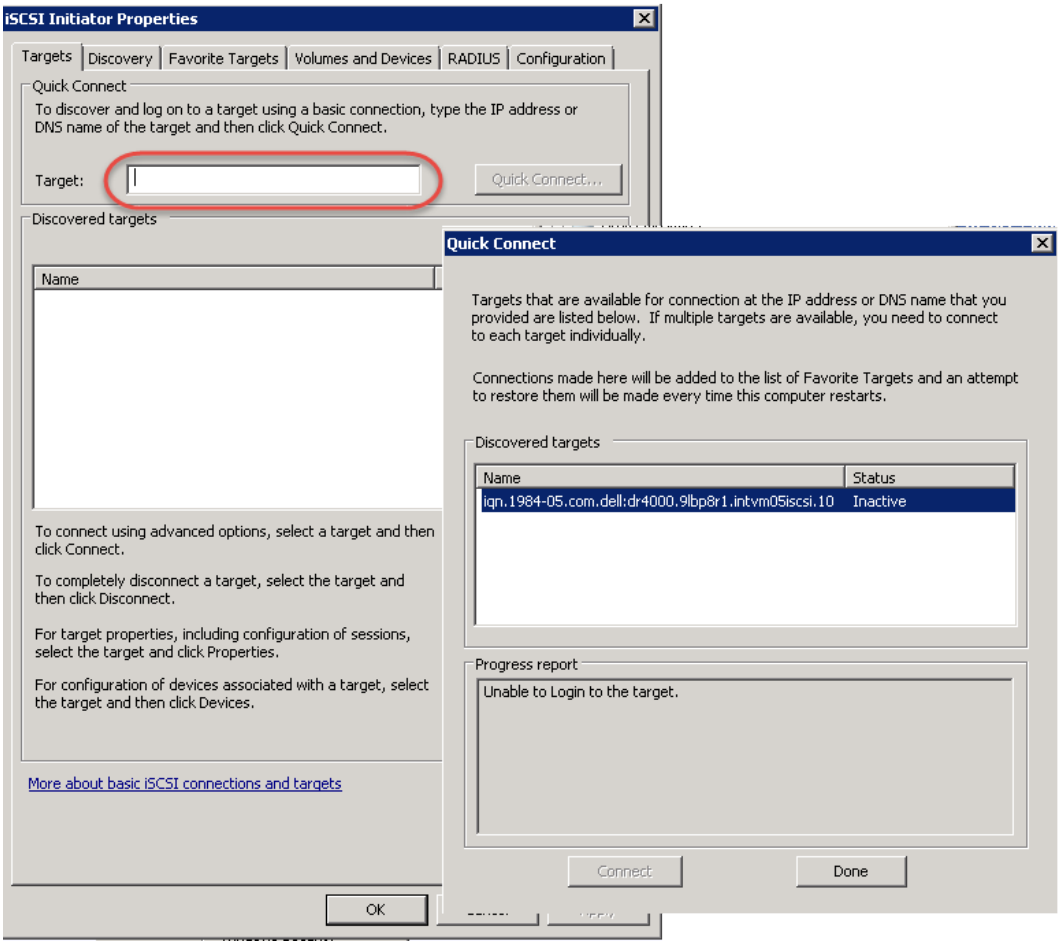


4. Finalize VTL creation by clicking **Creating a New Container**.

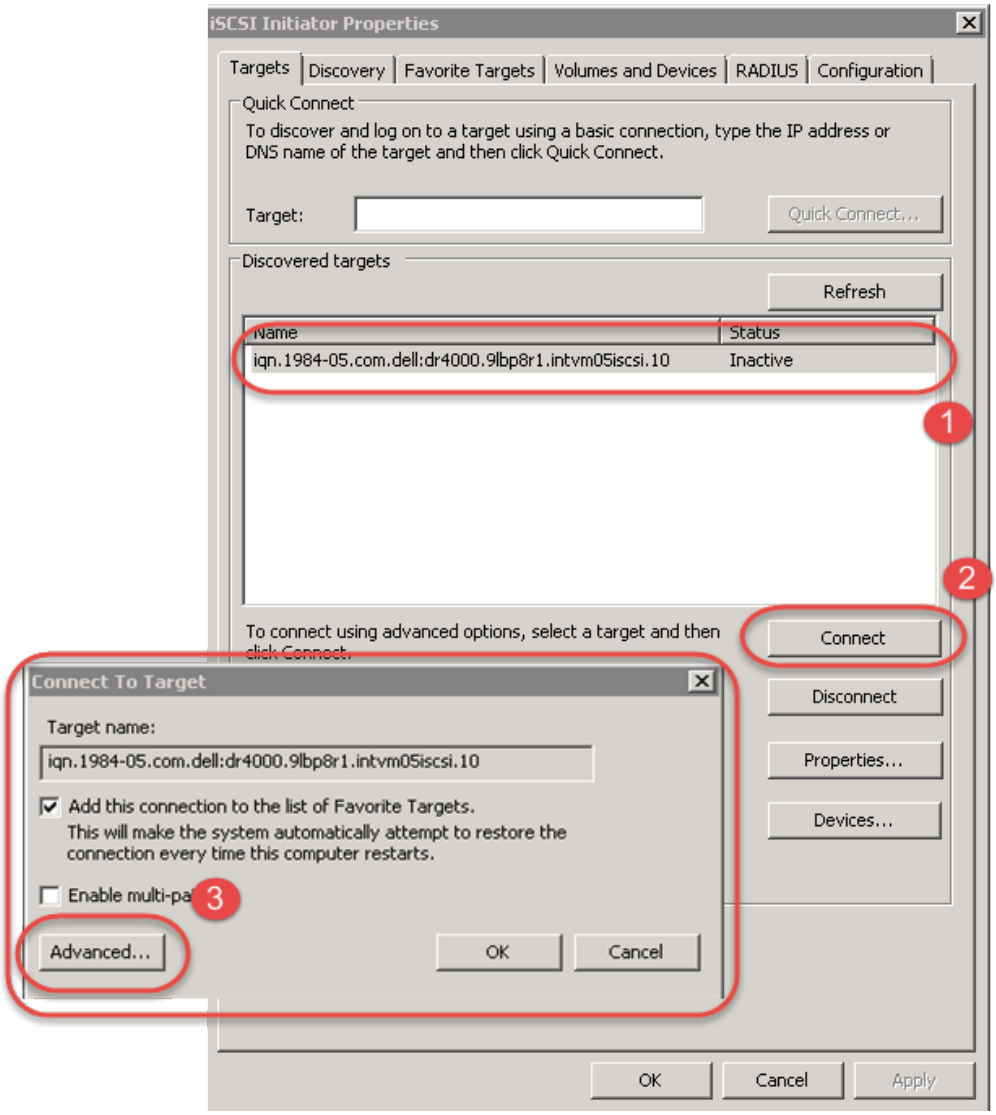


3.1.2 Configuring the iSCSI target - Windows

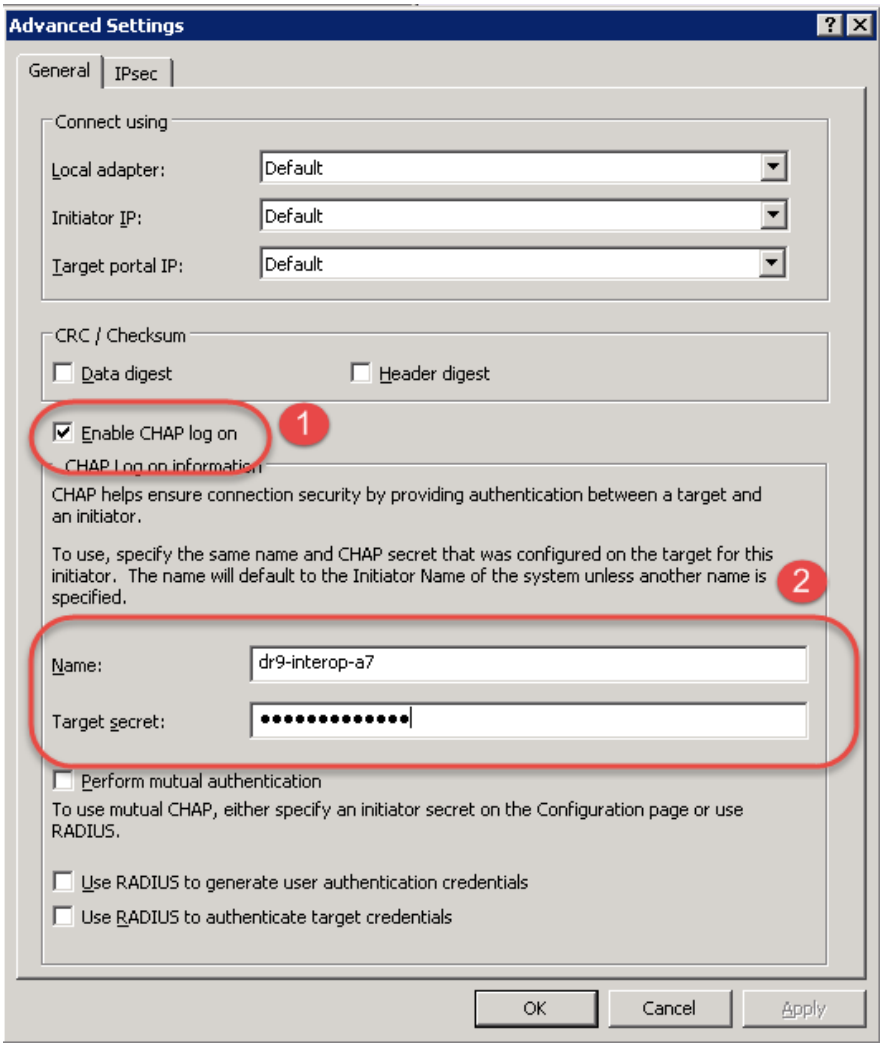
1. You configure the **iSCSI Initiator Software** for Windows by providing the IP or FQDN of the DR unit in the **Quick Connect** > **Target** field. Click **Quick Connection** to open the Quick Connect dialog box, which indicates a connection was made but was set as inactive.



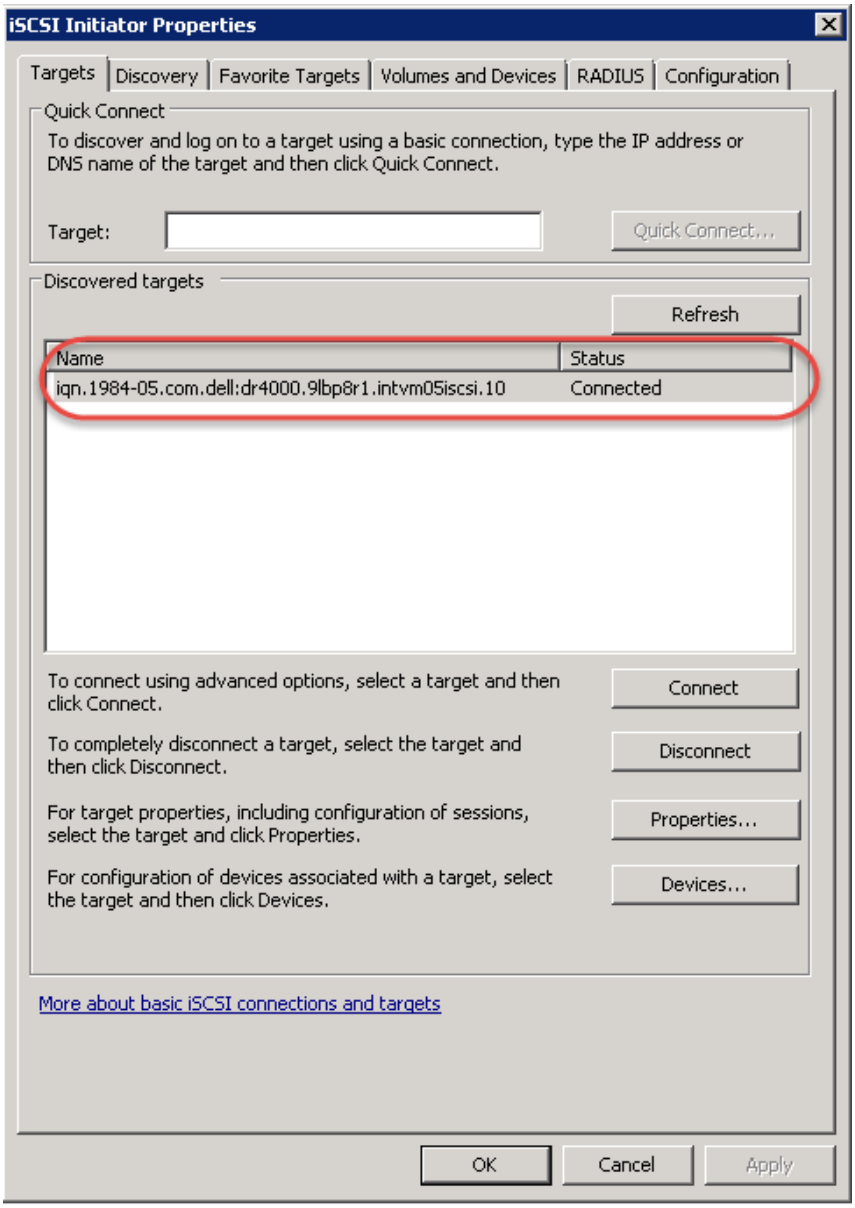
2. Close the dialog box and then select the newly discovered target. This target will have an **Inactive Status** as it requires authentication parameters to be provided for iSCSI login. Select the Target from the list, click the **Connect** button, and then in the **Connect to Target** dialog box, click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



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

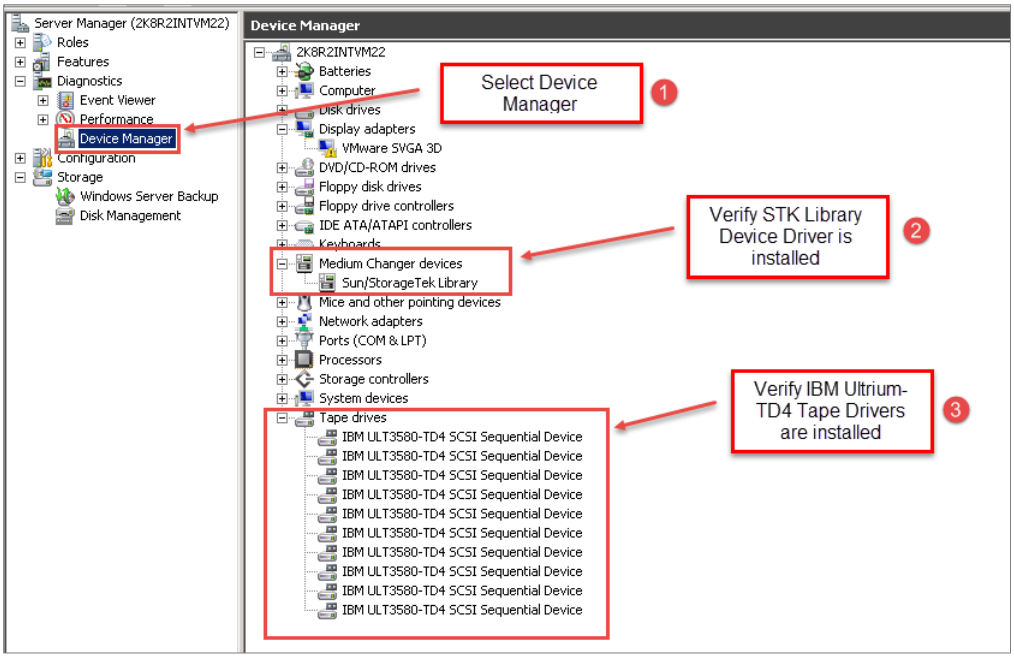


The iSCSI target should now show as connected, and device discovery can now proceed.



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 more information and assistance in acquiring Microsoft Device Drivers, e.g., StorageTeck Library Drivers.



