



Setting Up Dell™ DR Series Deduplication Appliance as Backup Target on CommVault Simpana™ 10

Dell Engineering
January 2014

Revisions

Date	Description
January 2014	Initial release

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.

© 2014 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, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. 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. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. 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 Install and Configure the DR Series Deduplication Appliance..... 5
- 2 Set up CommVault Simpana 10 13
 - 2.1 Single System Environment (DR as CIFS Disk Library)..... 13
 - 2.2 Single System Environment (DR as NFS Disk Library)..... 15
 - 2.3 Replicated System Environment 17
 - 2.4 Use Continuous Data Replicator to replicate client data to a DR container..... 25
 - 2.5 Create backup job with DR Series Deduplication Appliance as the target..... 28
- 3 Set Up the DR Series Deduplication Appliance Cleaner 37
- 4 Monitoring Deduplication, Compression and Performance 38



Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a Backup device for CommVault Simpana 10. This paper is a quick reference guide and does not include all DR Series Deduplication Appliance deployment best practices.

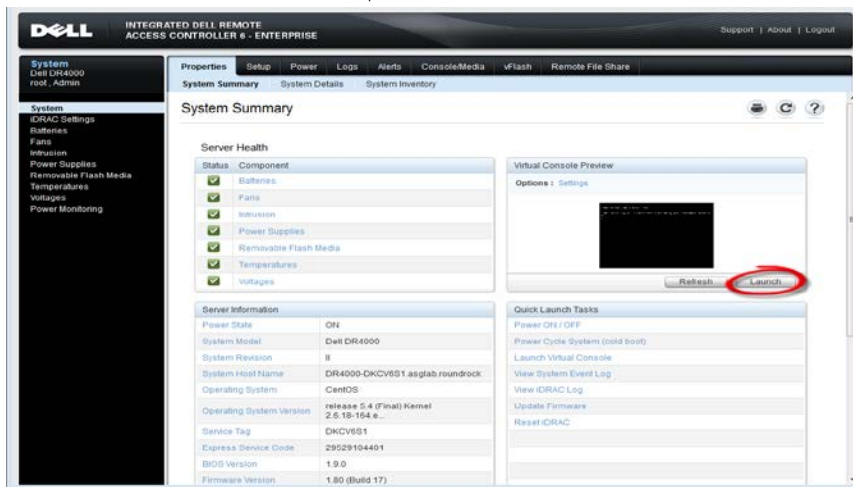
See the DR Series Deduplication Appliance documentation for other data management application best practices whitepapers at <http://www.dell.com/support/troubleshooting/us/en/04/Product/powervault-dr4100>, under "Manuals & Documentation".

Note: The DR Series Deduplication Appliance/CommVault Simpana build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/Symantec NetBackup software version used.

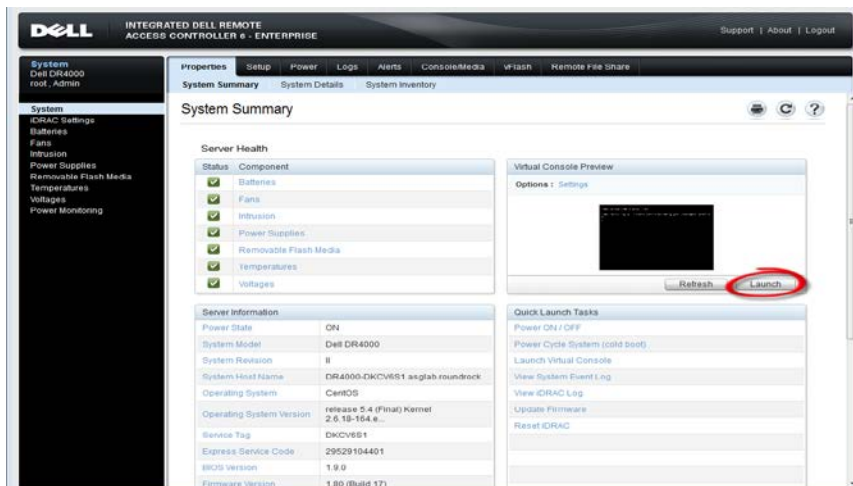


1 Install and Configure the DR Series Deduplication Appliance

1. Rack and cable the DR Series Deduplication Appliance, and power it on.
2. Please refer to *Dell DR Series System Administrator Guide*, under sections of "iDRAC Connection", "Logging in and Initializing the DR Series System", and "Accessing iDRAC6/iDRAC7 Using RACADM" for using iDRAC connection and initializing the appliance.
3. Log in to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use user name and password of "root/calvin".



4. Launch the virtual console.



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

```
Ocarina release 1 (EAR-1.00.00) Build: 32858
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password: St0r@ge!
```

6. 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:
```

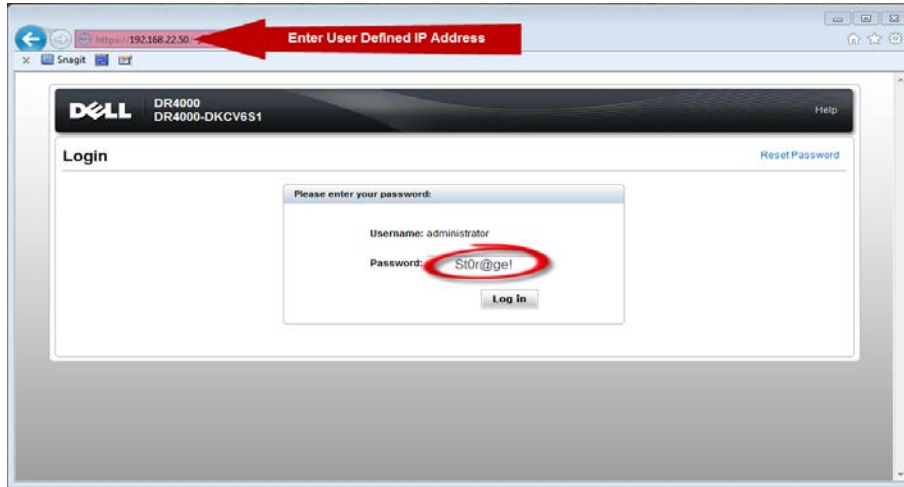
7. View the summary of preferences and confirm that it is correct.