3.1.3 Configuring the iSCSI target – Linux

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

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

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

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
   ```

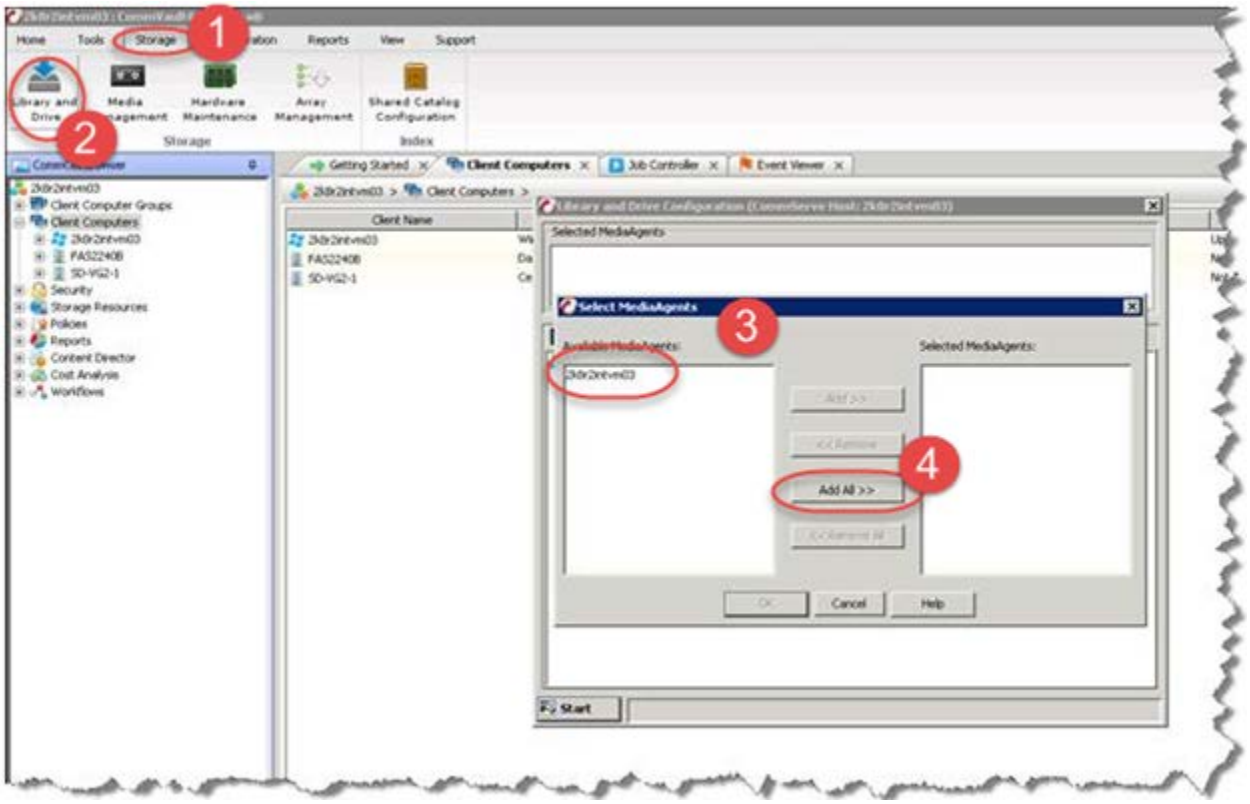
   For example:

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

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

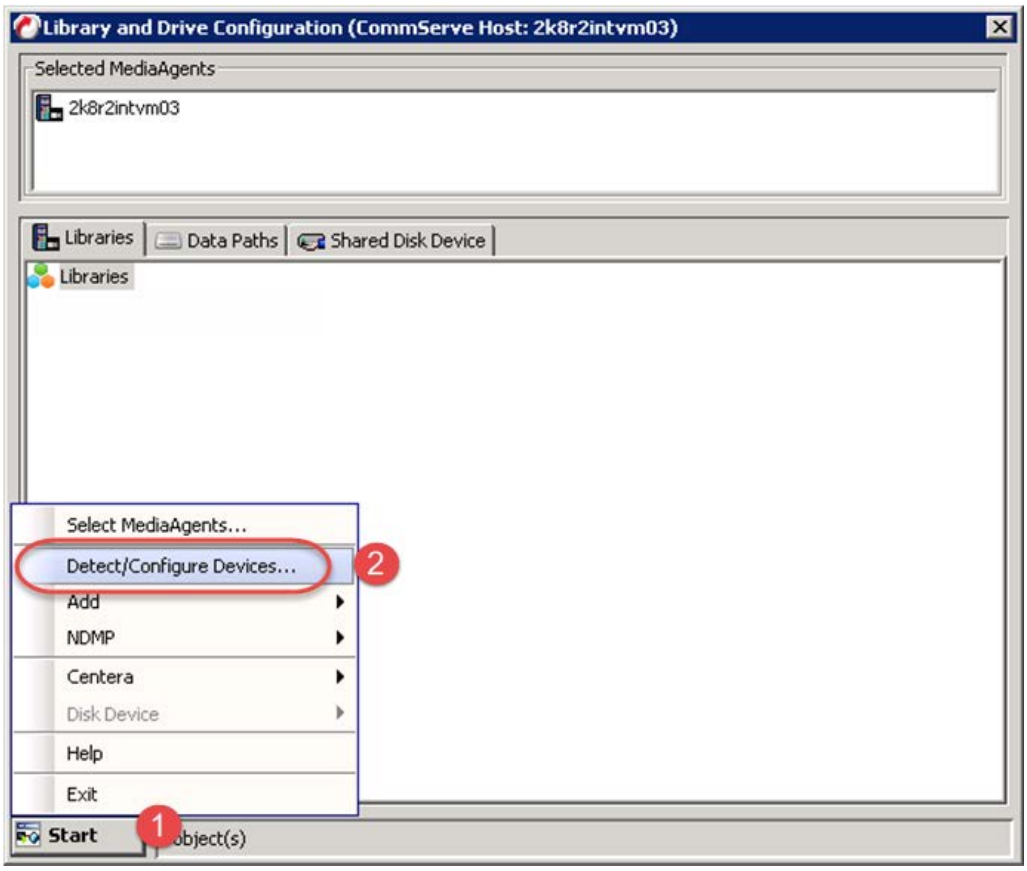
3.1.4 Configuring CommVault to use the newly created iSCSI VTL

1. Open the **CommCell** Console and, on the **Storage** tab, click **Library and Drive**. Move the desired **Available MediaAgent** to the **Selected MediaAgents** list box and click **OK**.

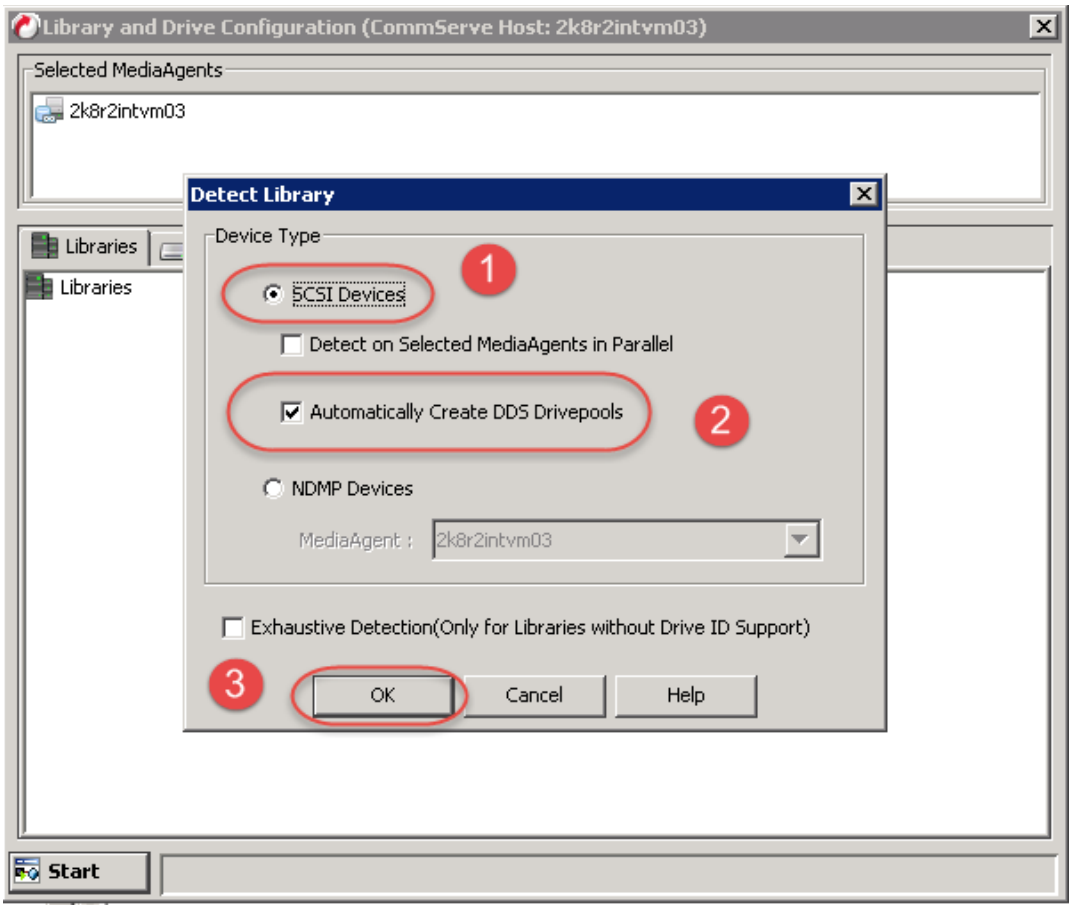


2. Click **OK** to continue.

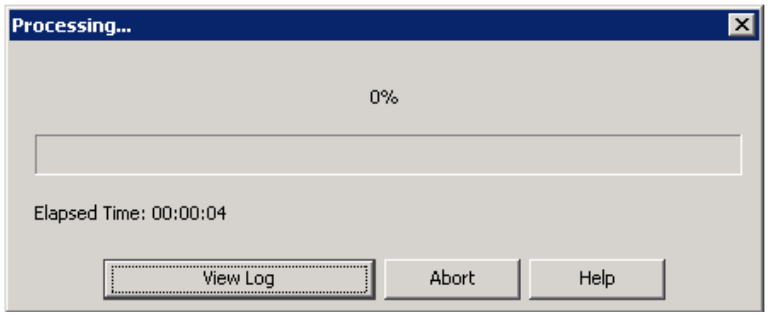
3. Select the **Detect/Configure Devices...** menu from the **Start** button.



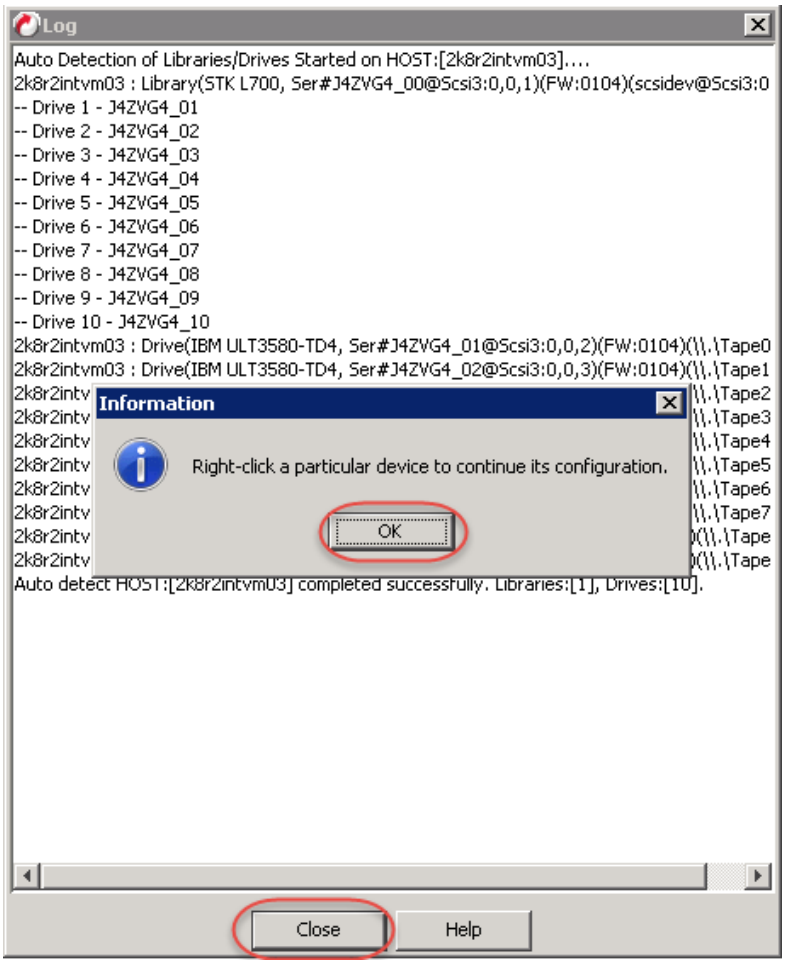
4. Make sure that **SCSI Devices** and **Automatically Create DDS Drivepools** are selected, and then click **OK**.



It may take a few moments to detect the iSCSI VTL.

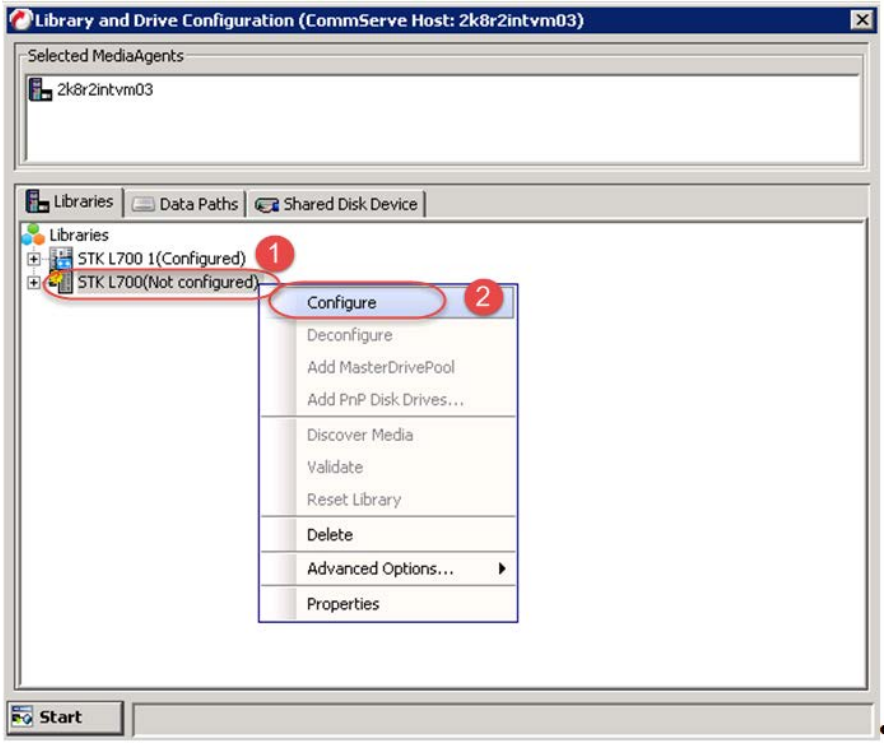


5. Click **OK** and then click **Close**.

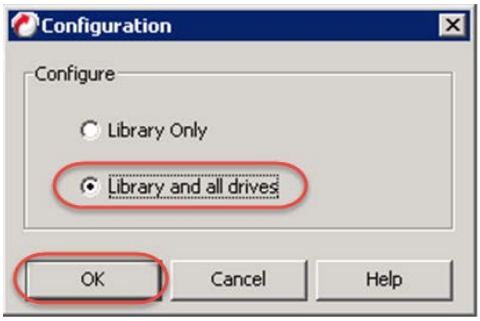


6. Click **OK**.

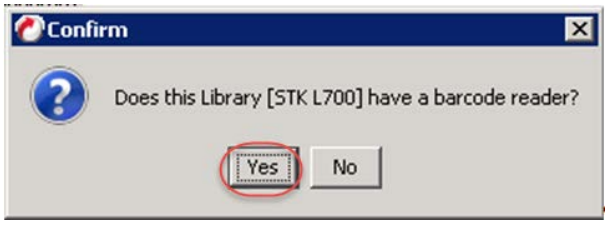
7. Right-click the library you just added, and select the **Configure** context menu.



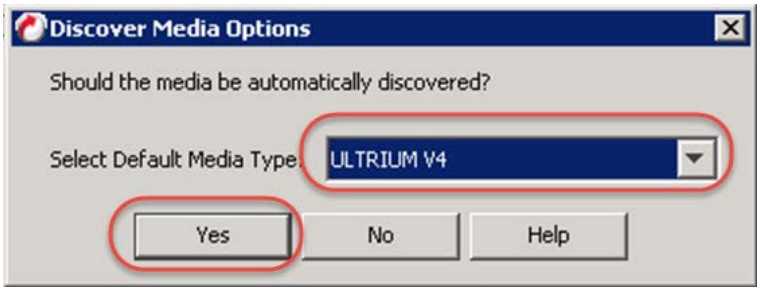
8. Select the **Library and All Drives** radio button and click **OK**.



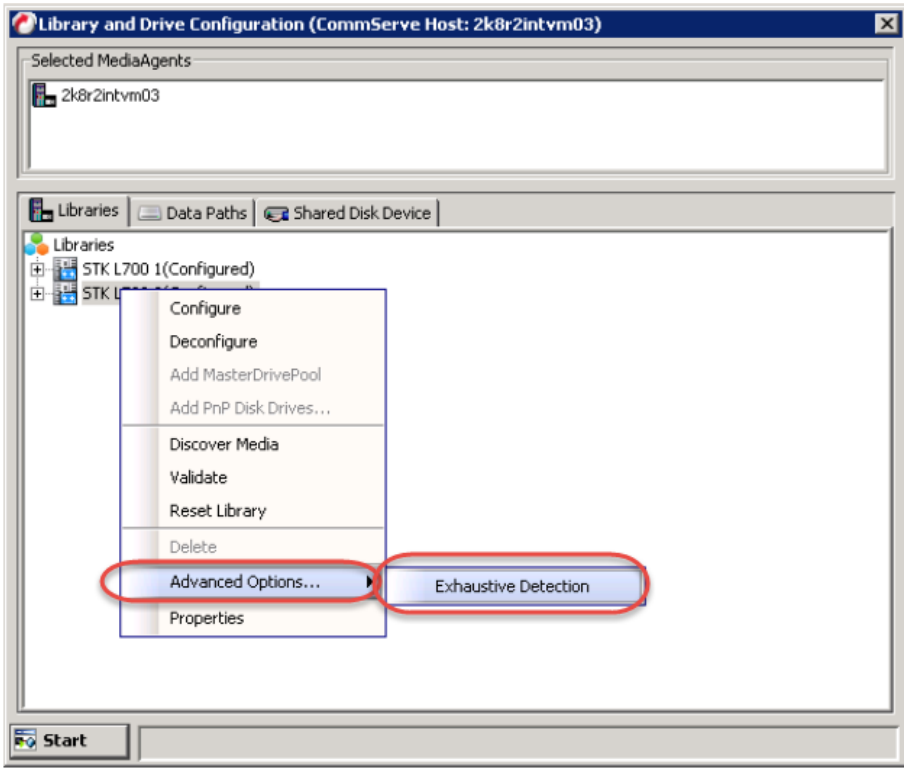
9. Click **Yes** to confirm.



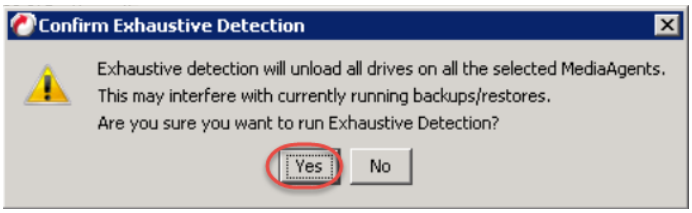
10. Select the appropriate media type, and then click **Yes**.



11. Select the new library and select **Advanced Options...**> **Exhaustive Detection** context menus.



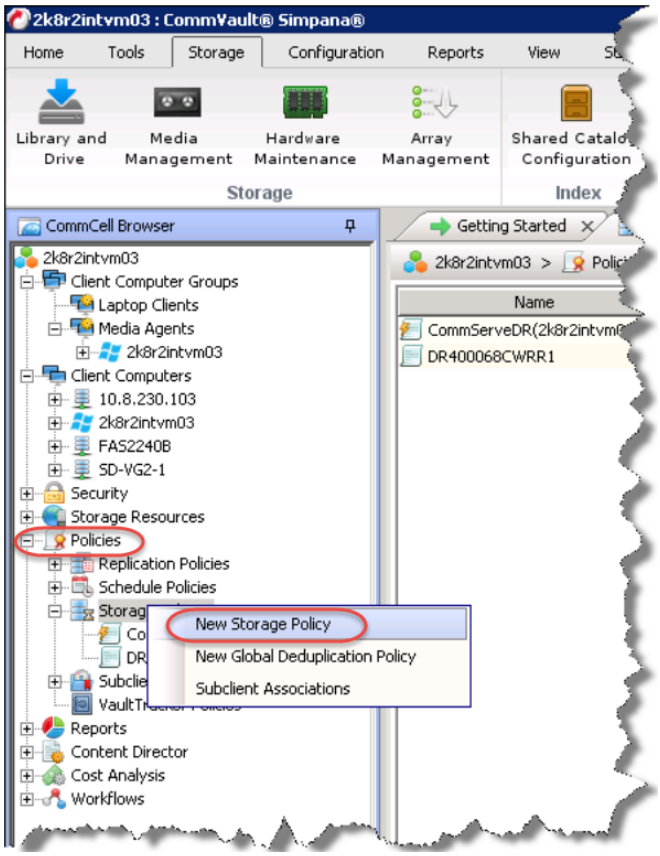
12. Click **Yes** to confirm.



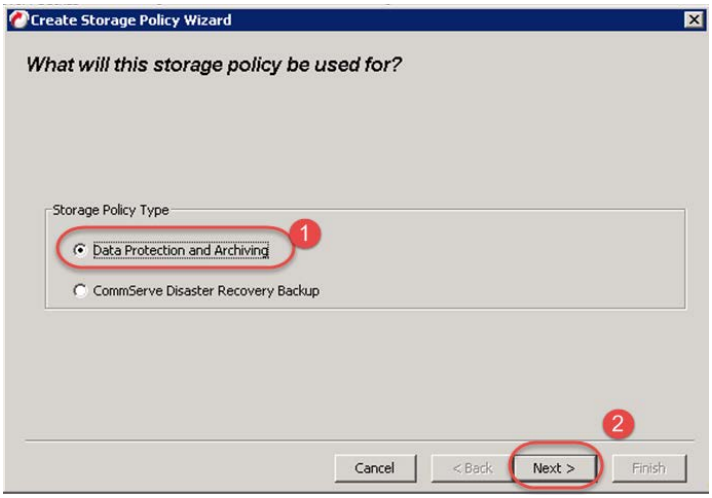
13. Click **Close**

14. Click **OK**.

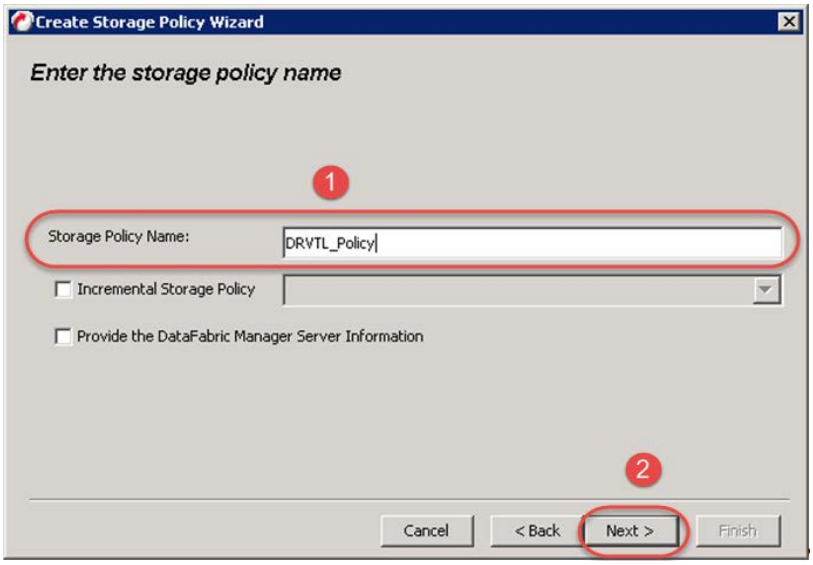
15. Close the Library and Drive Configuration dialog box.