```
=====
                          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) ? _
```

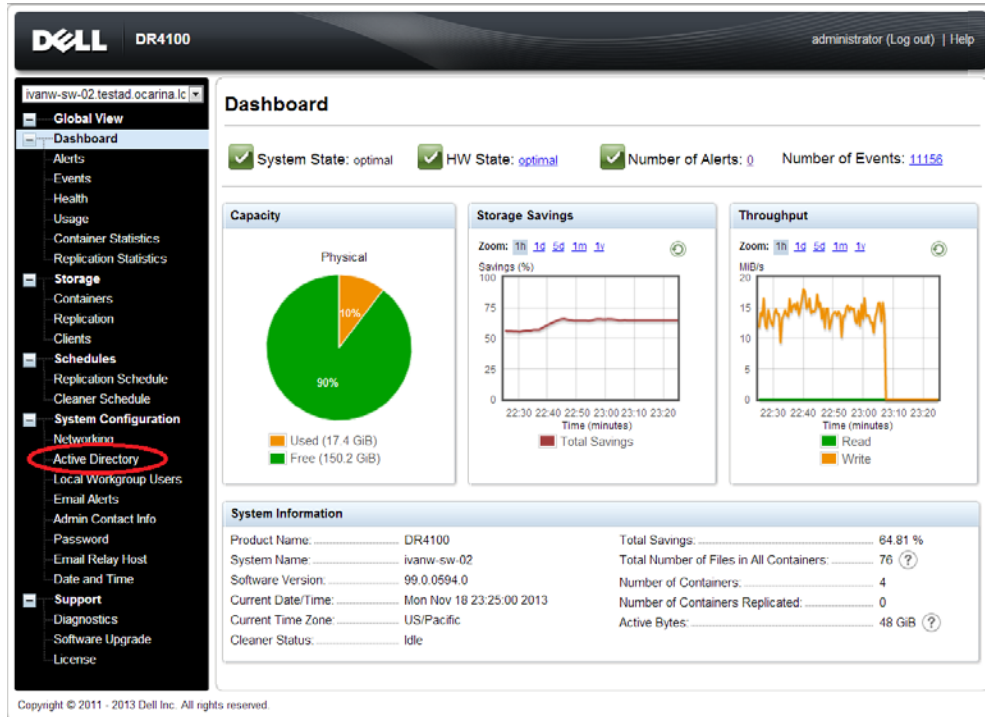


8. Log on to DR Series Deduplication Appliance administrator console, using the IP address you just provided for the DR Series Deduplication Appliance, with username **administrator** and password **St0r@ge!** (The "0" in the password is the numeral zero).

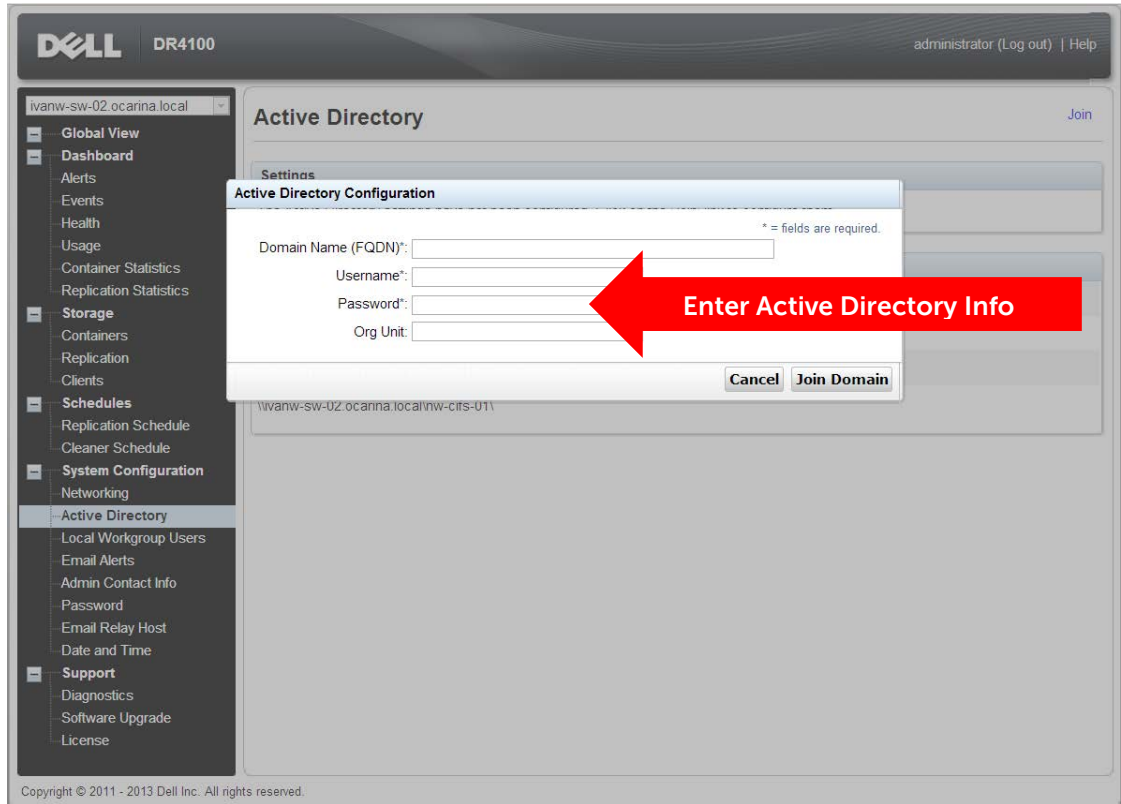


Note: if you do not want to add DR Series Deduplication Appliance to Active Directory, please see the *DR Series Deduplication Appliance Owner's Manual* for guest login instructions.

9. Join the DR into Active Directory domain.
 - Select **Active Directory** from the menu panel on the left side of the management interface.



- Enter your Active Directory credentials.



10. Create and mount the container. Select **Containers** in the tree on the left side of the dashboard, and then click the **Create** at the top of the page.

DELL DR4100 administrator (Log out) | Help

ivanw-sw-02.testad.ocarina.lc

Containers [Create](#) | [Delete](#) | [Display Statistics](#)

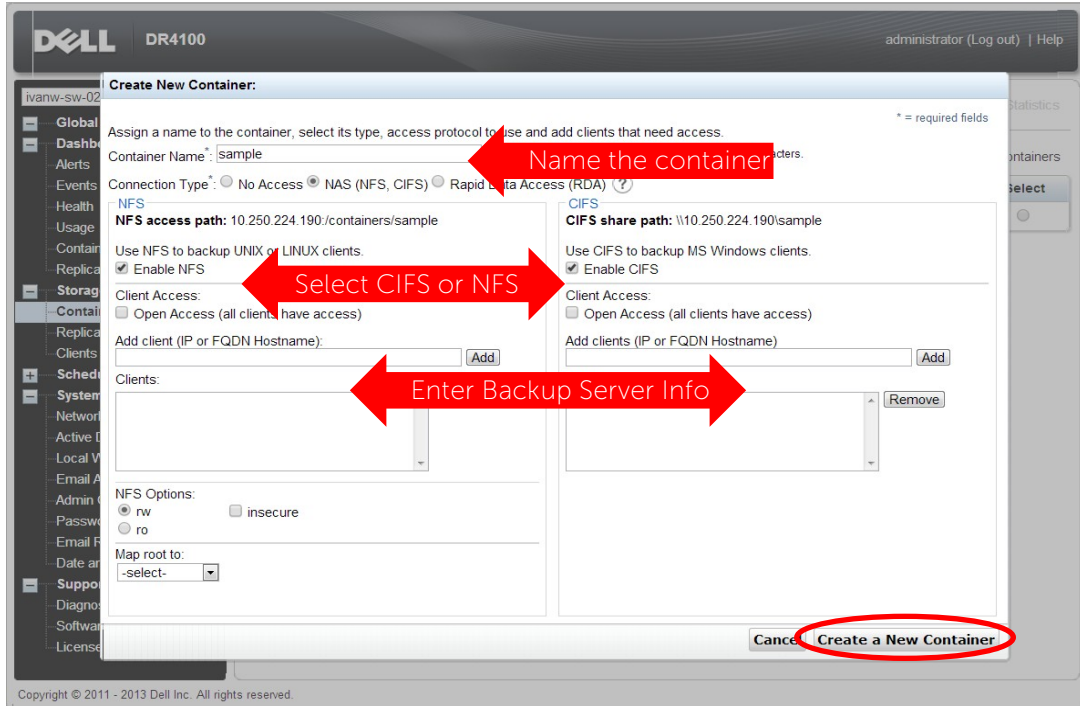
Number of Containers: 1 Container Path: /containers