16. Select **Policies** > **Storage Polices** in the navigation pane and then select the **New Storage Policy** context menu.



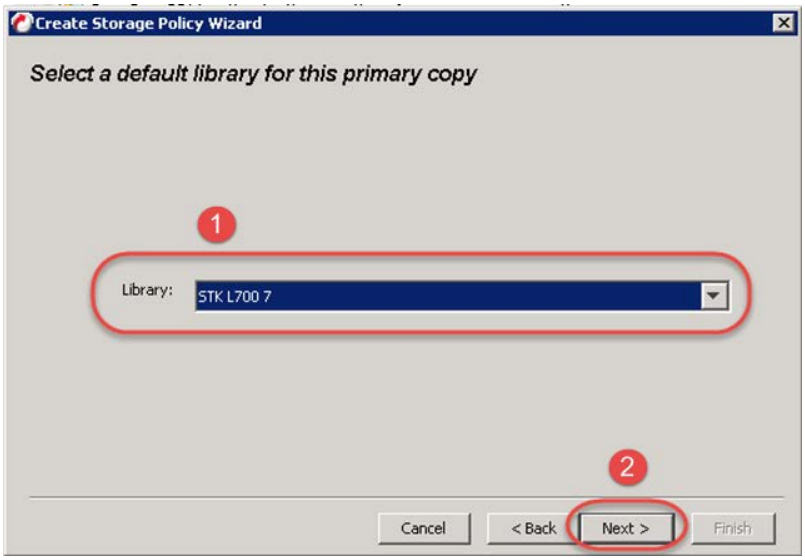
17. Select the **Data Protection and Archiving** radio button and click **Next**.



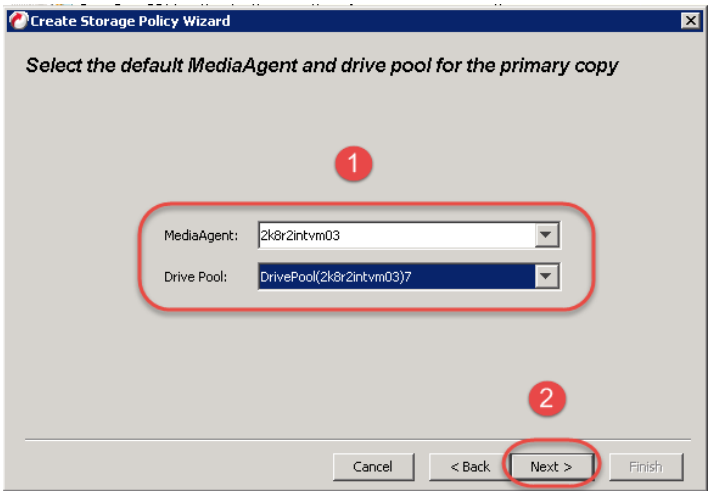
18. Enter a Storage Policy Name and click Next>.



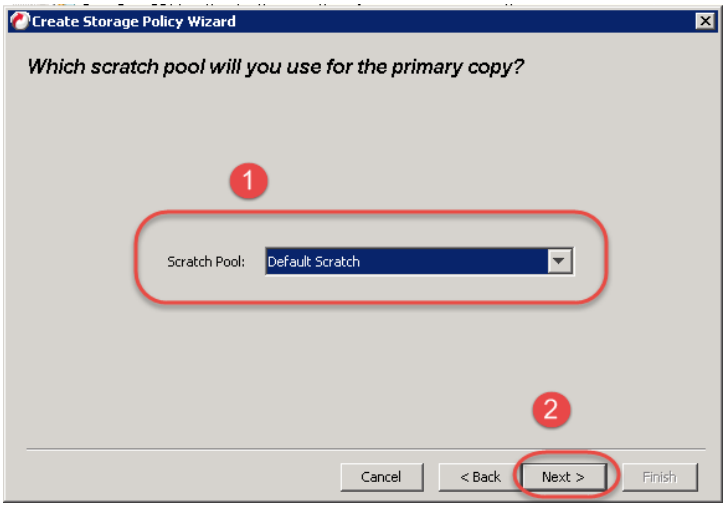
19. Select the newly added library and click **Next**.



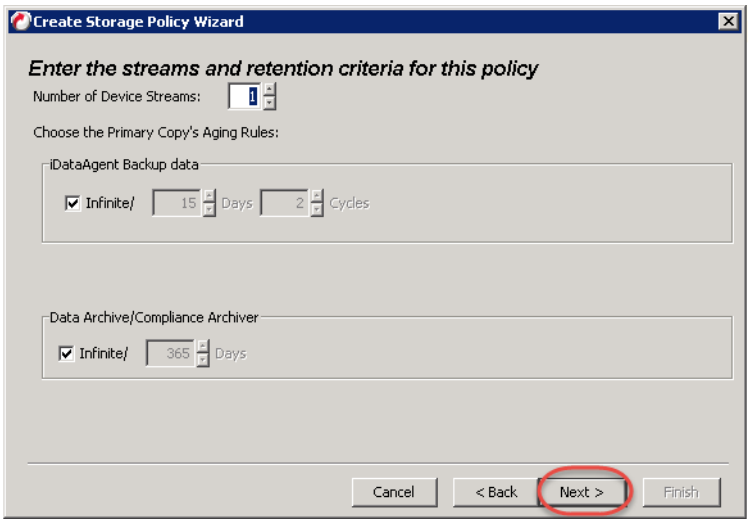
20. Select the **Drive Pool** for the newly added library and click **Next >**.



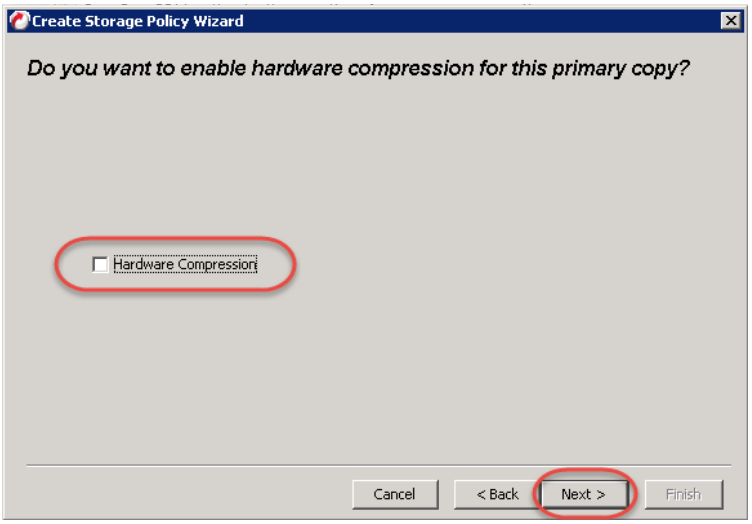
21. Select the **Scratch Pool** that you want to use for this library.



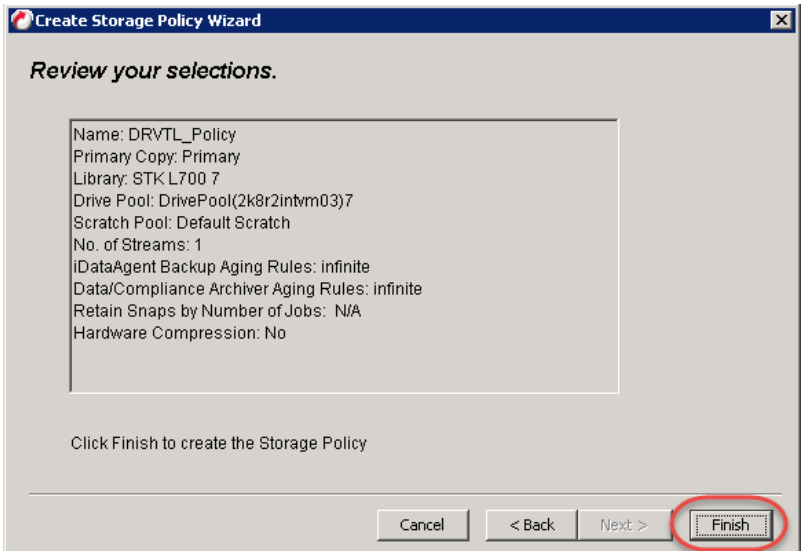
22. Click **Next**.



23. Deselect Hardware Compression and click **Next**.



24. Click **Finish**.

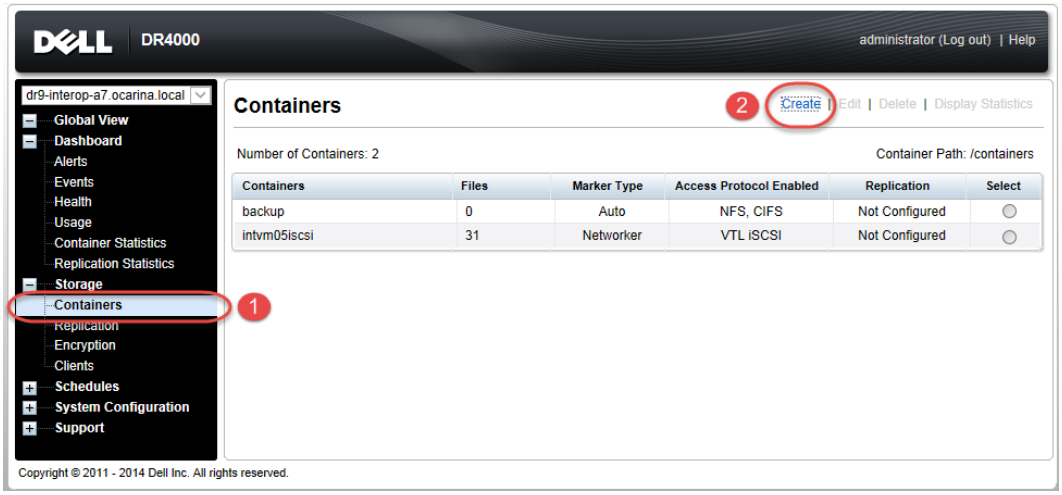


3.2 Creating and configuring NDMP target container(s) for CommVault Simpana

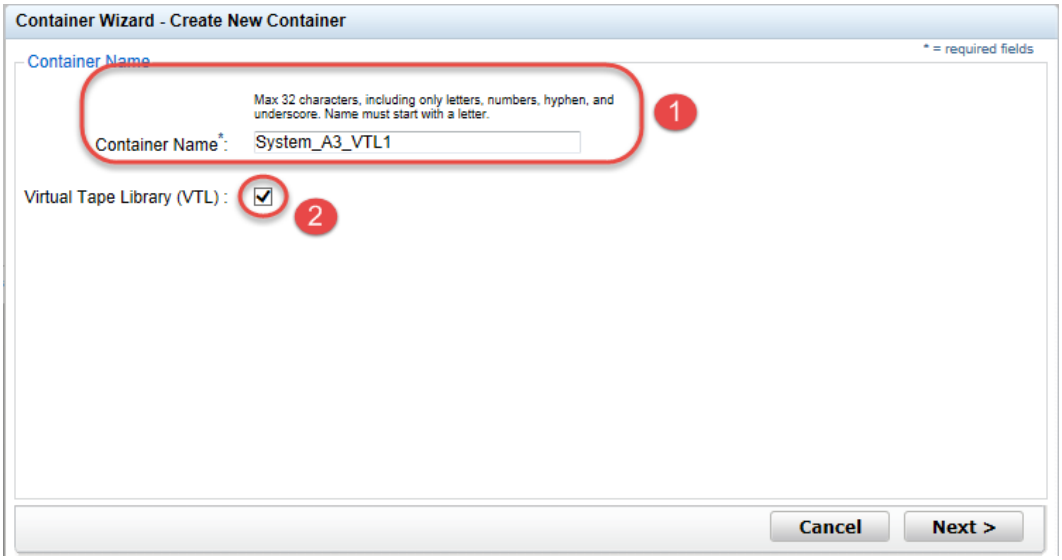
3.2.1 Create the NDMP VTL container for CommVault Simpana

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

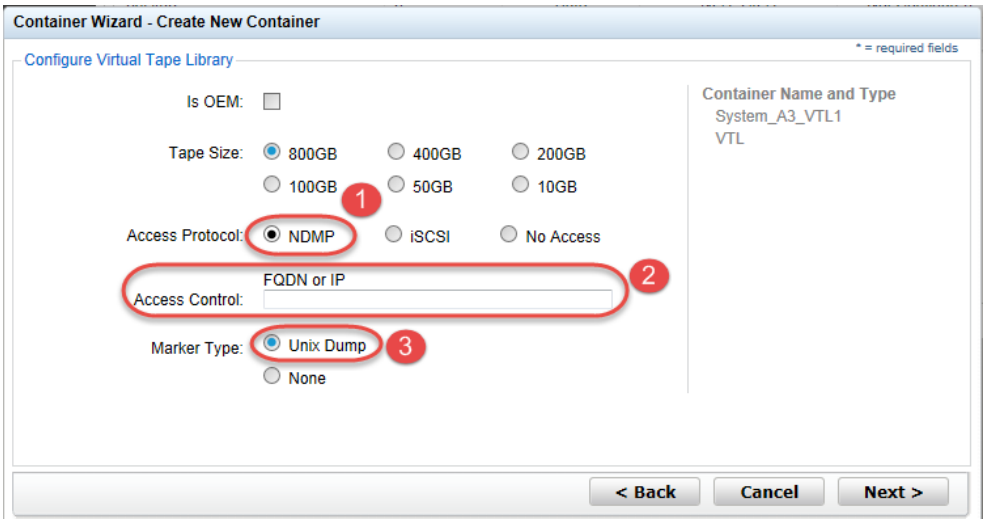
1. Select **Containers** in the navigation panel on the left side of the dashboard, and then click the **Create** at the top of the page.



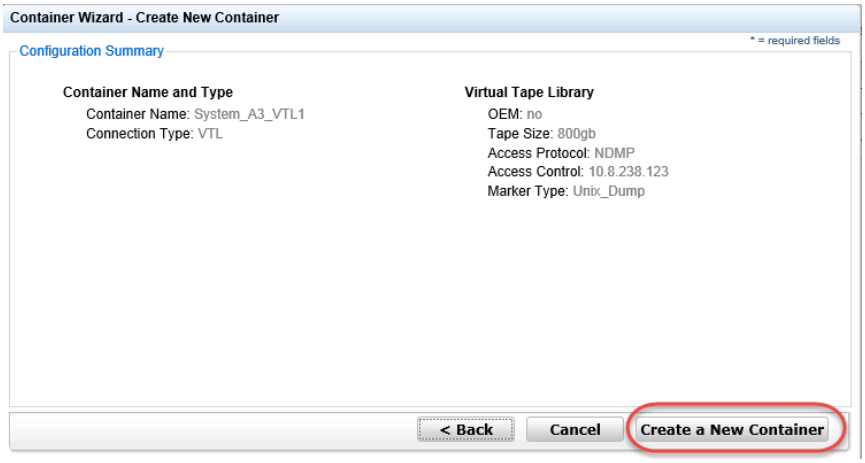
2. Specify your container name and select the **VTL** container option.



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** and click **Next.**



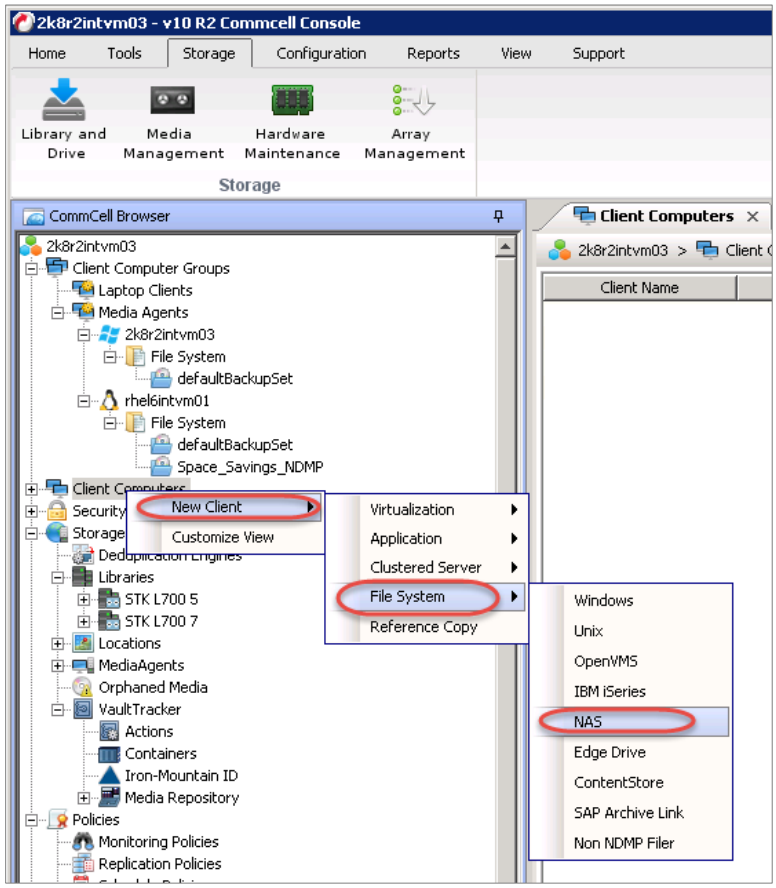
4. Finalize the VTL creation by clicking **Create a New Container**.



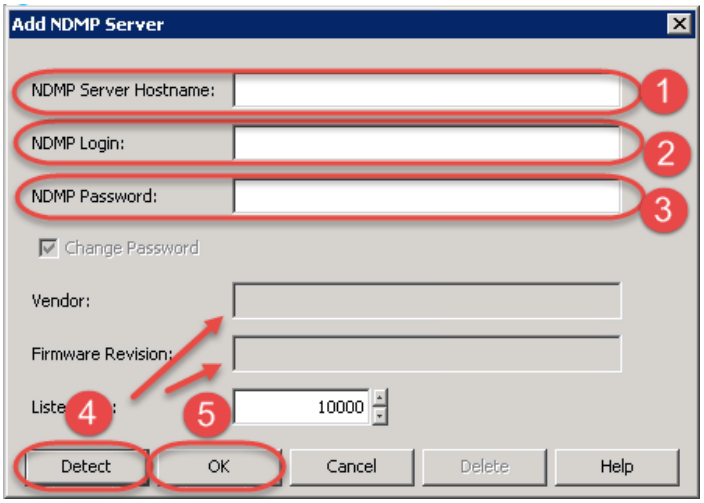
Note: All of the tapes will display as having a capacity of 799 GB in CommVault. This will not affect the use of smaller tapes. Smaller tapes will still be managed properly.

3.2.2 Configure CommVault to use the newly created NDMP VTL

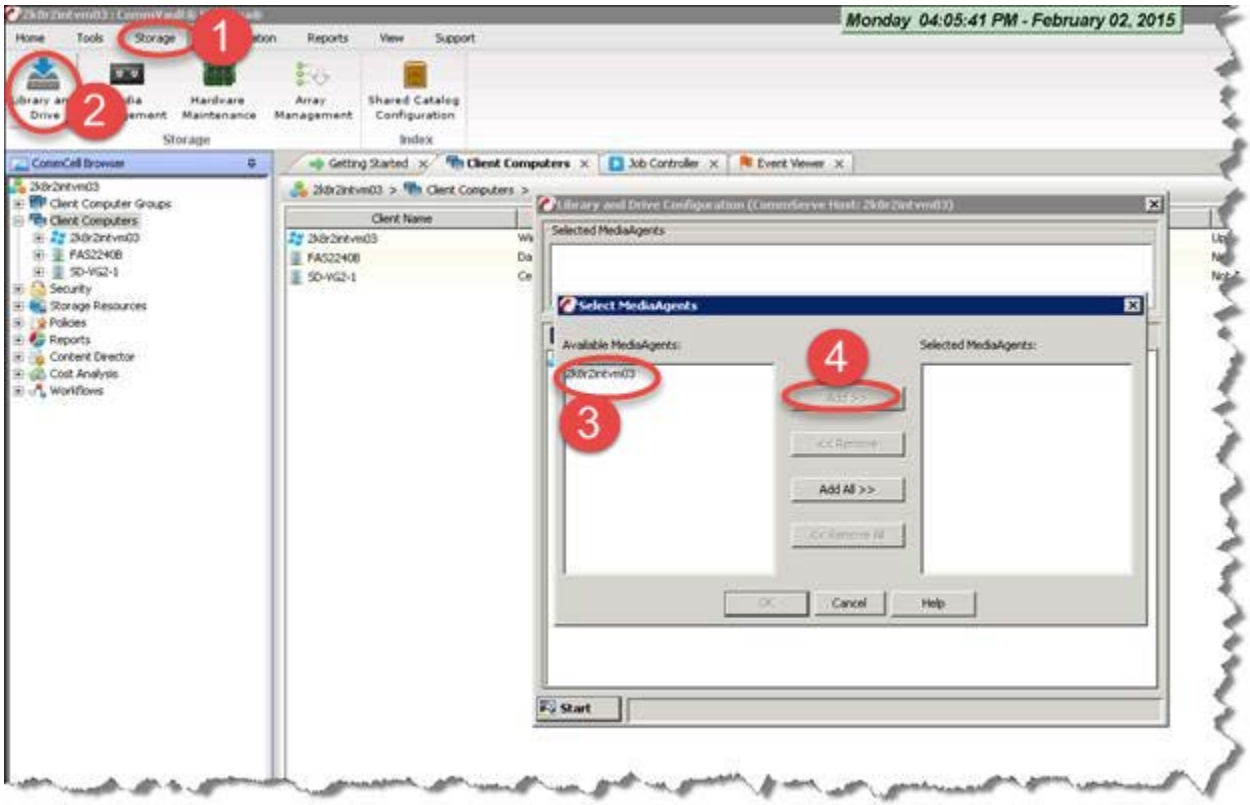
1. Open the **Commcell Console** and **select Client Computers** in the navigation pane. Select the **New Client** > **File System** > **NAS** context menu to add the DR Series system credentials.



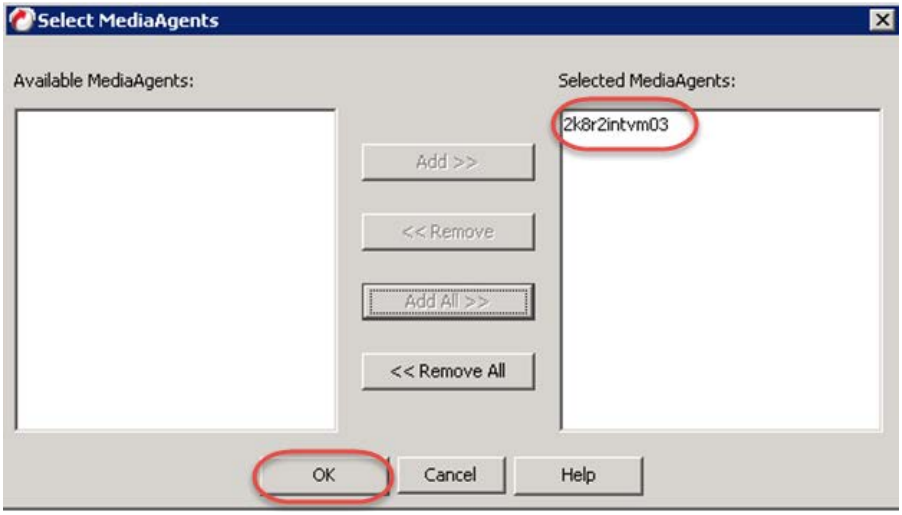