Containers	Files	NFS	CIFS	RDA	Replication	Select
backup	2	✓	✓		Not Configured	

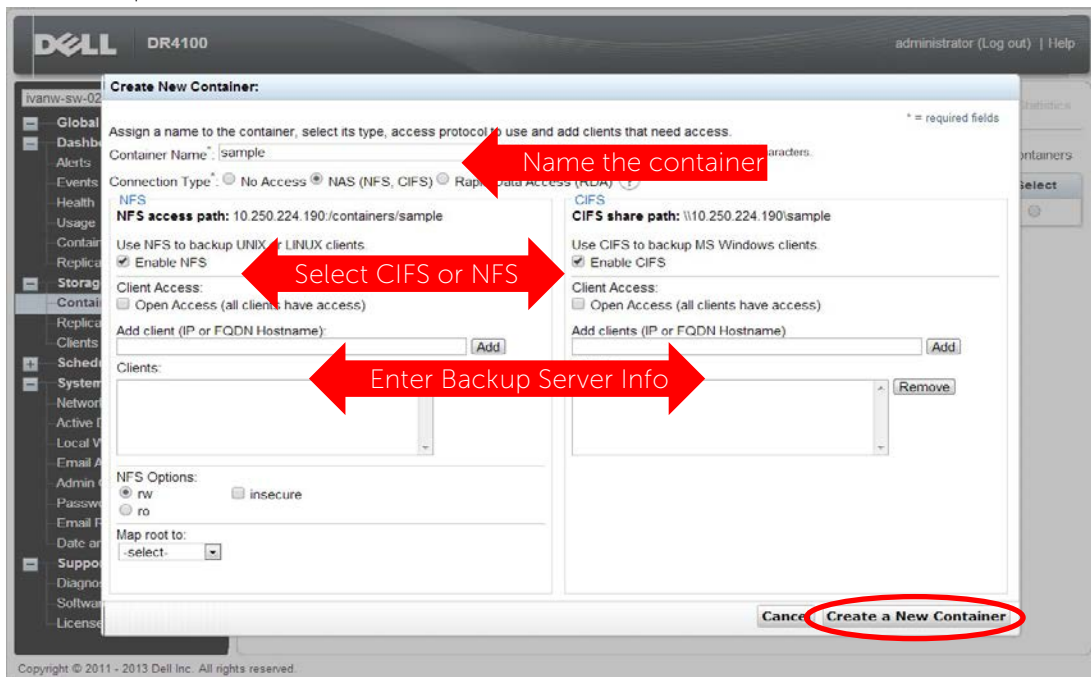
Copyright © 2011 - 2013 Dell Inc. All rights reserved.



11. Enter a **Container Name**, select the **Enable CIFS** or **Enable NFS** check box. Symantec NetBackup supports both CIFS and NFS protocols.



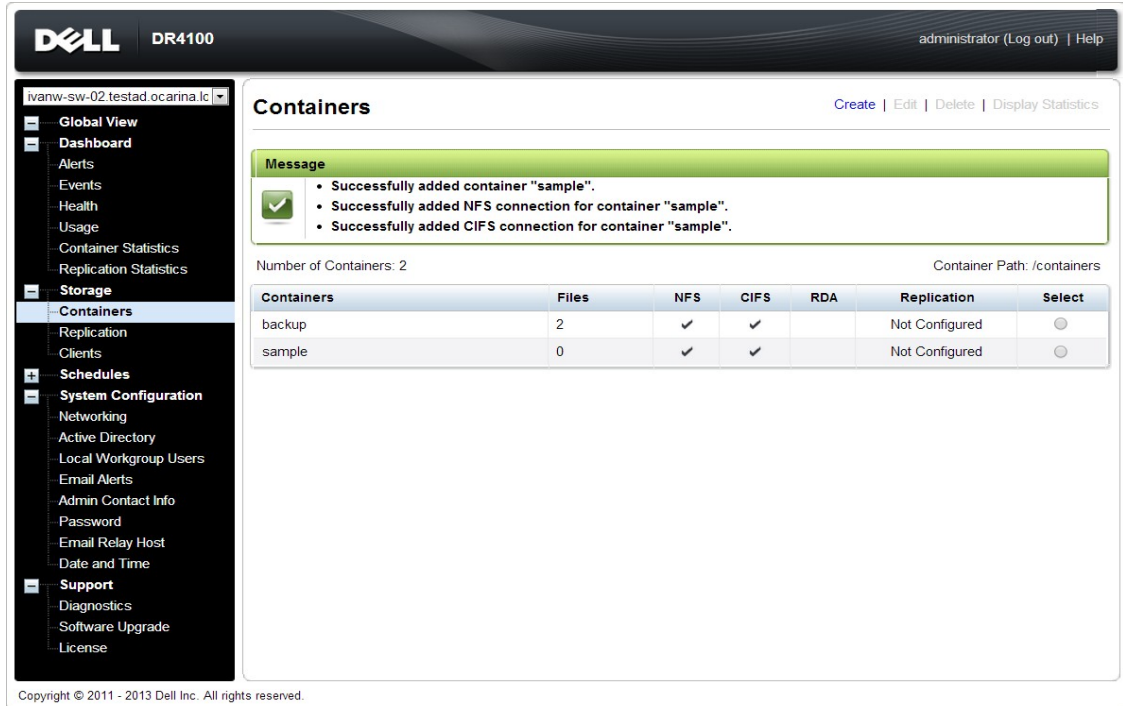
12. Select the preferred client access credentials.



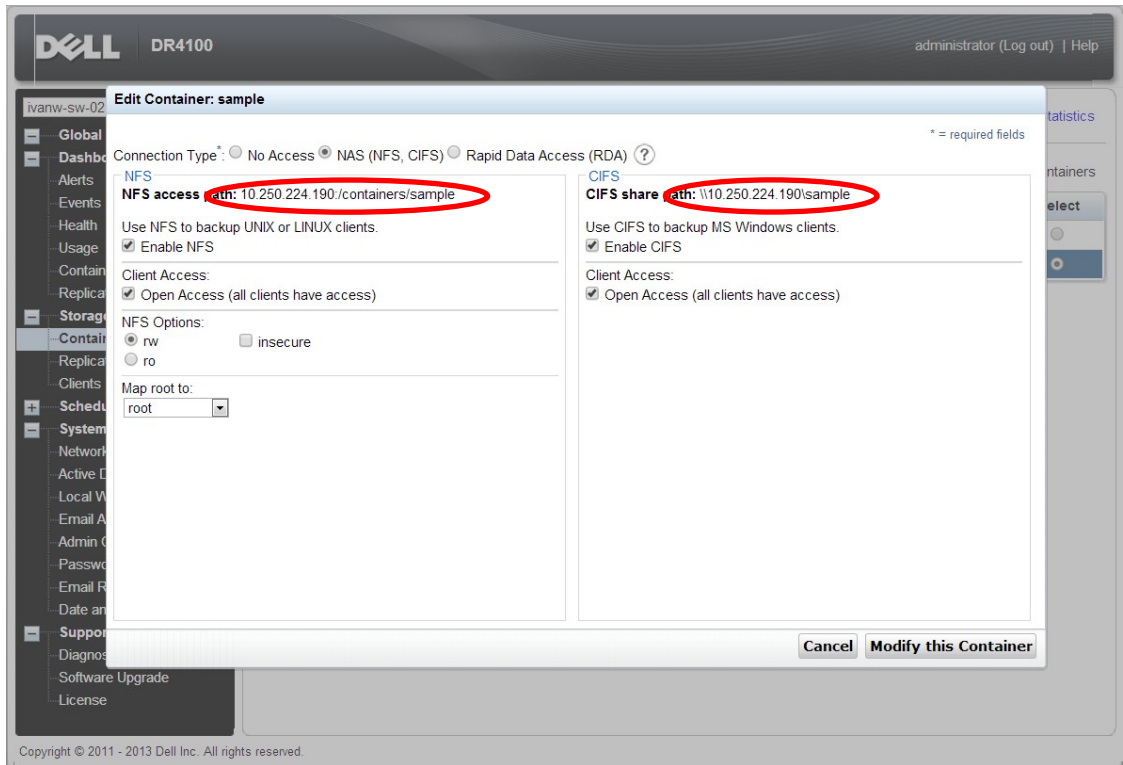
Note: For improved security, Dell recommends adding IP addresses for the following (Not all environments will have all components): Backup console (CommVault Server, CommVault Media Agents)



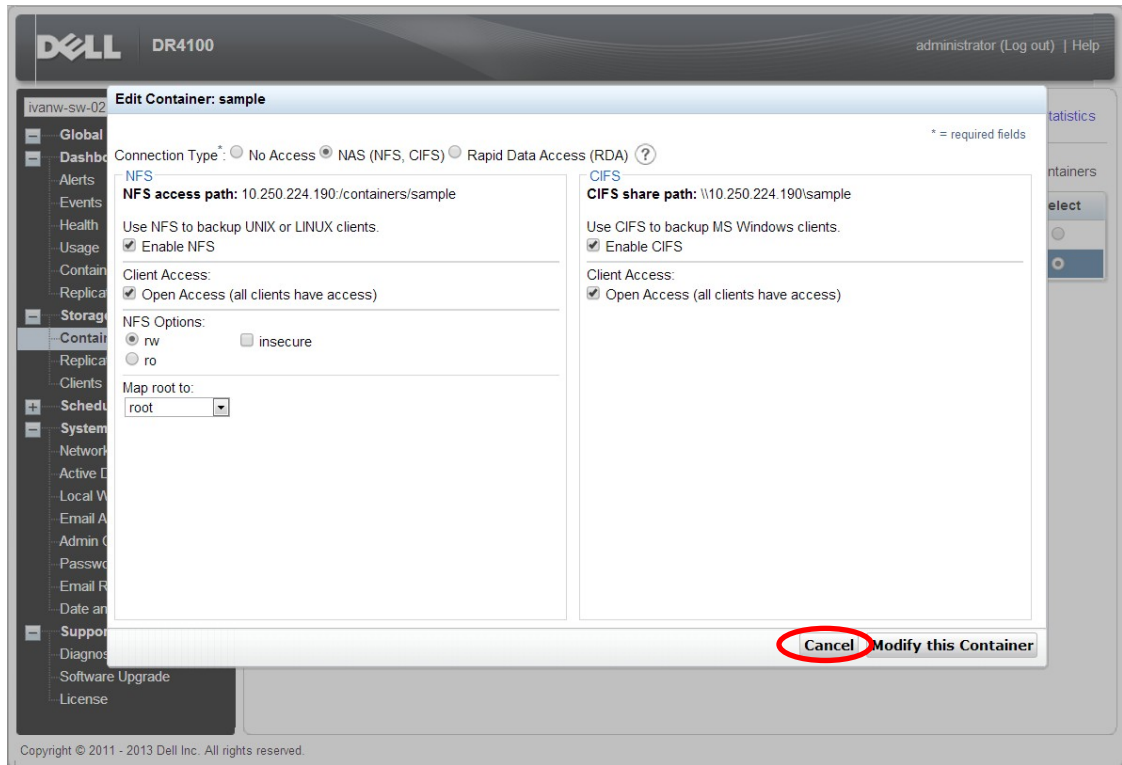
- Click **Create a New Container**. Confirm that the container is added.



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



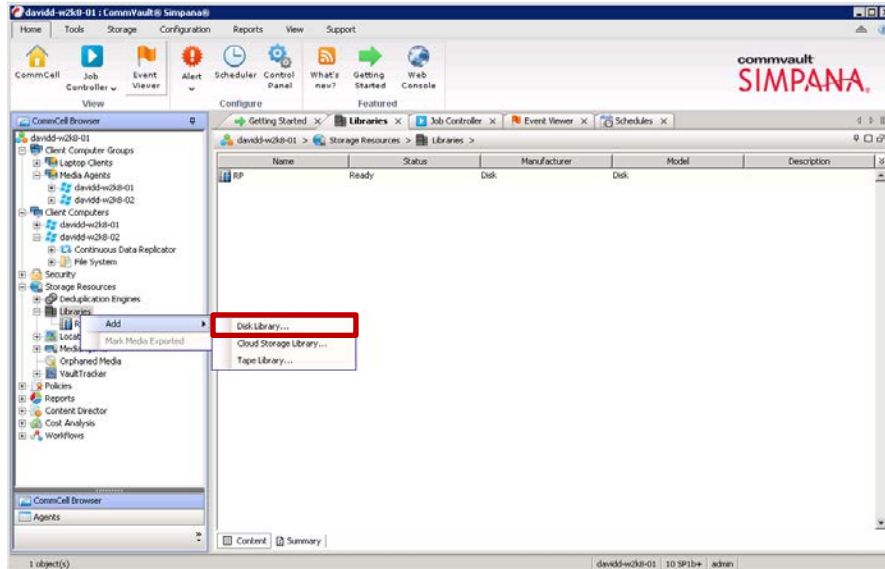
15. Click **Cancel** to exit.



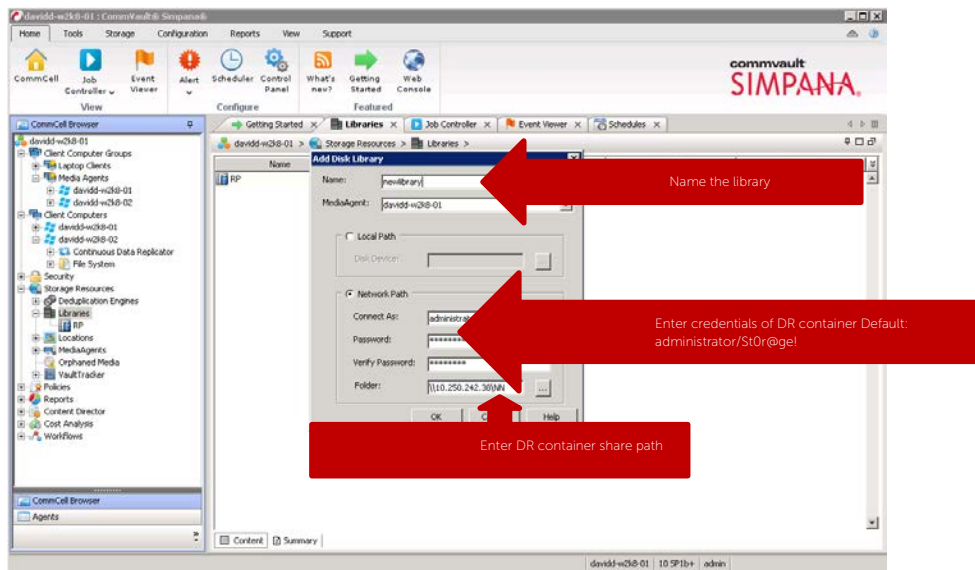
2 Set up CommVault Simpana 10

2.1 Single System Environment (DR as CIFS Disk Library)

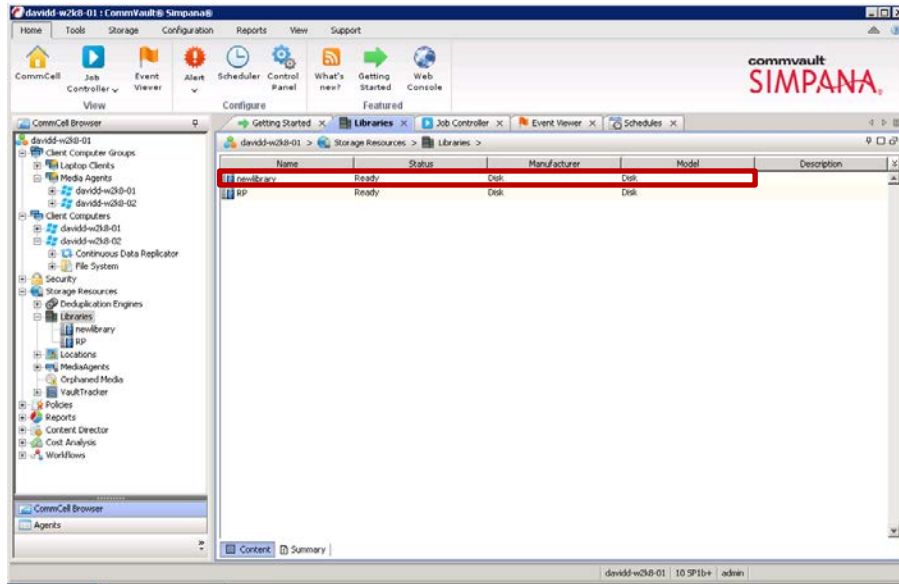
1. Open **Simpana Administrative Console**, expand **Storage Resources**, right-click on **Libraries**, select **Add** -> **DiskLibrary...**