2. Enter information for the Add NDMP Server dialog box, including the newly added VTL DR hostname or IP address, Login and Password. Click **Detect** and wait for the **Vendor** and **Firmware Revision** boxes to populate. Click **OK**.



3. In the CommCell Console, on the Storage tab, click **Library and Drive**. Select the MediaAgent and click **Add**.

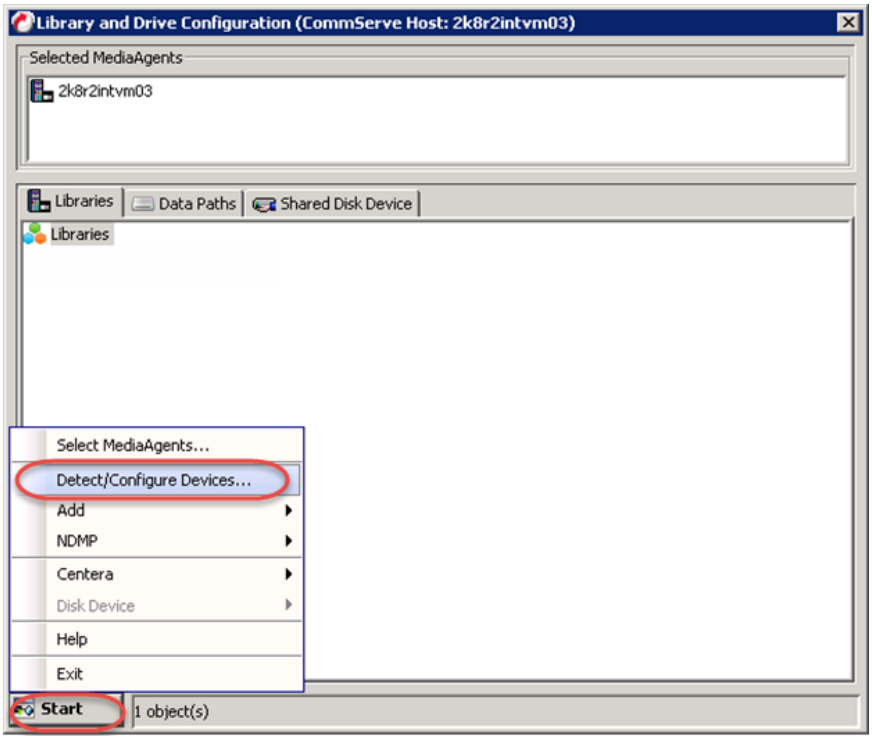


4. This will move the desired **MediaAgent** to the Selected **MediaAgents** list box. Click **OK**.

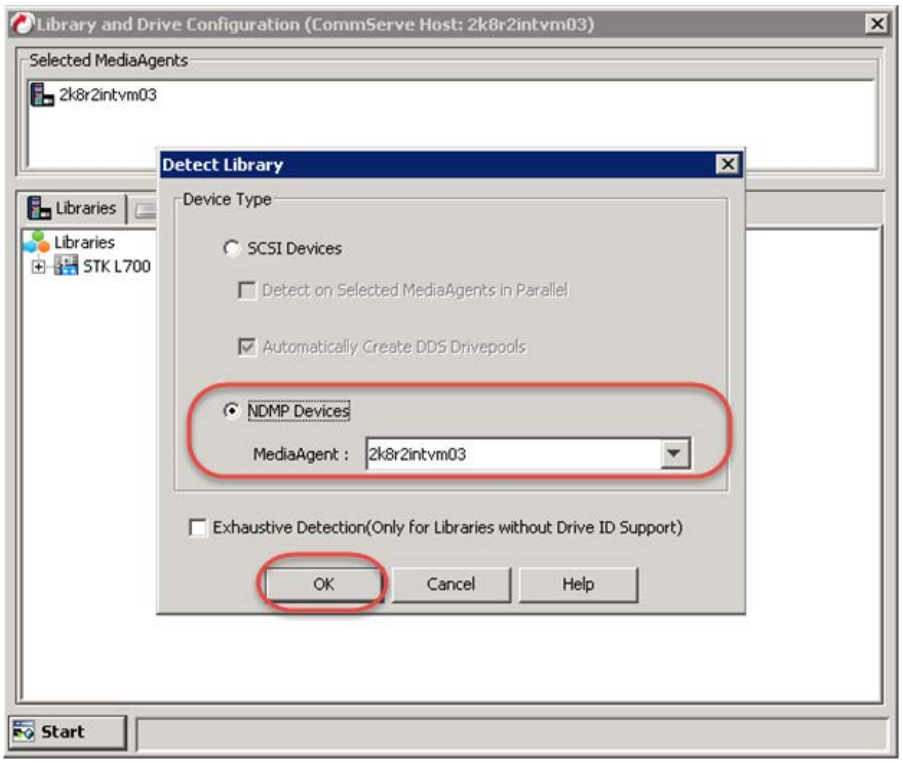


5. Click **OK** to continue.

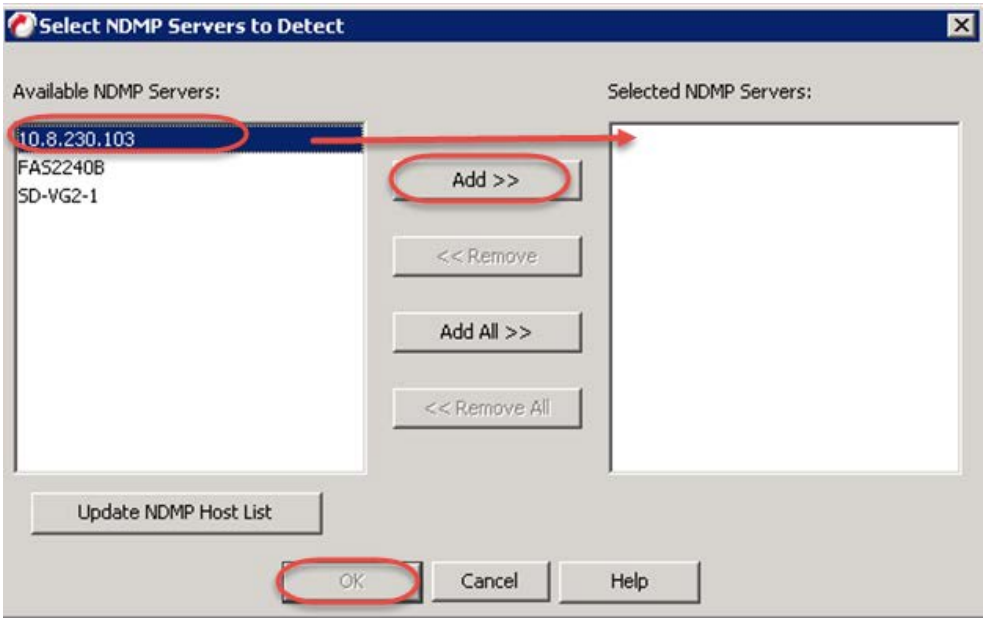
6. Click **Detect/Configure Devices...** menu from the **Start** button.



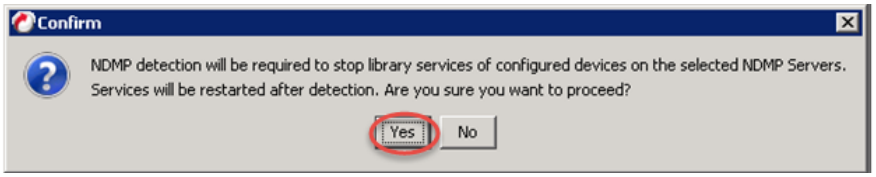
7. Select the **NDMP Devices** radio button and the **MediaAgent** of your choice. Click **OK**.



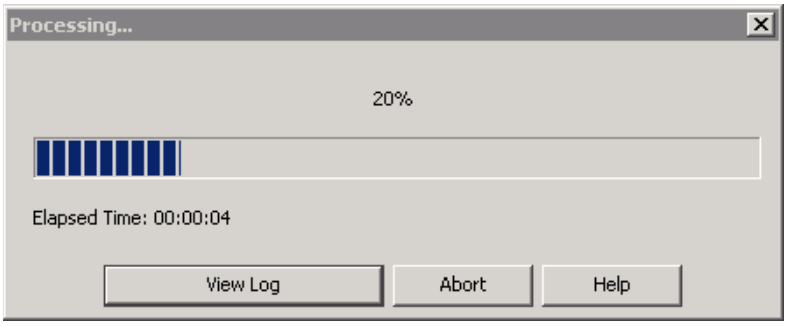
8. Select the **DR** for the **NDMP Server** and click **Add**. Click **OK**.



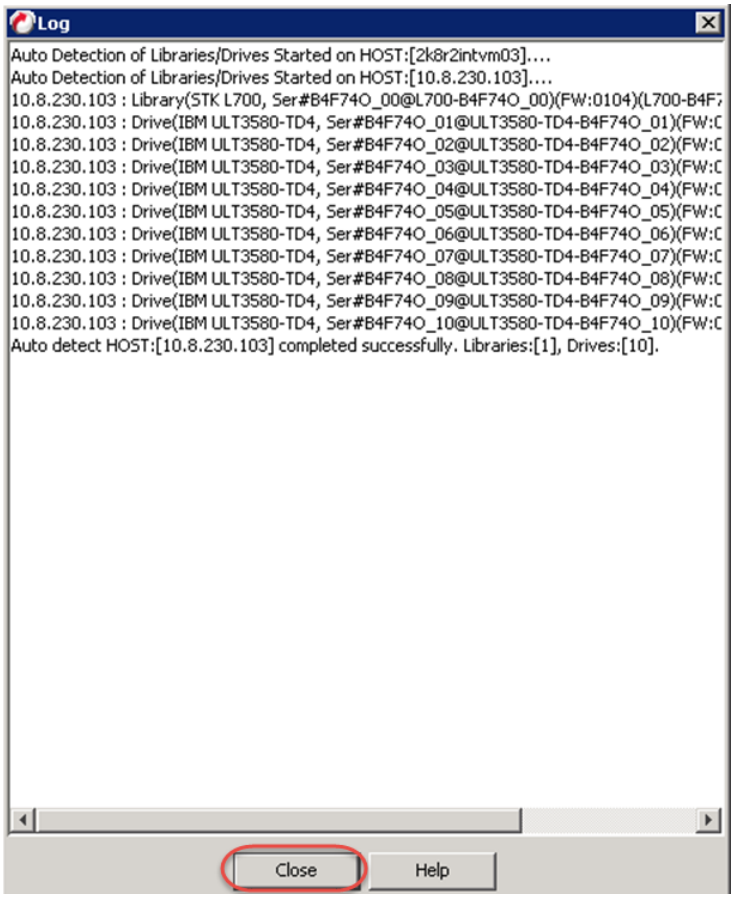
9. Click **Yes** to confirm.



A dialog box opens showing progress.

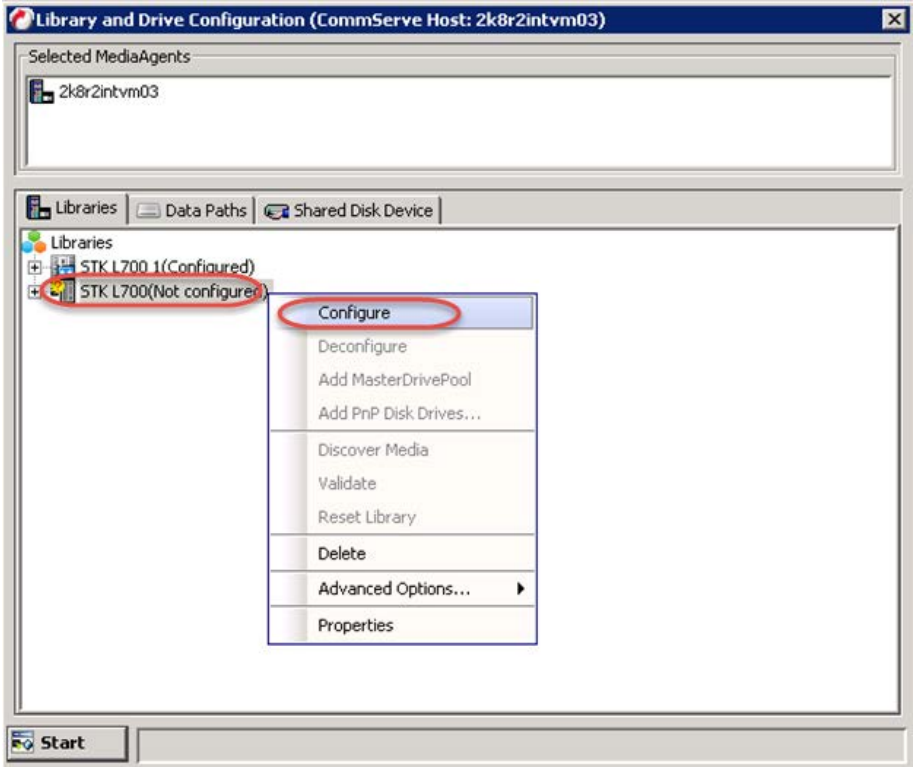


10. Close the **Log** dialog box.

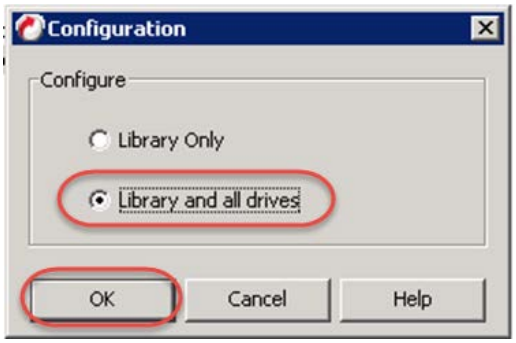


11. Click **OK**.

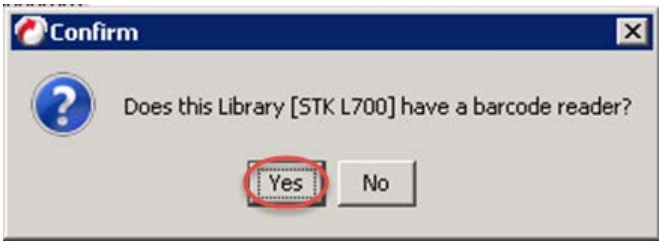
12. Right-click the library you just added and select the **Configure** context menu.



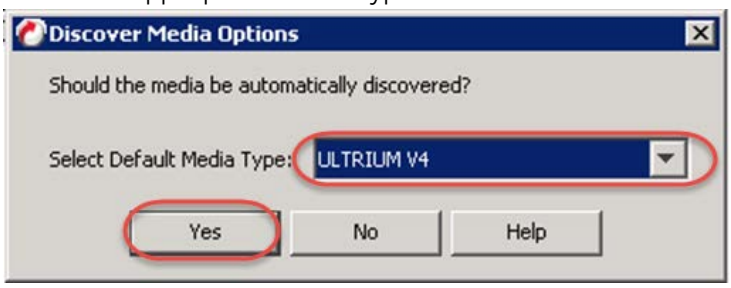
13. Select the **Library and All Drives** radio button and click **OK**.



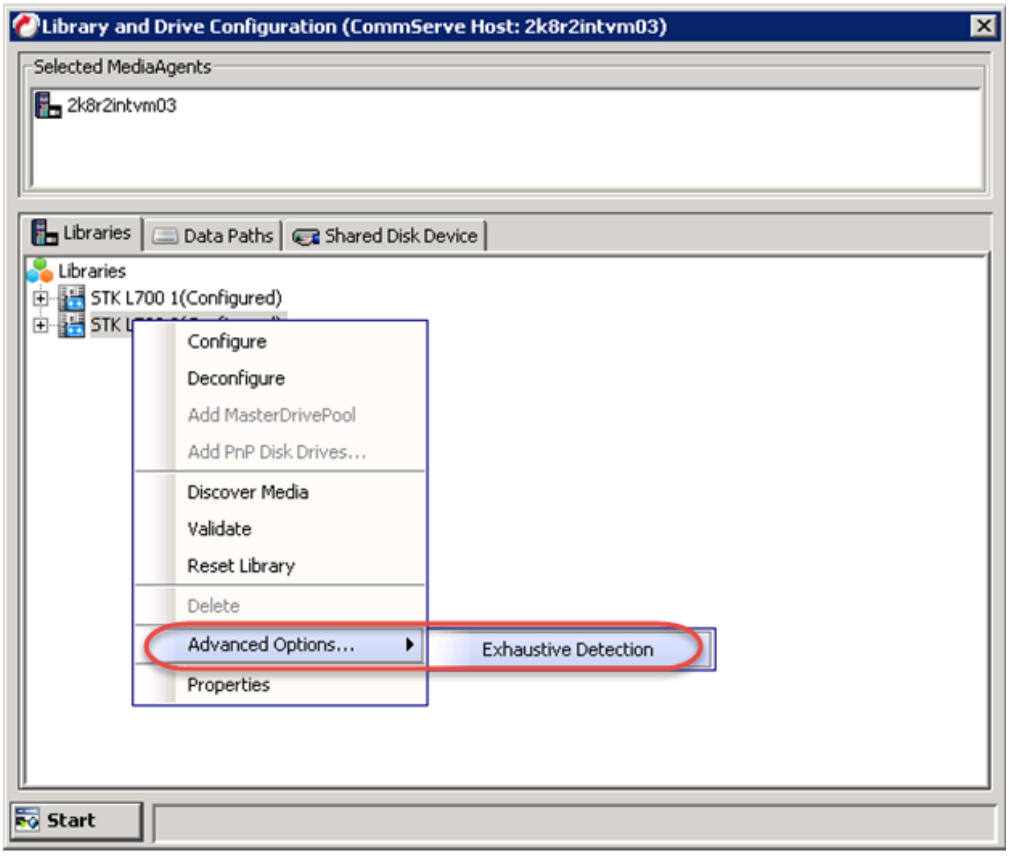
14. Click **Yes** to confirm.



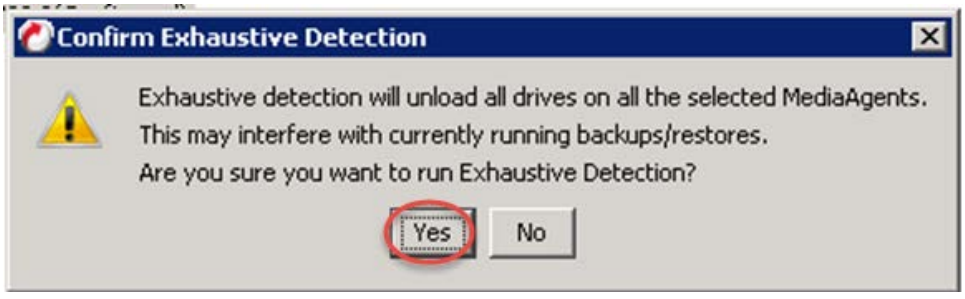
15. Select the appropriate media type and click **Yes**.



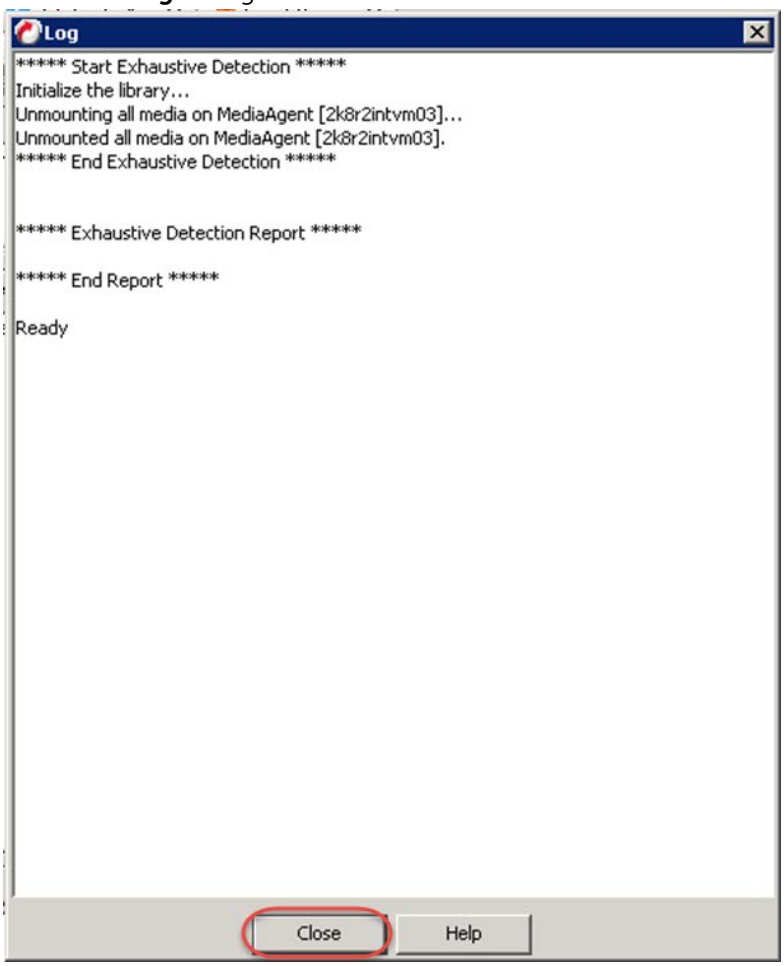
16. Select the tape library you just added and select the **Advanced Options** > **Exhaustive Detection** context menu.



17. Click **Yes** to confirm.

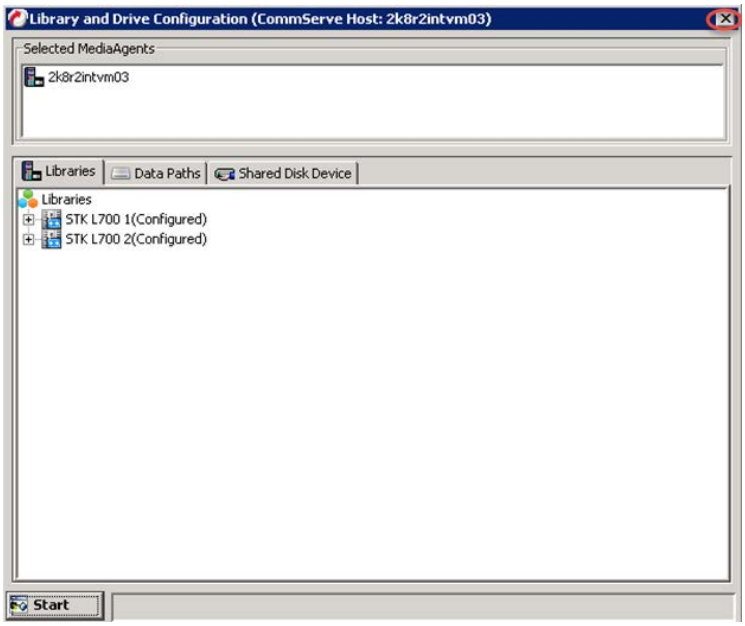


18. Close the **Log** dialog box.

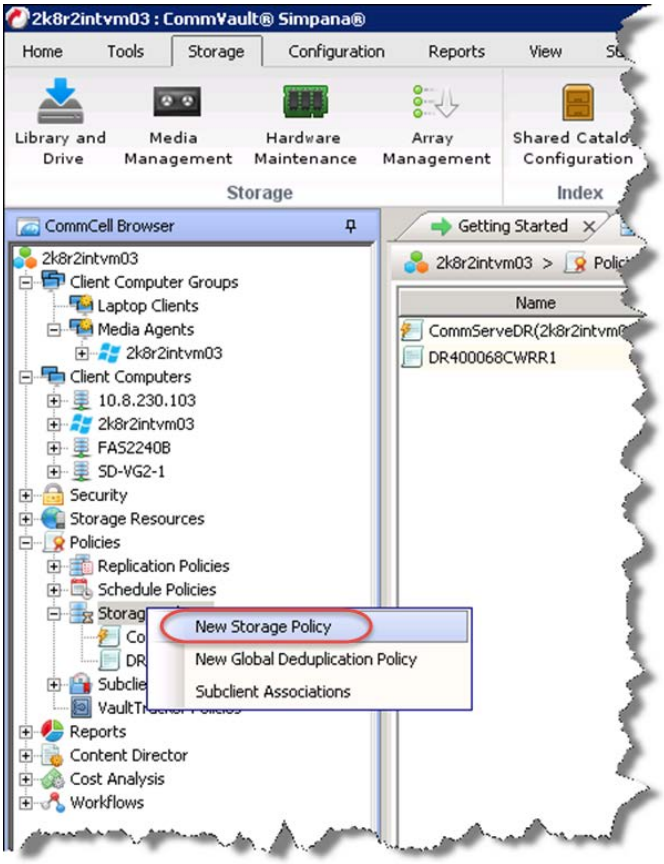


19. Click **OK**

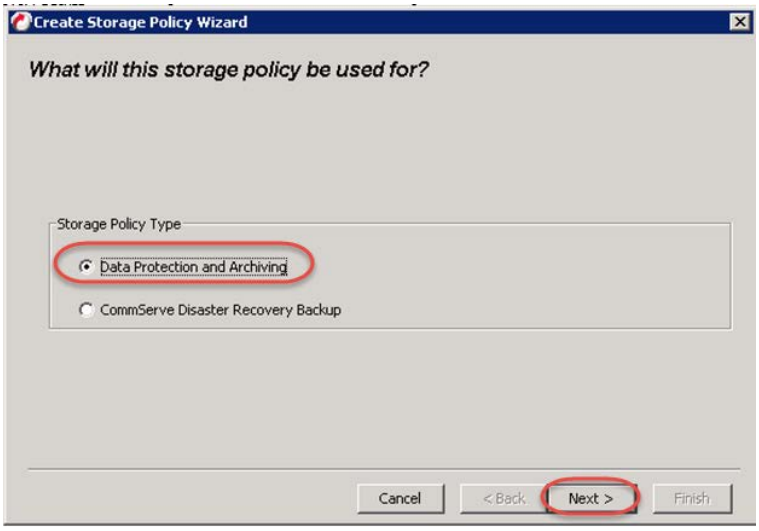
20. Results show that the library is now configured. Close the Library and Drive Configuration dialog box.



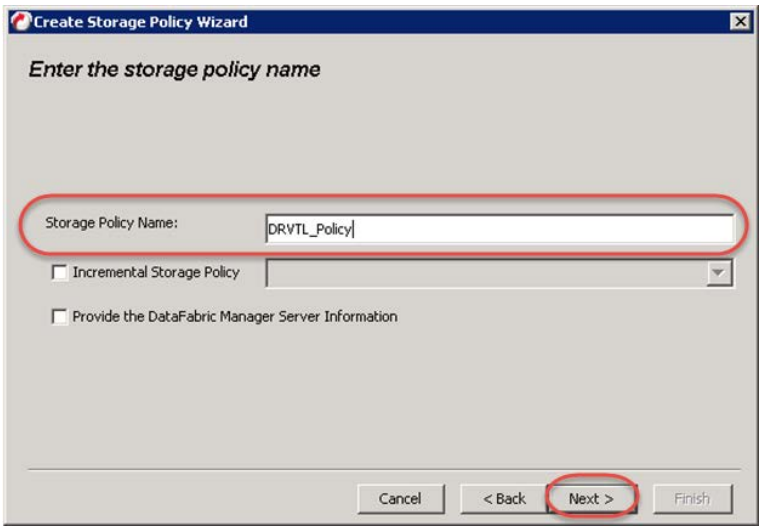
21. Create a new Storage Policy by selecting **New Storage Policy** after selecting **Policies** > **Storage Policies** in the navigation pane.



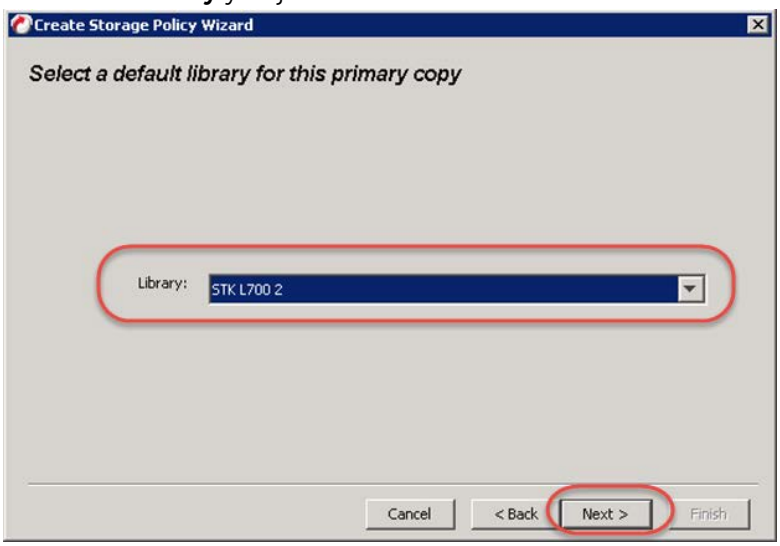
22. Click the **Data Protection and Archiving** radio button and then click **Next**.



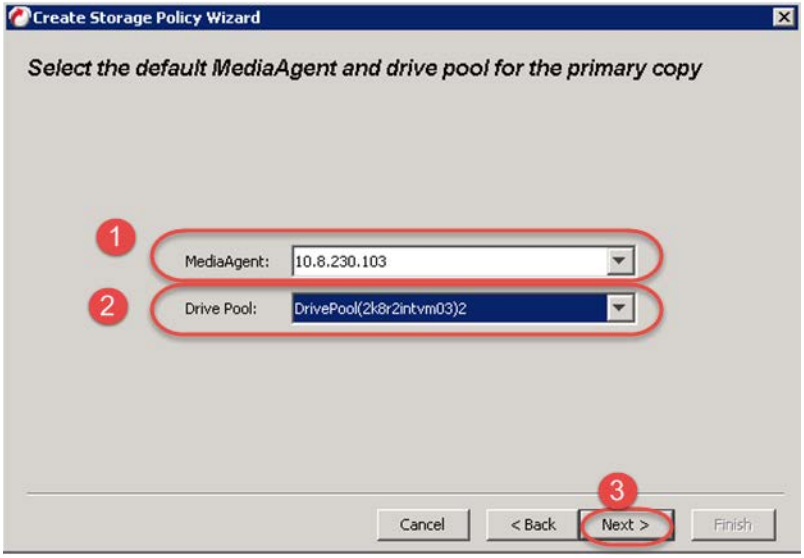
23. Enter a Storage Policy Name and click **Next**.



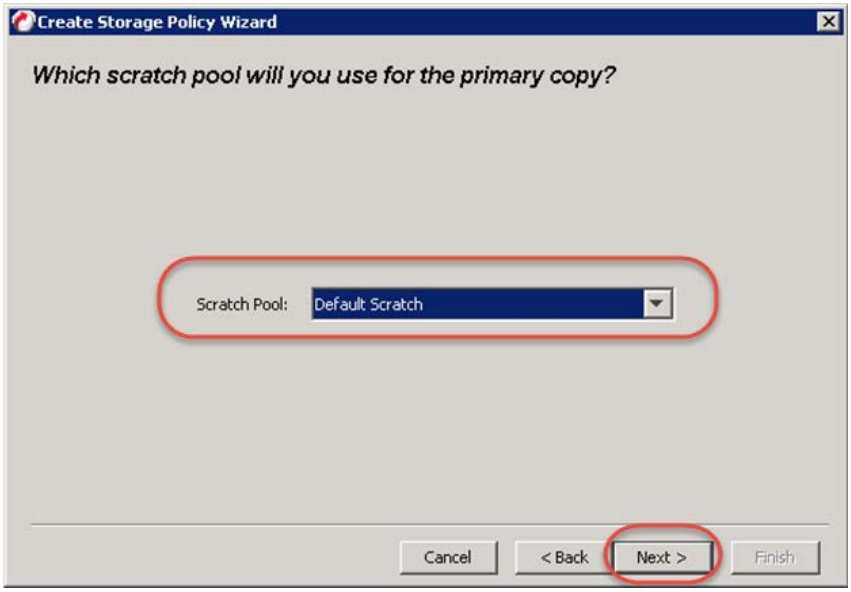
24. Select the **Library** you just added and click **Next**.



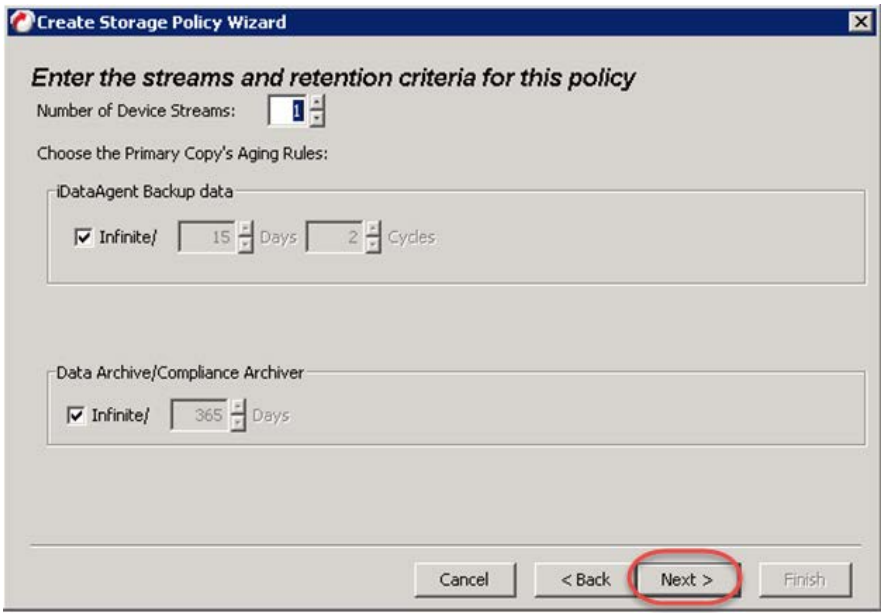
25. Make sure that these selections are correct and click **Next >**.



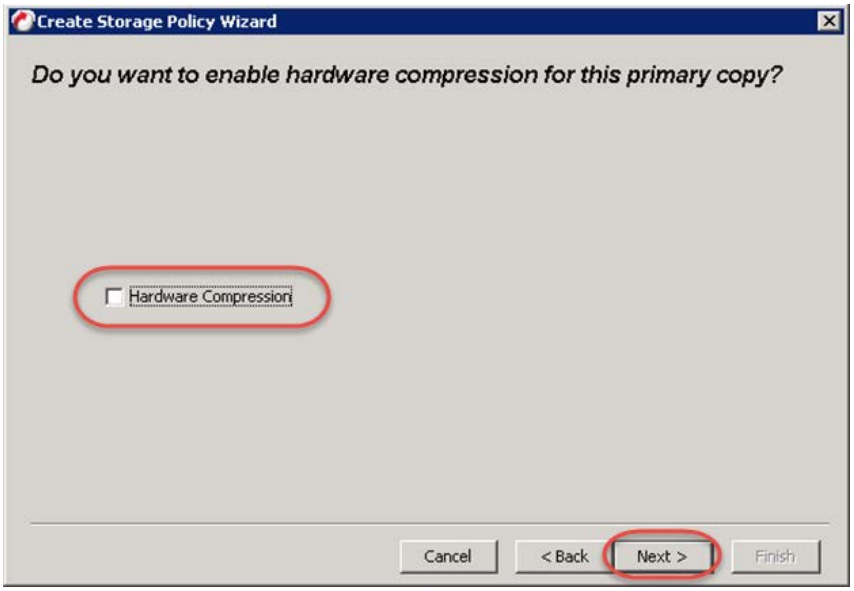
26. Select the **Scratch Pool** that you want and click **Next**.



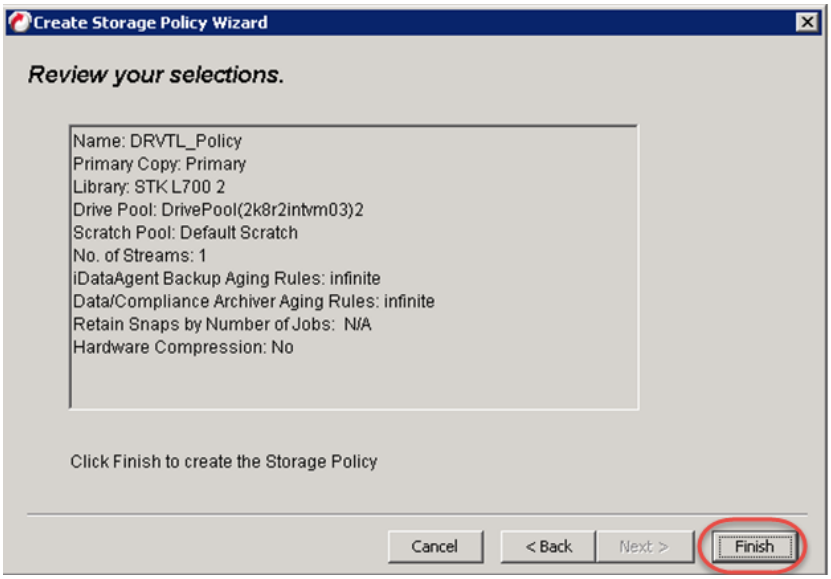
27. Click **Next >**.



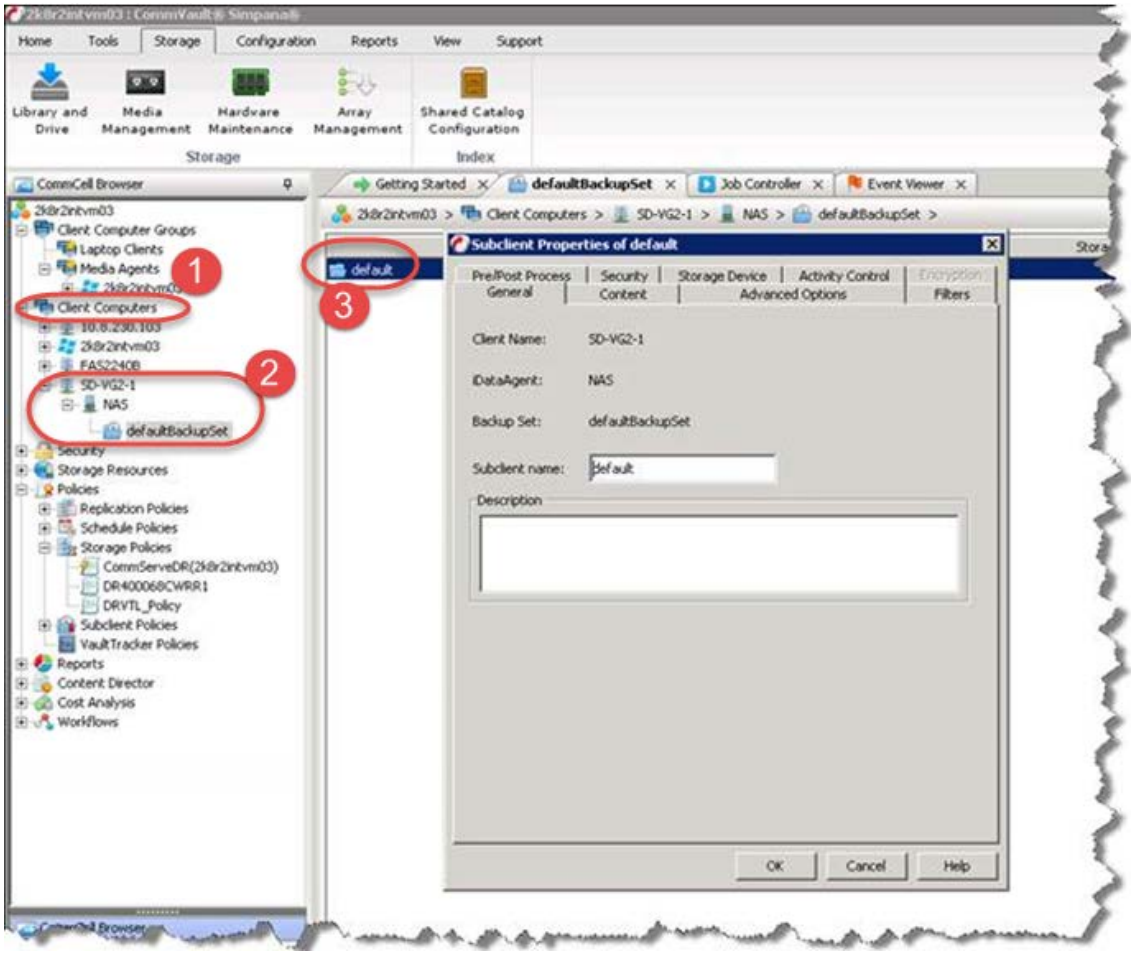
28. Clear the **Hardware Compression** checkbox. Click **Next >**.



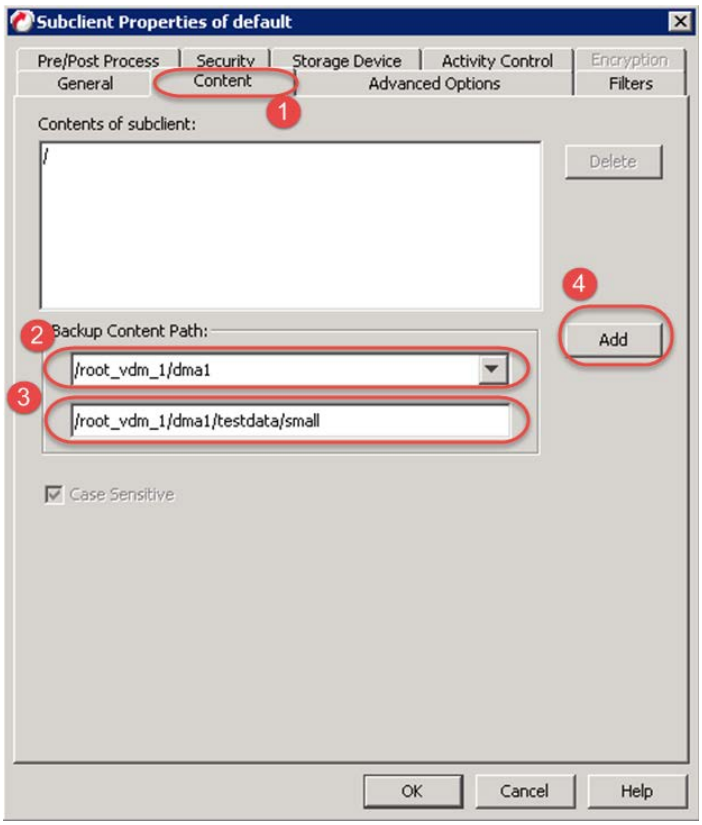
29. Click **Finish**.



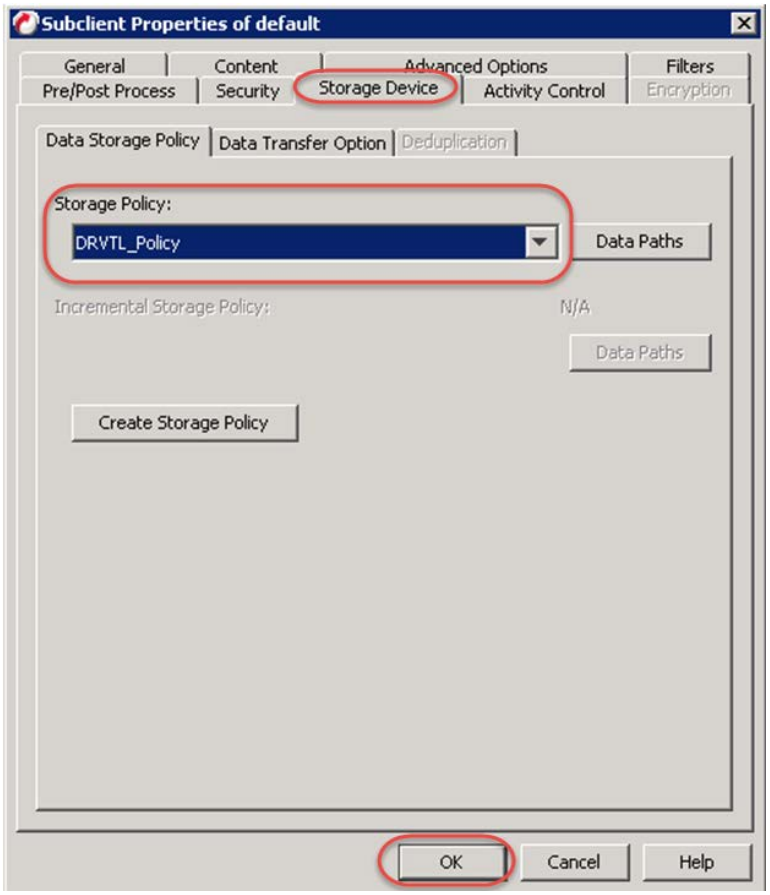
30. In the **CommCell Console,** expand the newly added filer in the tree under **Client Computers**. You should see a **NAS** node followed by a **defaultBackupSet** node. Double-click **default** in the right pane.



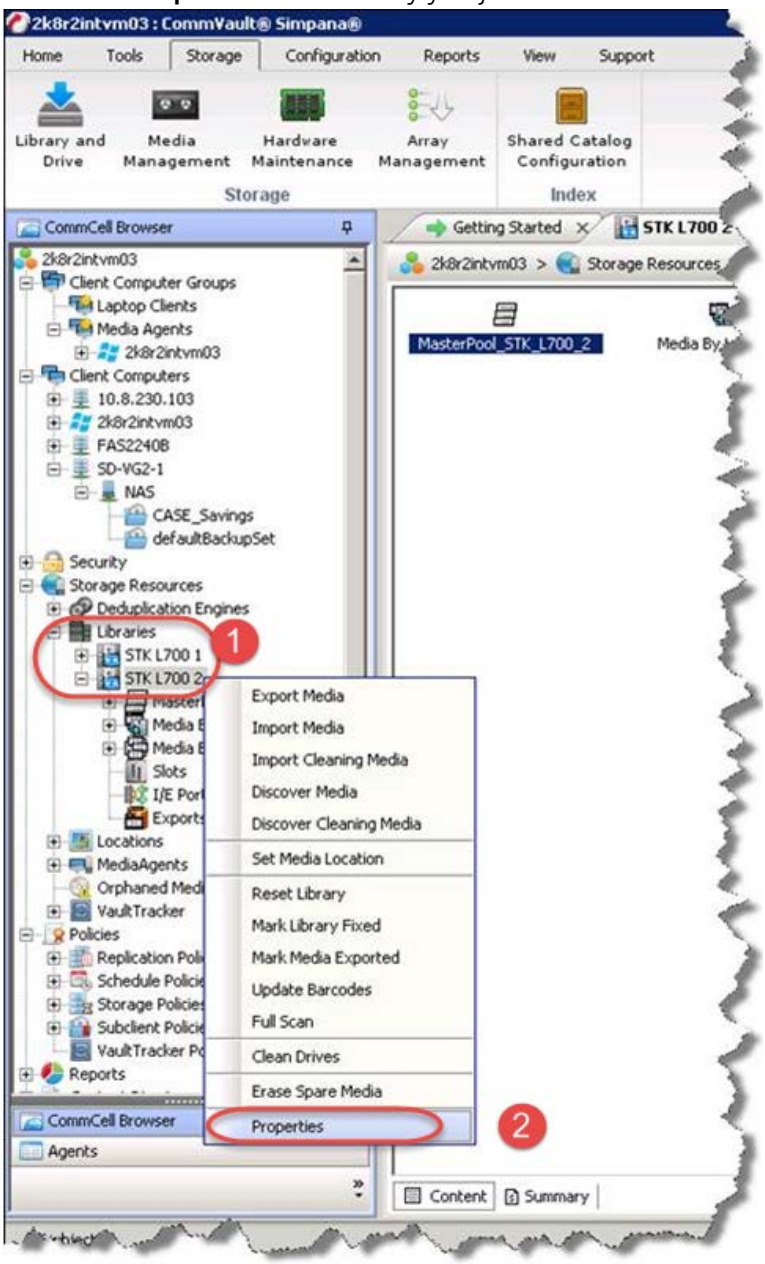
31. Enter the path to back up in the text box of the **Content** tab and click **Add**. Use the drop down box to help you navigate the filer you want to back up.



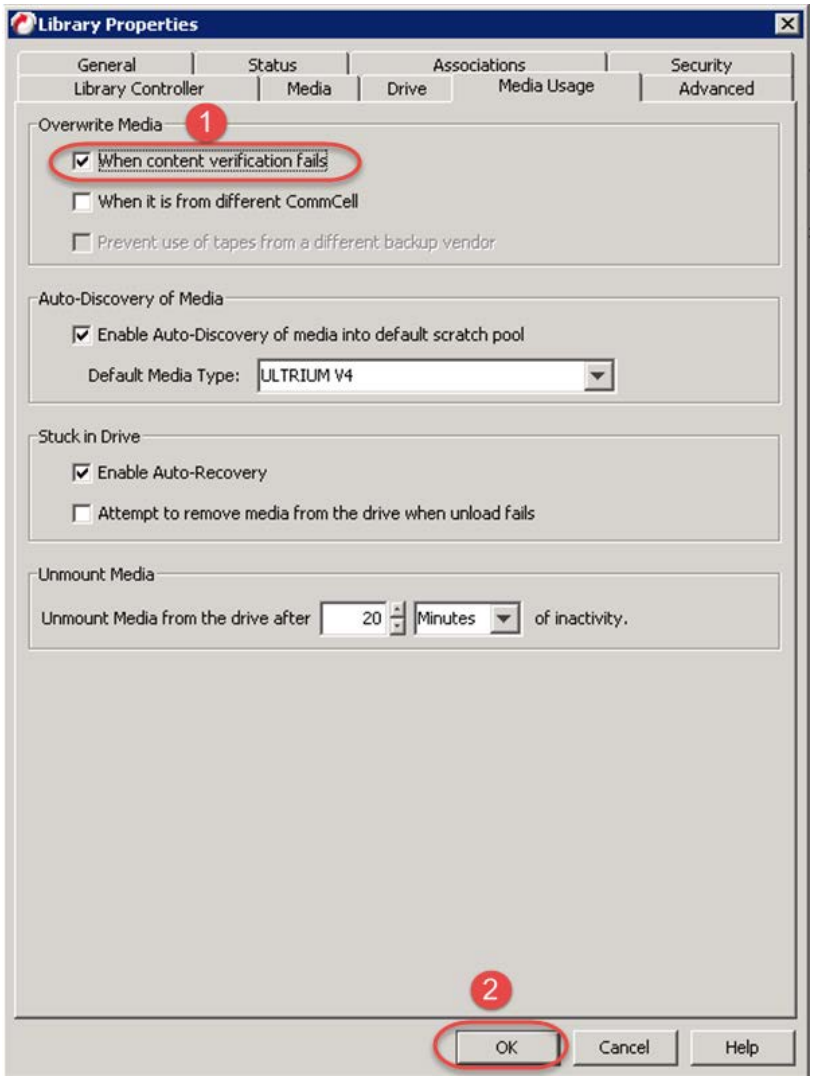
32. Specify the **Storage Policy** that you just added and click **OK**.



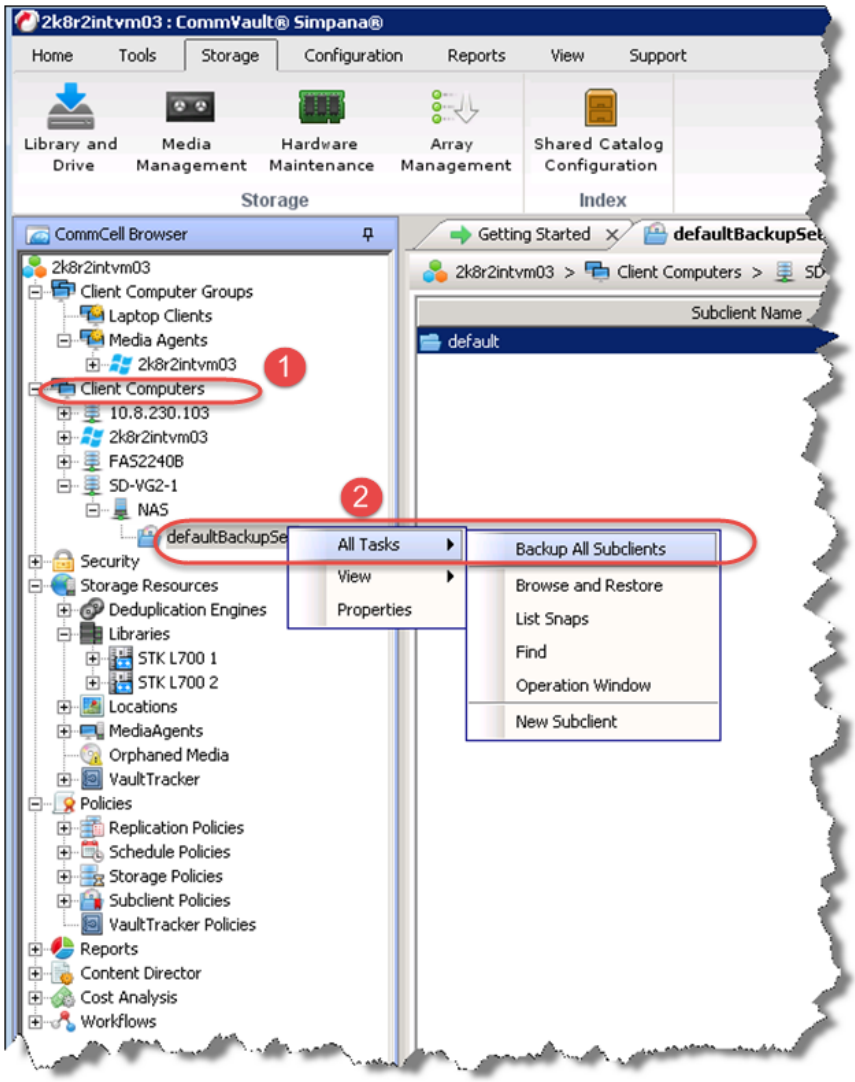
33. Select the **Properties** of the library you just added.



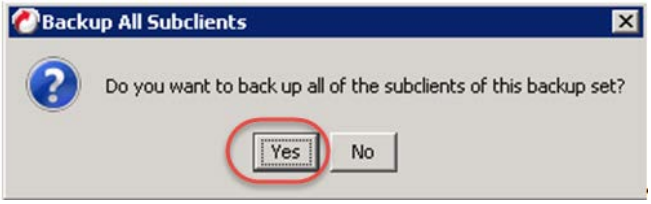
34. Select the **When Content Verification Fails ch**eckbox in the Media Usage tab and click **OK**.



35. Select the newly updated **defaultBackupSet** and select **All Tasks** > **Backup All Subclients** context menu to start the backup job.

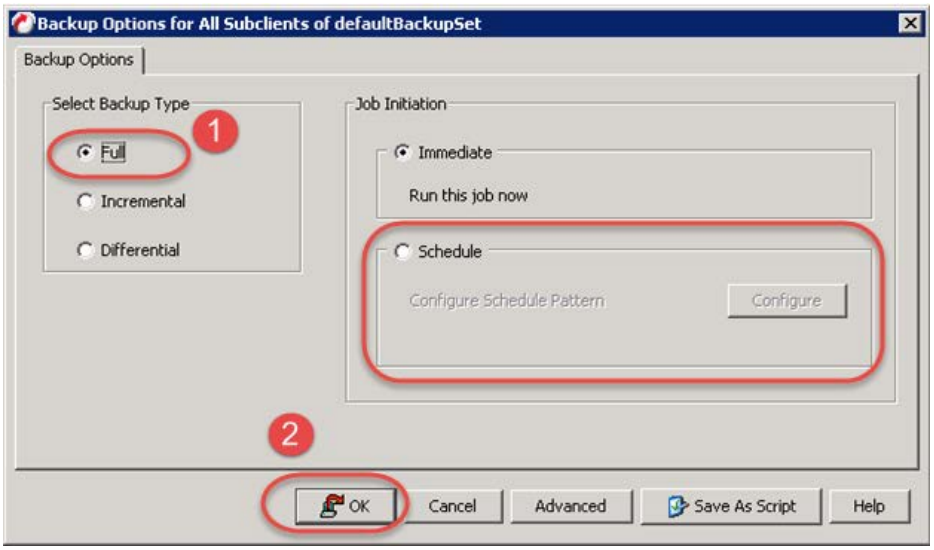


36. Click **Yes** to confirm backup.

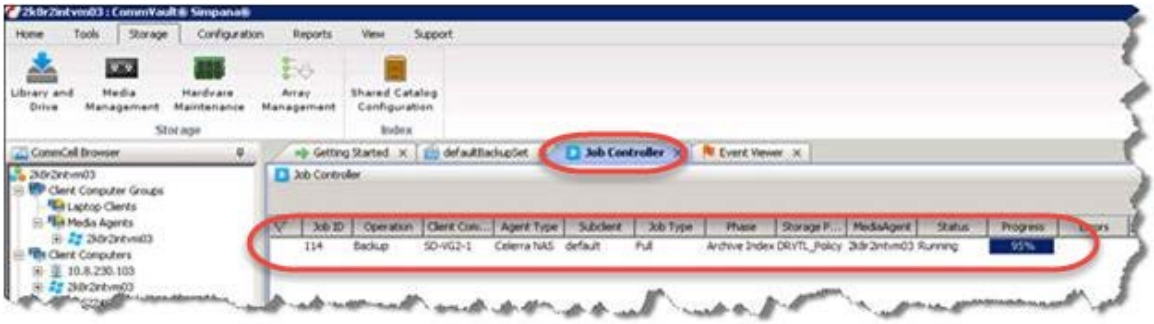


37. Click **OK**.