2. In **Add Disk Library** window, enter the name for the Disk Library and the information of DR container, and Click **OK**.



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

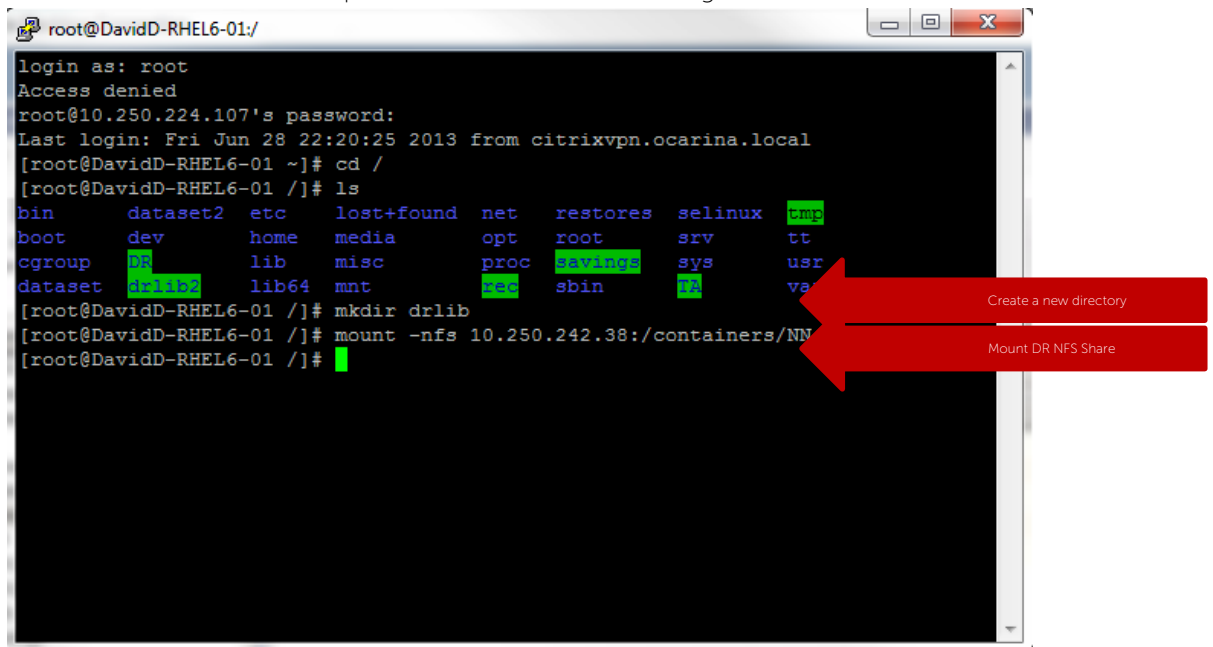


- 4.

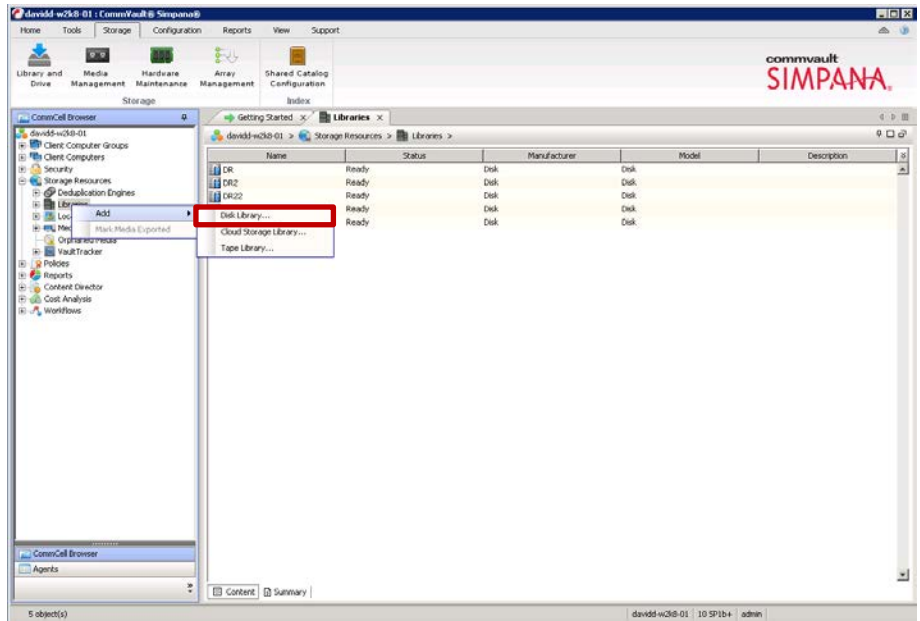


2.2 Single System Environment (DR as NFS Disk Library)

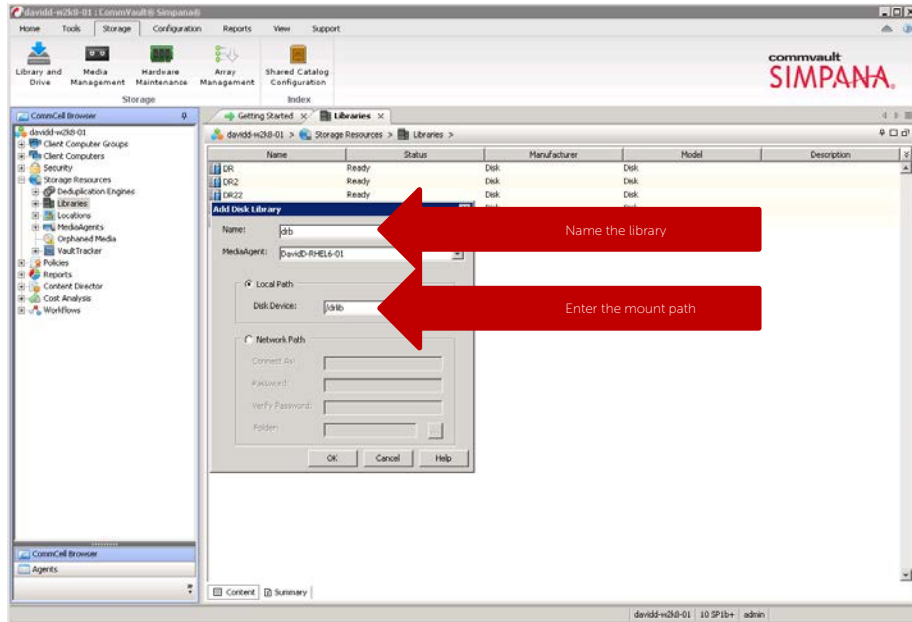
1. Mount DR container NFS export onto Unix/Linux Media Agent.



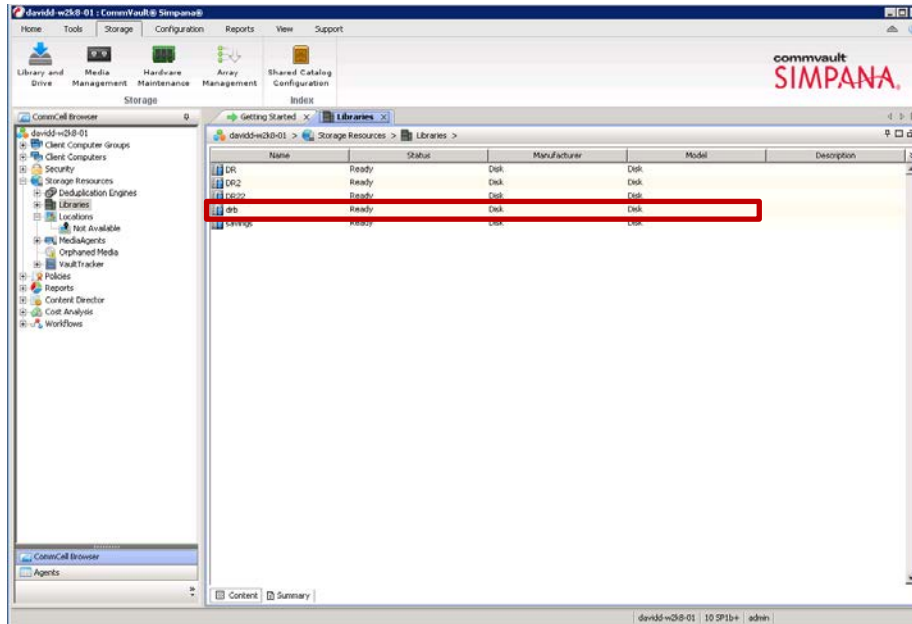
2. Open **Simpana Administrative Console**, expand **Storage Resources**, right-click on **Libraries**, and Select **Add -> DiskLibrary...**