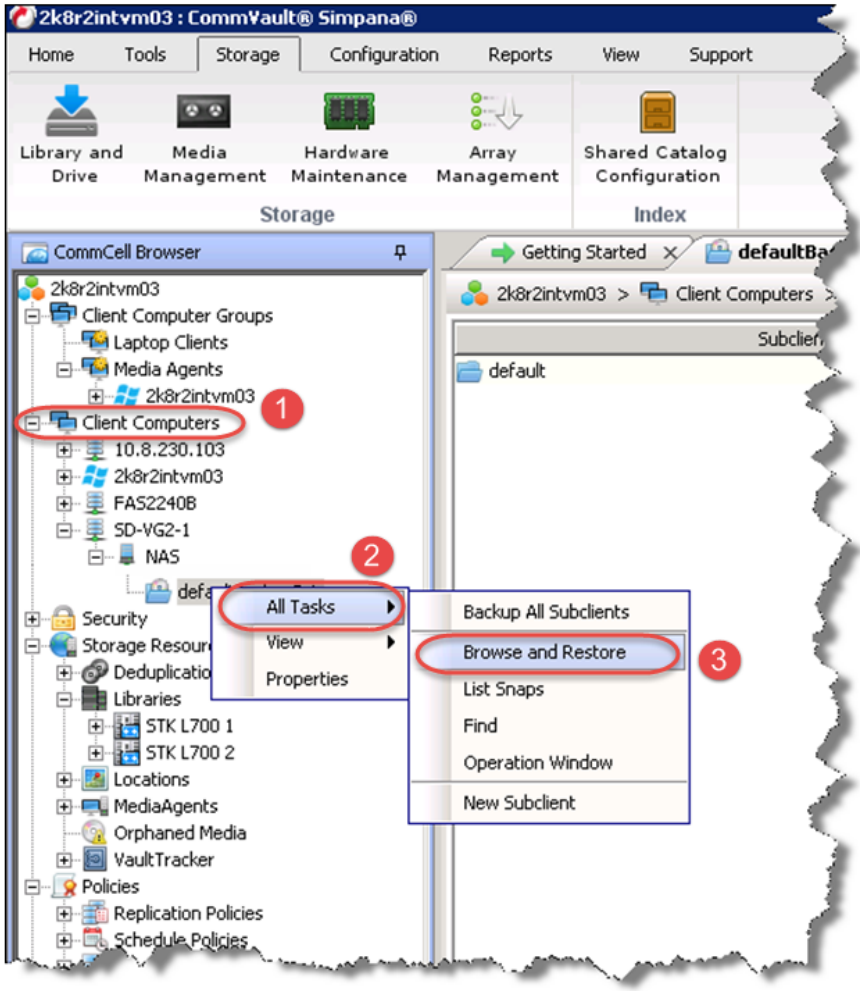
38. Choose **Full** for the first backup job. You may schedule the job for later if needed. Click **OK**.



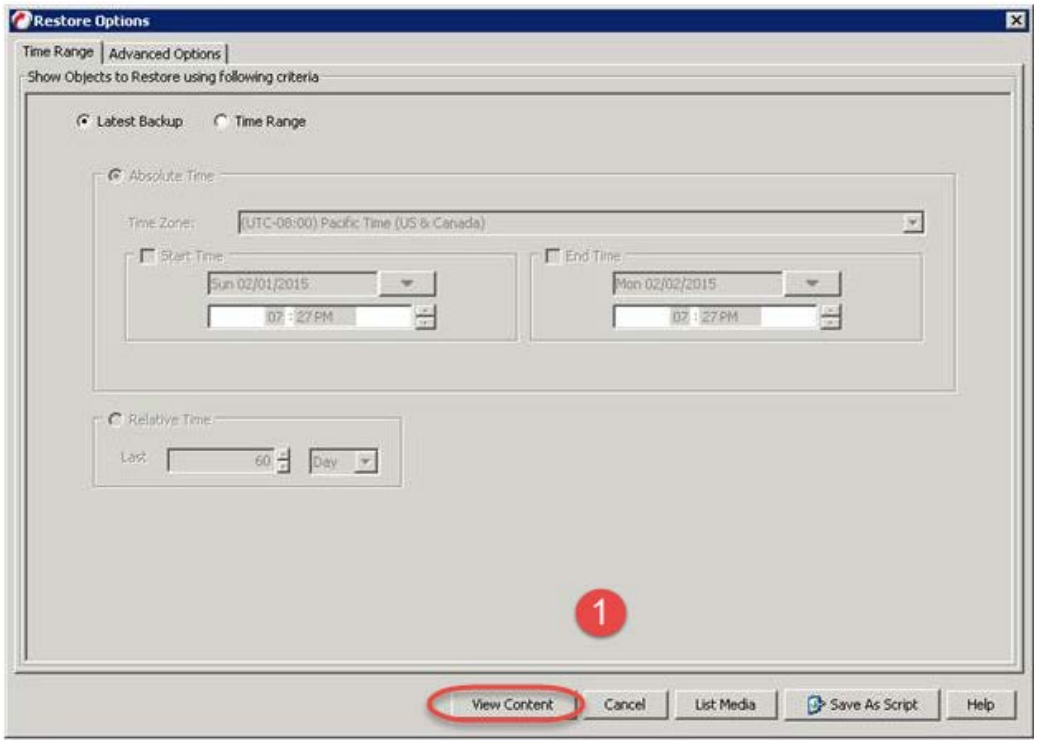
39. Monitor the progress of the job from the **Job Controller** tab.



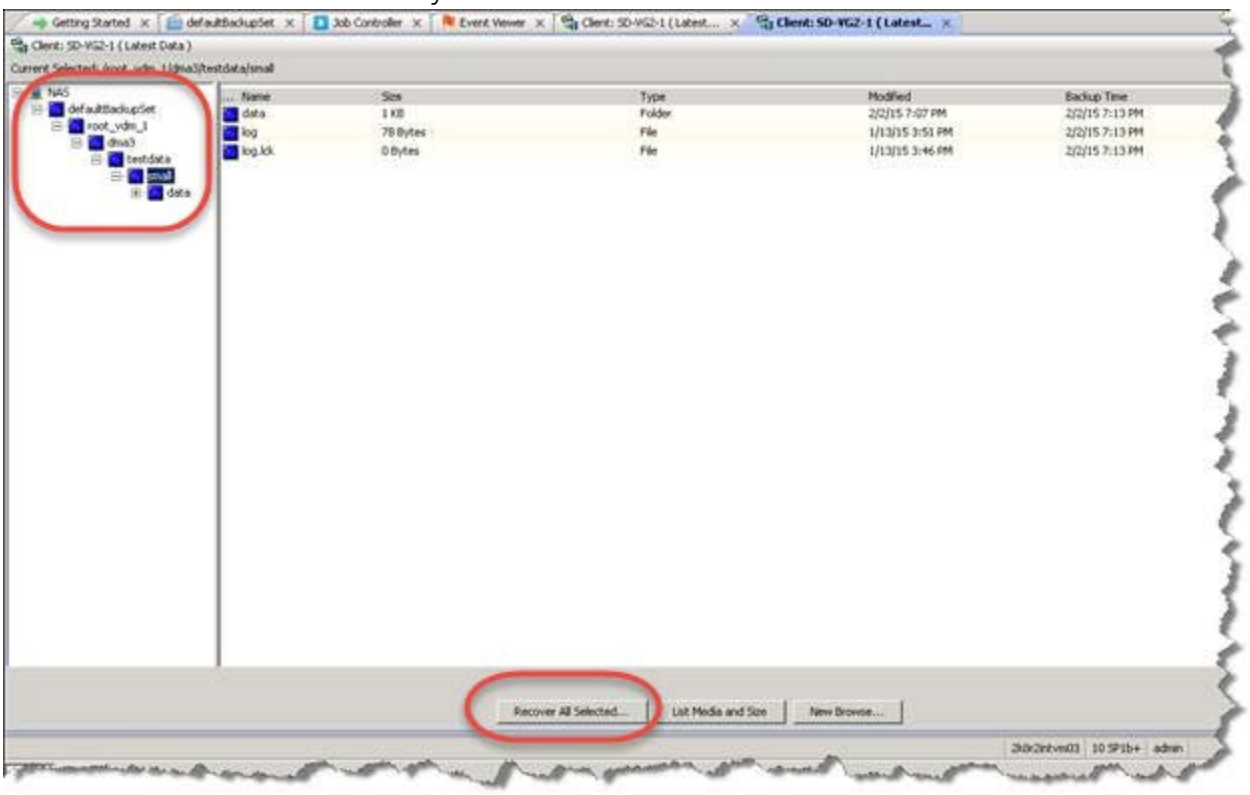
40. Expand **Client Computers** in the tree along with the filer you want to restore to. Expand **NAS** and **defaultBackupSet** then select **All Tasks** > **Browse and Restore** context menu for **defaultBackupSet**..



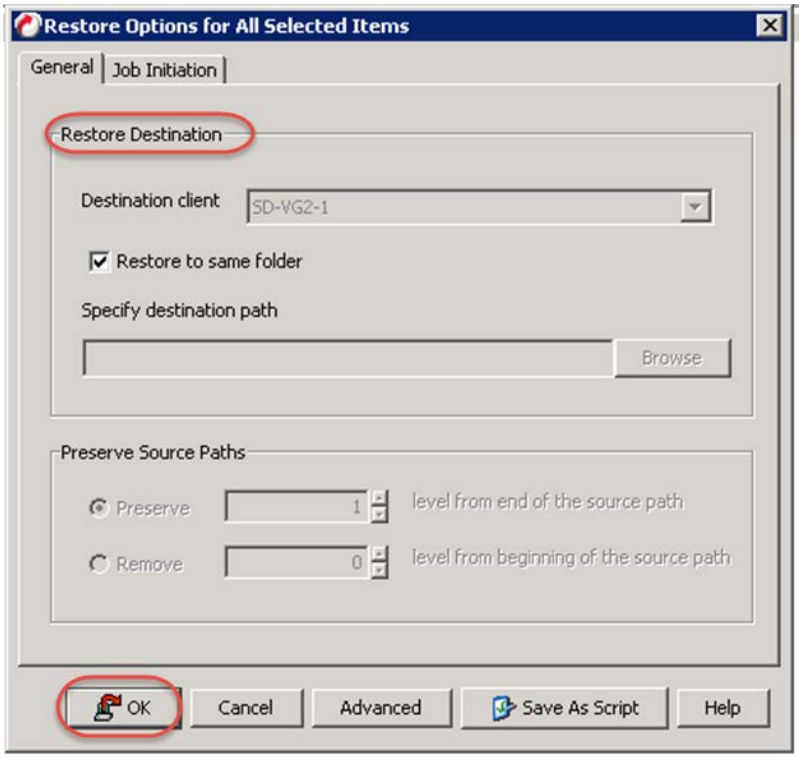
41. Select the backup you want to restore and click **View Content**.



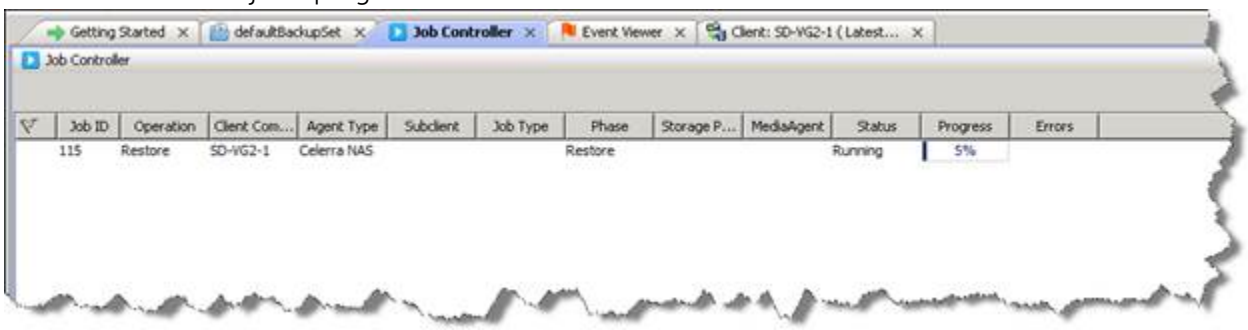
42. Select the data you want to restore and click **Recover All Selected...**



43. Specify the destination of the restore and click **OK**.



44. Monitor the job's progress from the **Job Controller** tab.

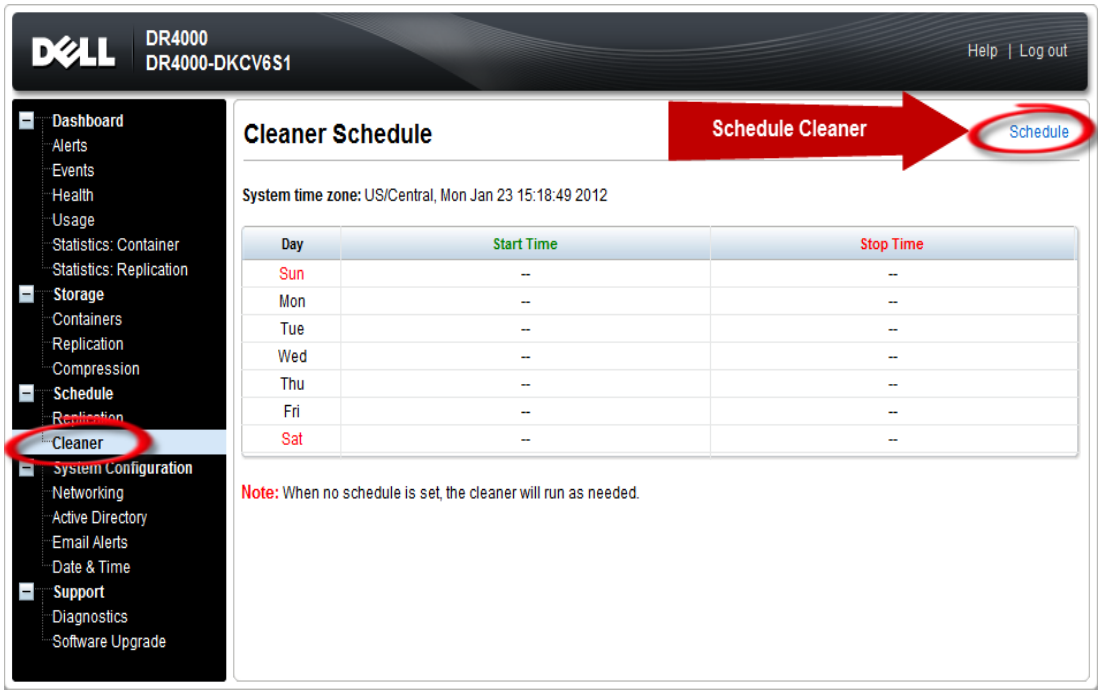


4 Setting up the DR Series system cleaner

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

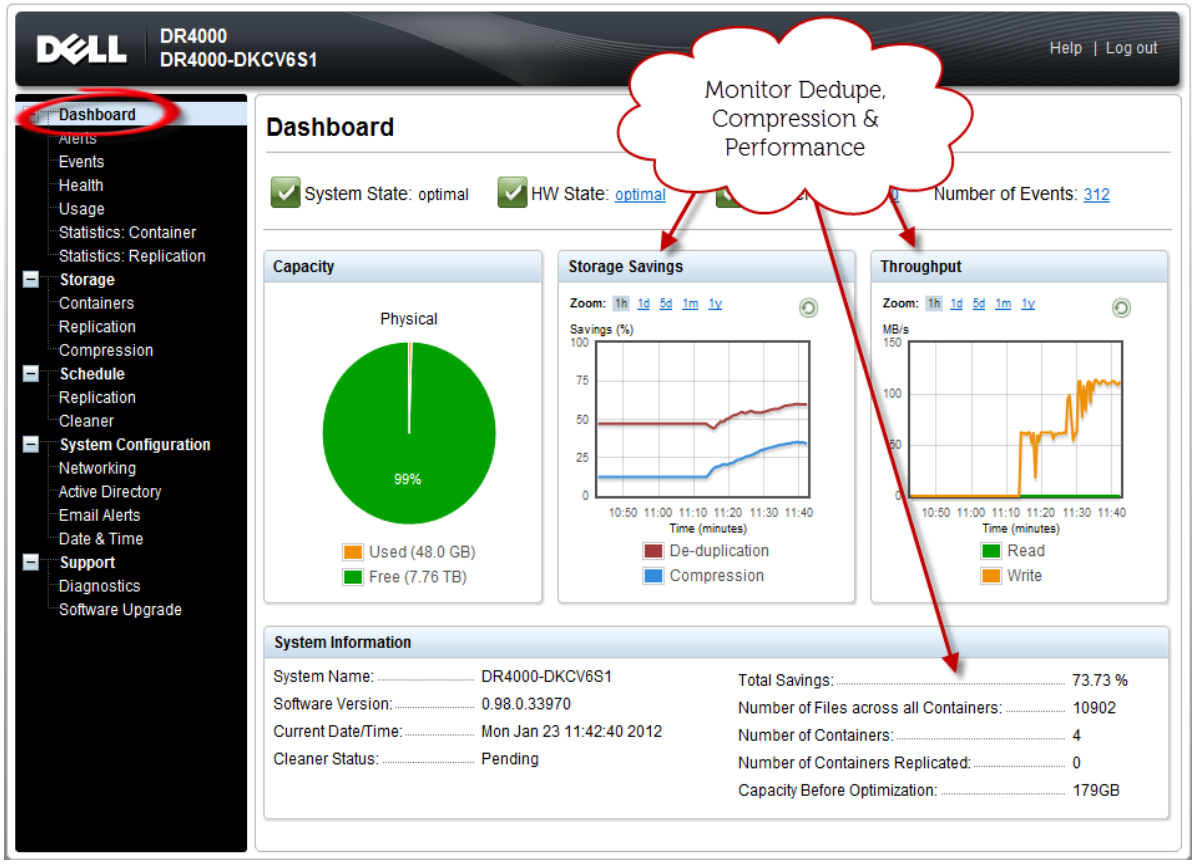
If necessary, you can perform the procedure shown in the following screenshot to force the cleaner to run. After all the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place, and generally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

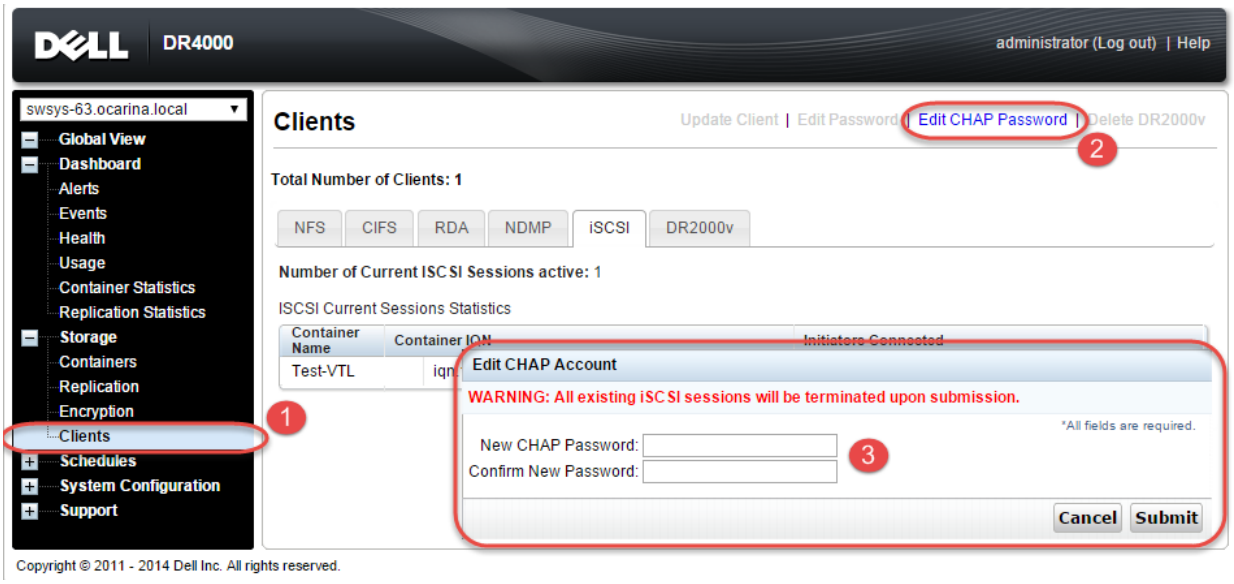
A.1.1 iSCSI account details and management

By default the iSCSI Username will be the **hostname** of the DR and can be confirmed by reviewing the output of the `iscsi –account --user` command. For example:

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

The default iSCSI Password is "**St0r@ge!iscsi**". This can be modified by navigating to the **Clients** Navigation option and selecting the **iSCSI** tab under the **Clients** menu. Select the the **Edit CHAP Password** and fill in the new password as needed.

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

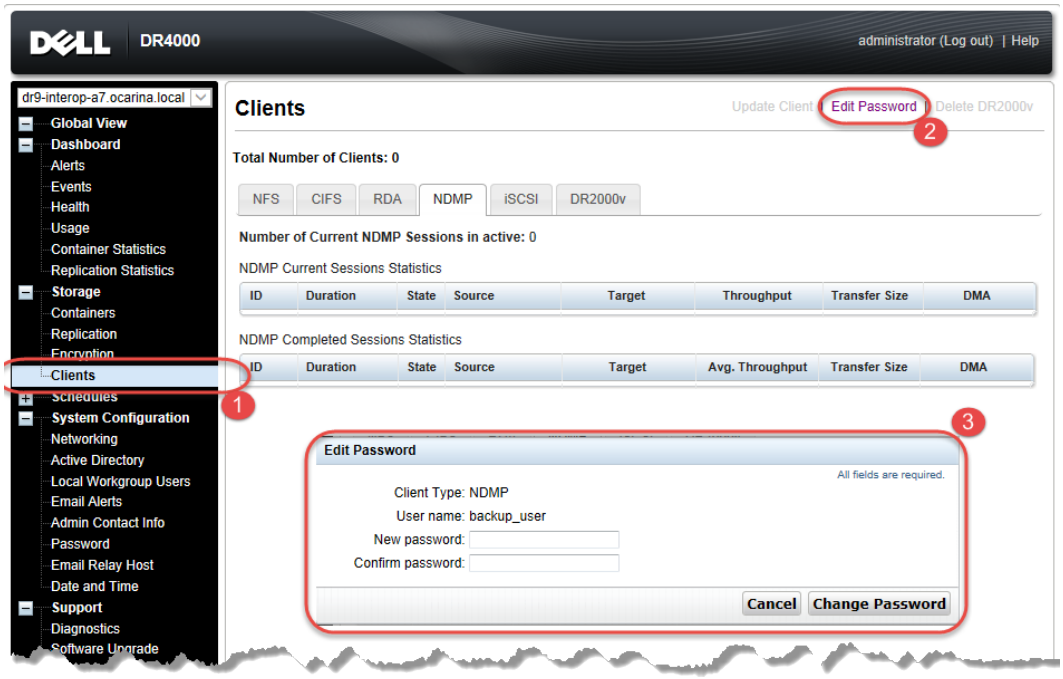


Alternatively, you may also use the "iscsi –setpassword" cli tool to change the iSCSI CHAP Password setting as shown in the following example:

```
> 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 "**backup_user**" and can be confirmed using the web UI interface:



Or, by using the following command line interface:

```
ndmp –show command:
administrator@dr9-interop-a7 > ndmp --show
NDMP User:      backup_user
NDMP Port:      10000
```

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

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

A.2 VTL default account summary table

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

A.3 Managing VTL media and space use

A.3.1 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.3.2 Physical 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.3.3 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.3.4 Media retention and grouping

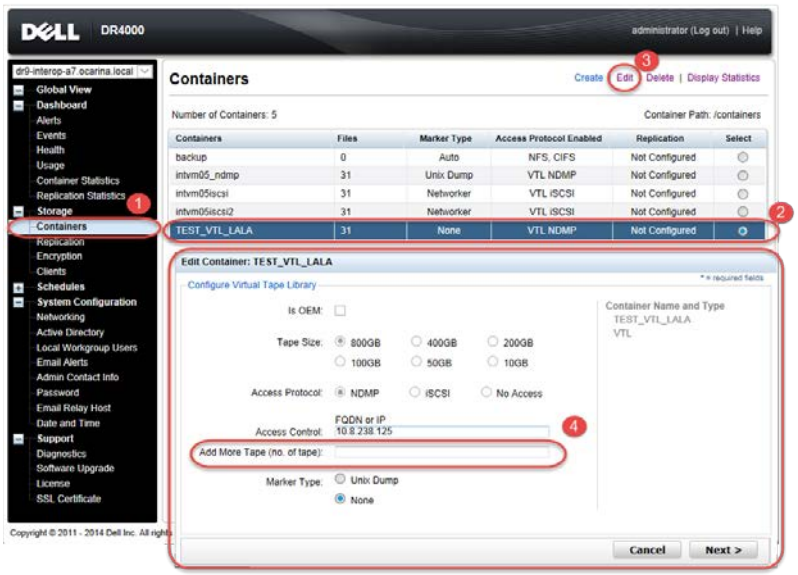
Due to the nature of Virtual Tape Libraries media must be managed in order to insure that physical capacity is reclaimed in an orderly fashion t avoid running out of space and disrupting operations. Media must be grouped within the data management application, such as NetVault: Backup, in a way that 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 insures 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.3.5 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.3.6 Adding the VTL media to the 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 dialogue 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. For example:

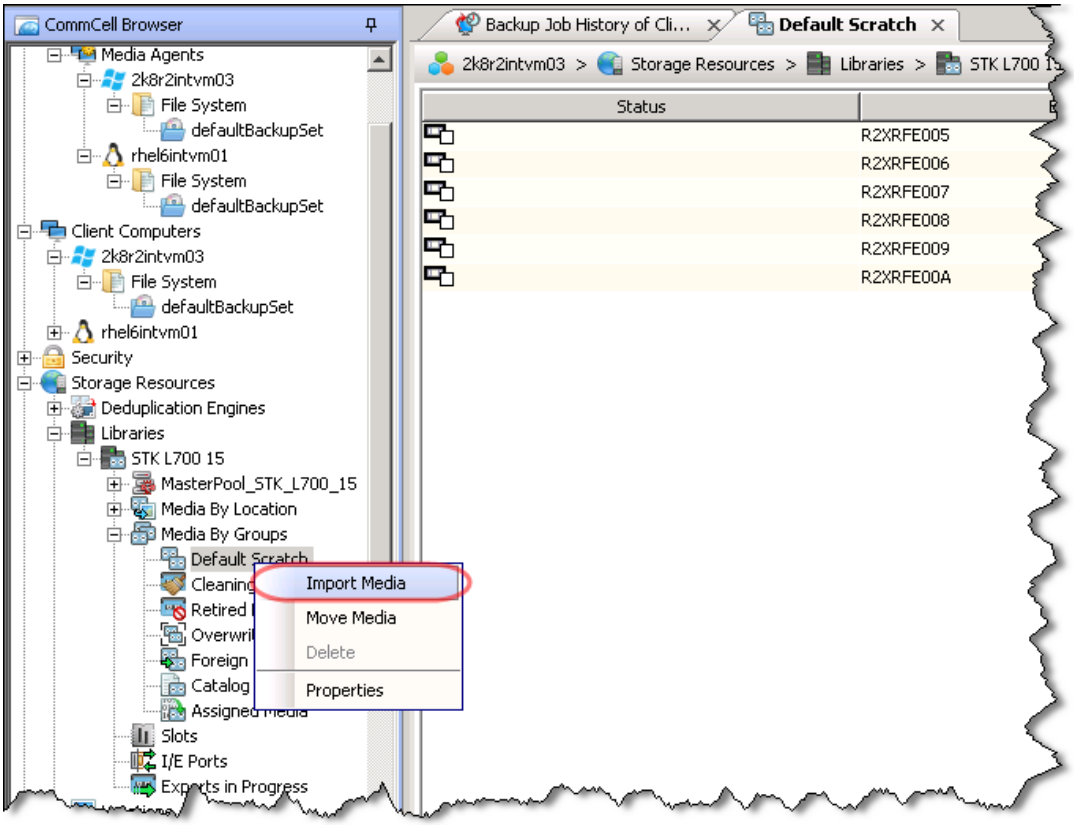
```
> vtl --create_carts --name TEST_VTL_LALA --tapes 10

Created 10 cartridges
```

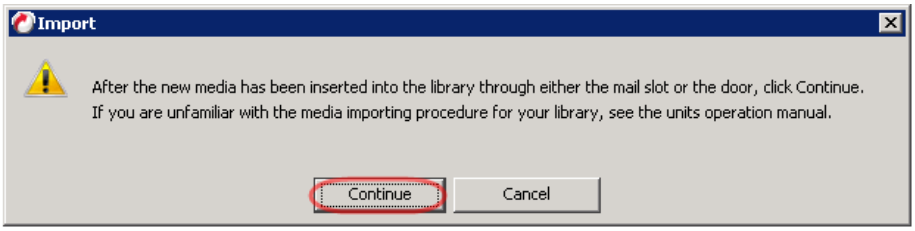
A.3.7 Updating CommVault to identify newly added VTL media

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

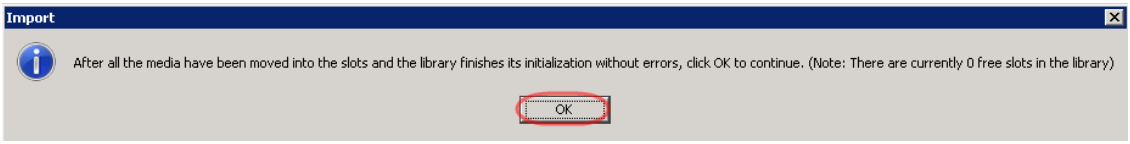
1. Select the **Default Scratch** of the library and select **Import Media**.