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



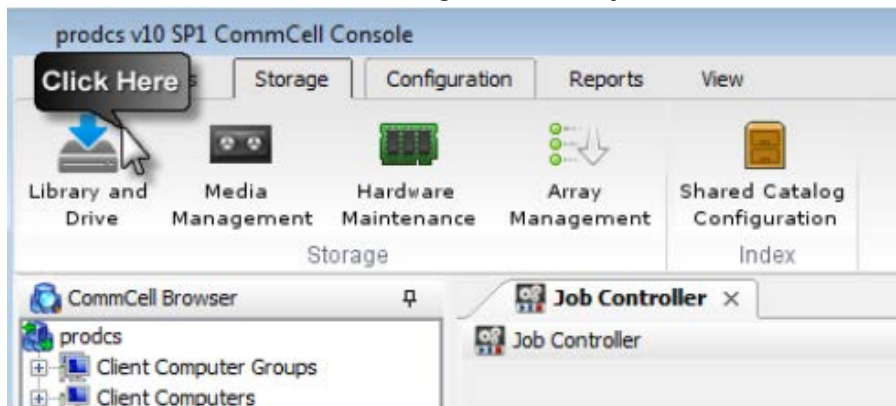
4. Confirm that the library is created, its **Status** is **Ready**.



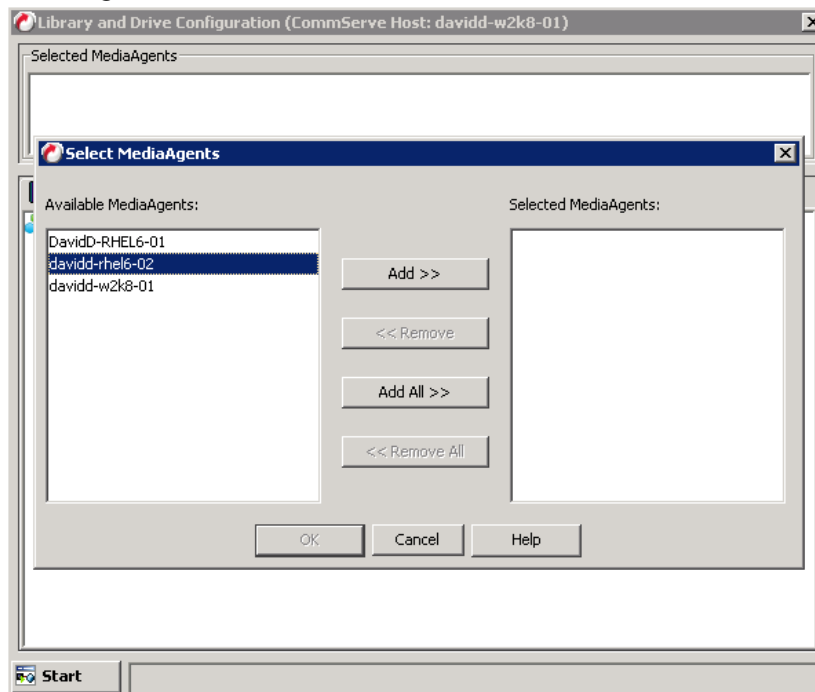
2.3 Replicated System Environment

NOTE: The replicated system environment includes minimum of 2 DR systems that are connected to 2 different Media Agents. CommVault manages data replication between the replication pair. For more details, please refer to CommVault books online : http://documentation.commvault.com/commvault/release_10_0_0/books_online_1/english_us/prod_info/flr.