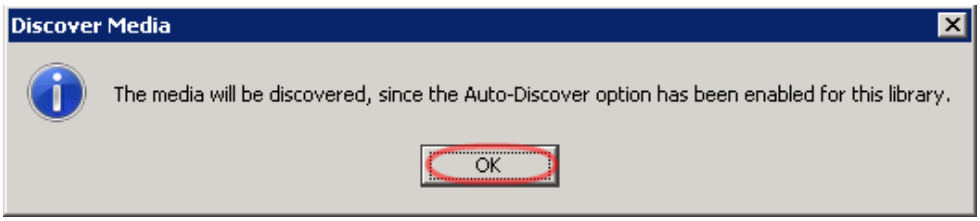
2. Click Continue.



3. Click **OK**.

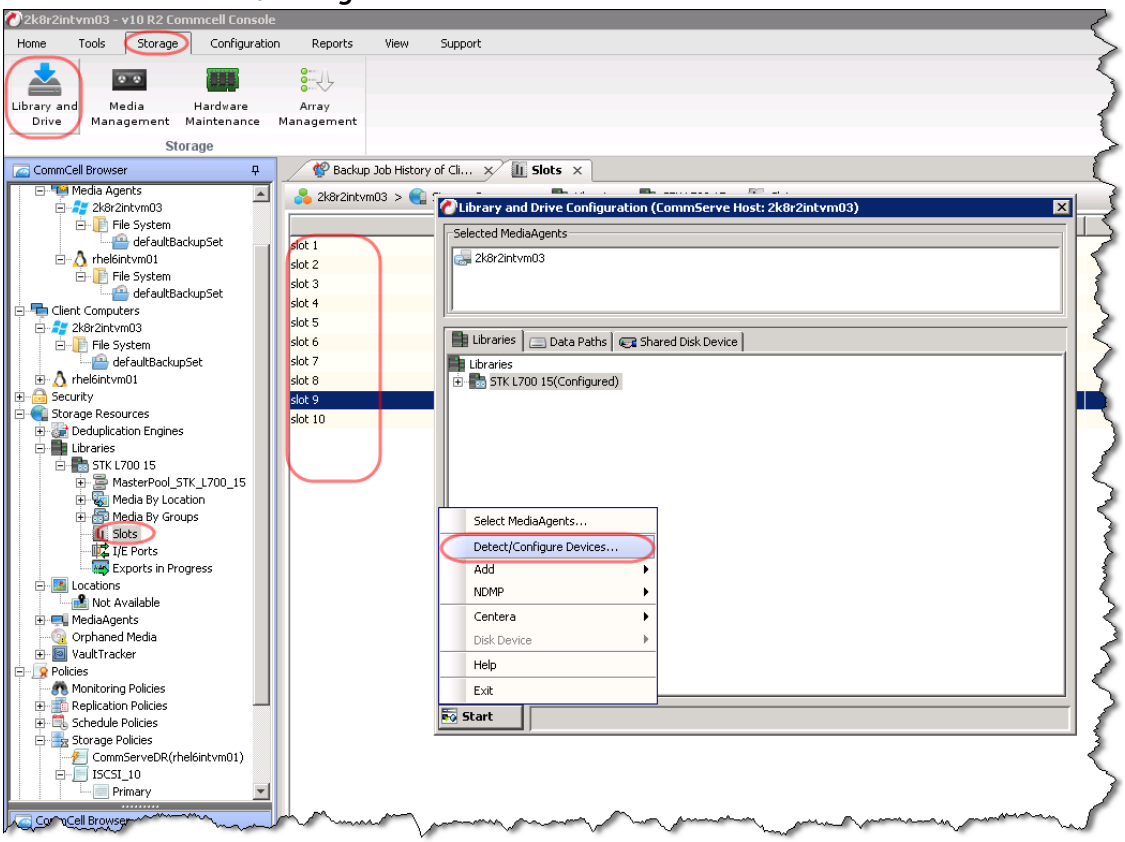


4. Click **OK**.

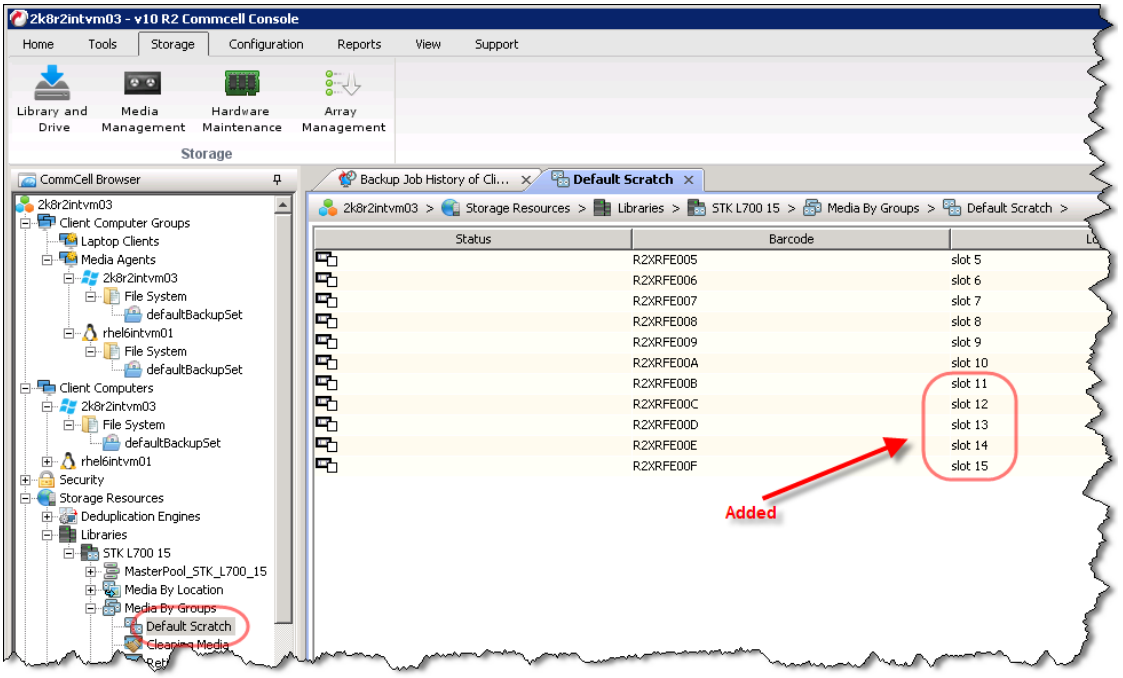


5. Review the resulting log and click **Close**.

6. Select **Start** > **Detect/Configure Devices...**



7. Notice the added tapes that were added.



A.3.8 Space reclamation

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.

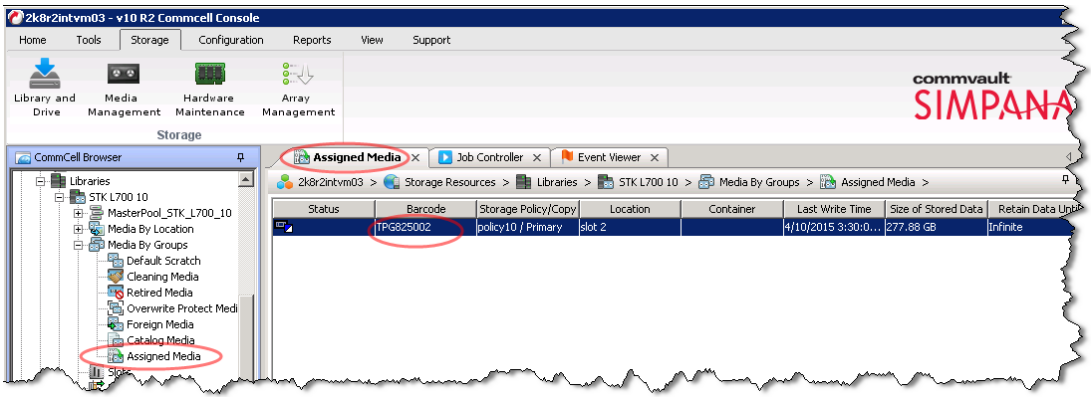
Product-**specific** Guidelines

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.

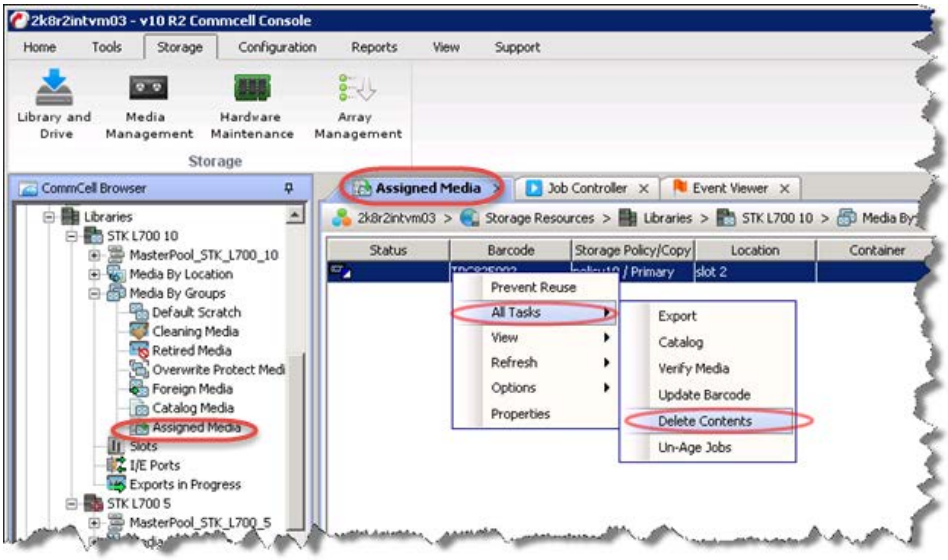
1. Identify the DR VTL tapes that you want to remove backups from via the **Simapana Commcell Console**. Note the **Barcodes** of the **Assigned** tapes that you want to erase and reclaim their storage on the DR.

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

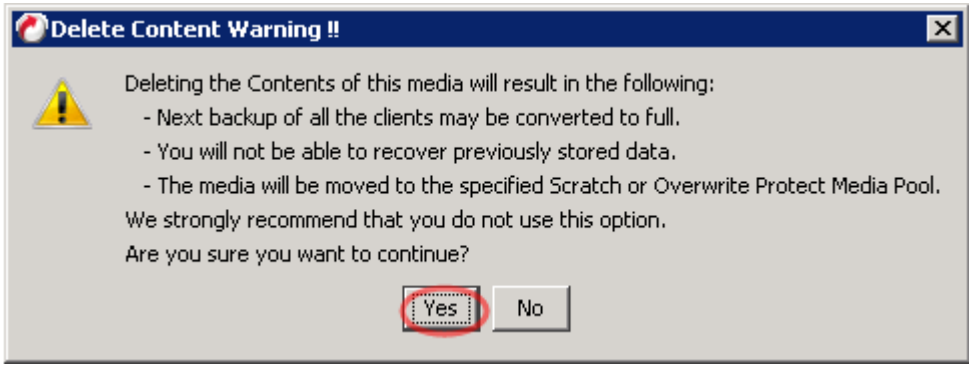
2.



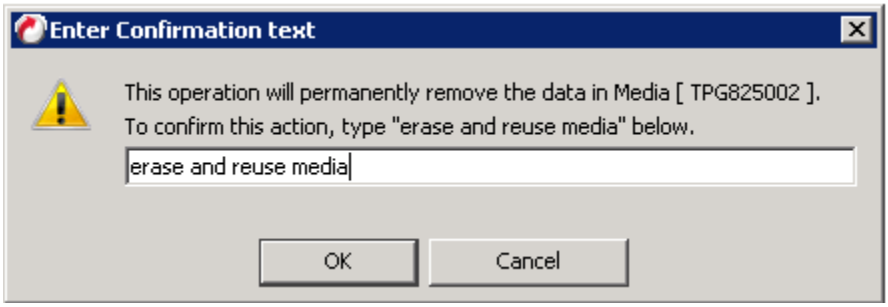
3. Select **All Tasks** > **Delete Contents** context menu for the tapes you want to erase.



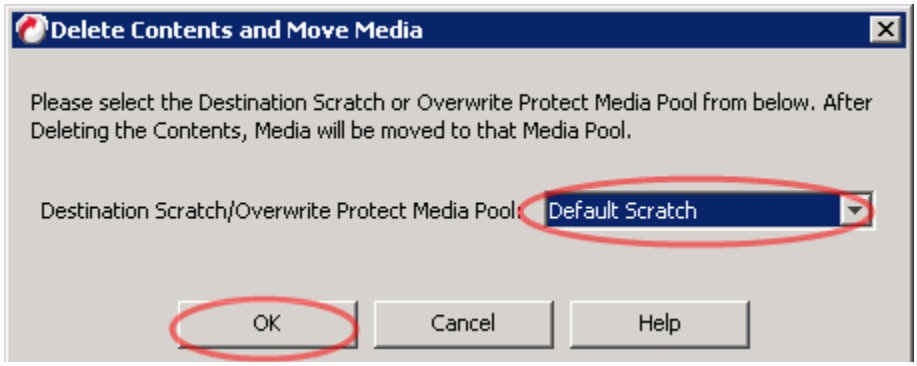
4. Click **Yes** in this warning box if you agree.



5. Enter "**erase and reuse media**" in the text box to confirm you want to remove the data from the selected tape.



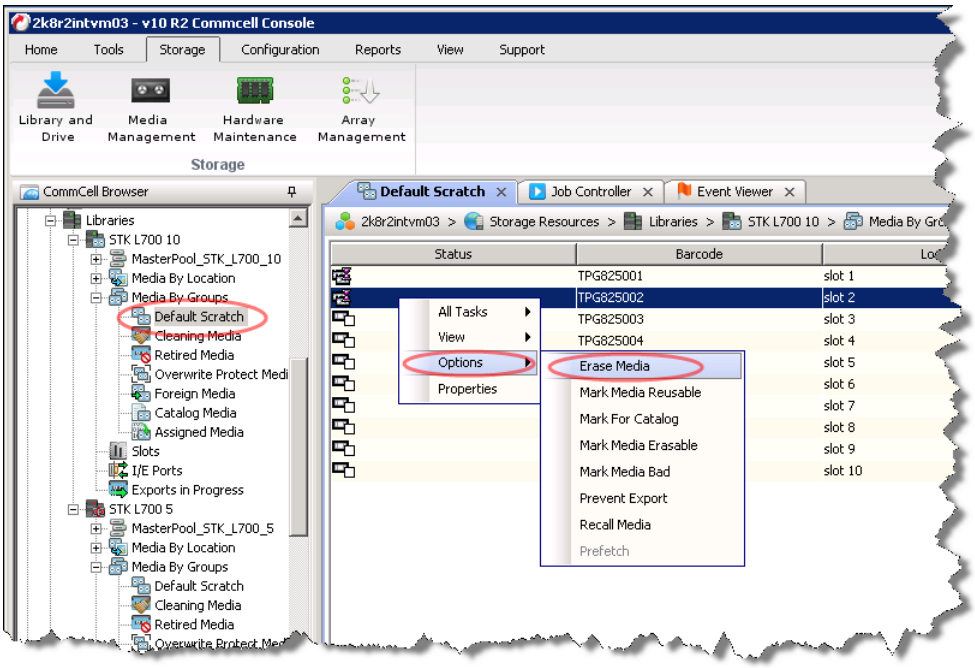
6. Select the **Media Pool** you want the tape to be moved to.



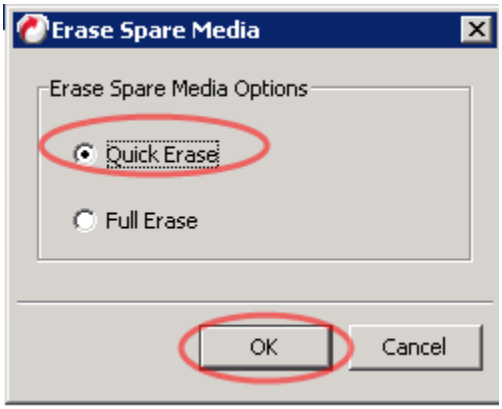
7.

8. Find that tape in the **Media Pool** you moved it to and select the **Options** > **Erase Media** context menu.

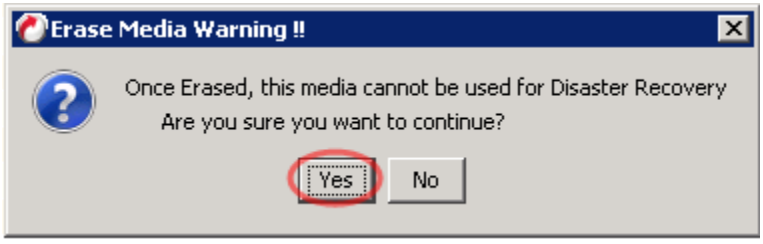
9.



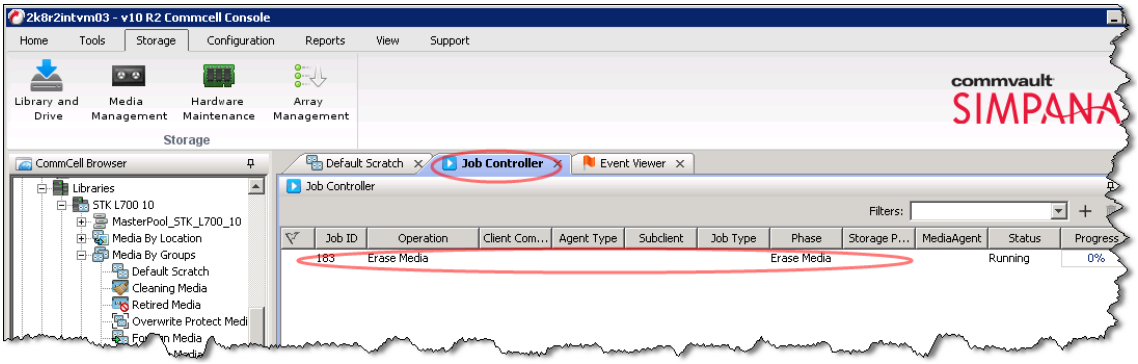
10. Select **Quick Erase** and click **OK**.



11. Click **Yes** if you want to erase the media.



12. Watch the progress of the erase from the **Job Controller** tab.



13. Once the reconciliation process has been completed on the CommVault software. From the DR initiate a cleaning cycle either via the UI or via the command line. For example:

```
> maintenance --filesystem --reclaim_space

Successfully started cleaner.
```

14. Check to make sure 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 %
```

B Glossary

RDA : Rapid Data Access, Dell proprietary technology for faster data access.

Dedupe Backup : In this mode Deduplication is done on the Client and then the deduplicated packets are sent to DR Series System.

Passthrough Backup : In this mode Deduplication is done on DR Series System after data is transferred from Clients and backup media server.

Synthetic backup: A synthetic backup is identical to a regular full backup in terms of data, but it is created when data is collected from a previous, older full backup and assembled with subsequent incremental backups.

Virtual Synthetic Backup/Optimized synthetic Backup: A synthetic backup that avoids the need to move data across the network. The media server tells the storage server which full and incremental images to use to create the synthetic image.

DMA: Data Management Application such as NetVault: Backup

CIFS: Common Internet File System

NFS: Network File System

VTL: Virtual Tape Library

iSCSI: Internet Small Computer System Interface

FQDN: Fully Qualified Domain Name (Host name and domain)