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**.

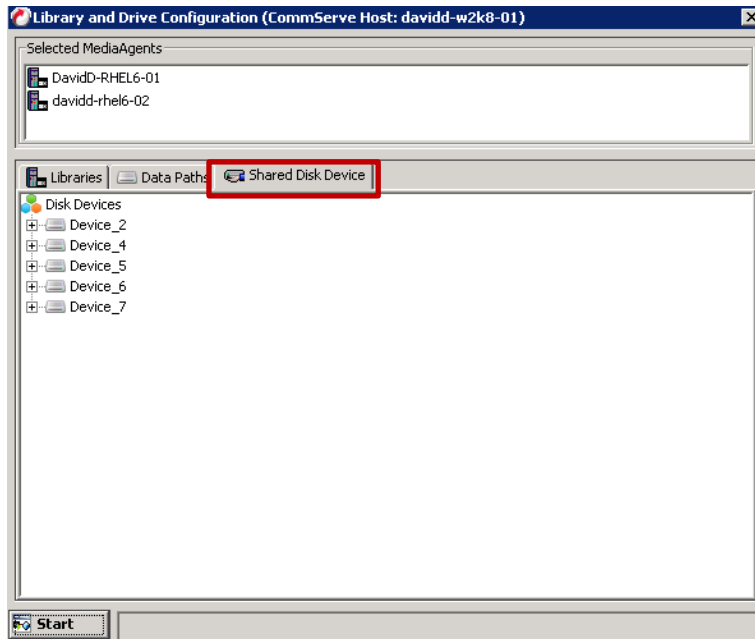


Note: To configure any shared library, make sure you select all the MediaAgents that share that library.

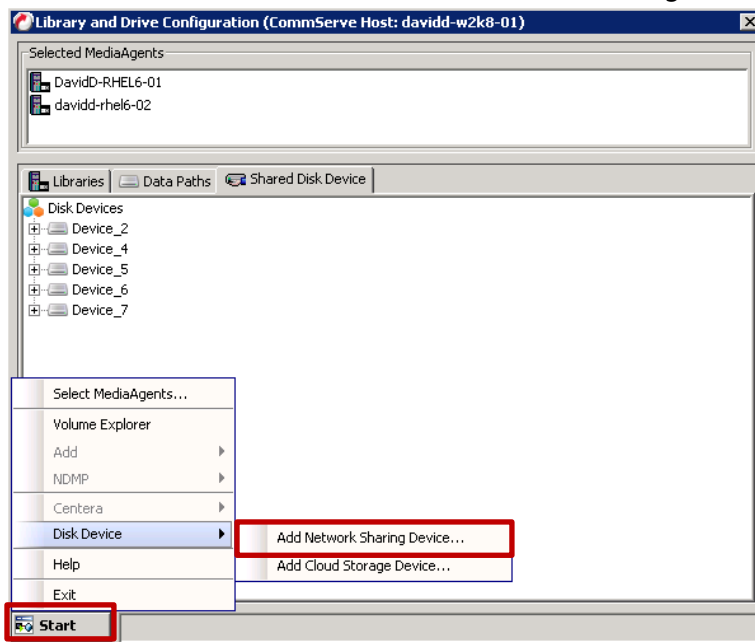
3. Click **OK** to continue.



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



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



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

Add Sharing Folder

Device Name: SharingDevice#

MediaAgent: DavidD-RHEL6-01

Sharing Folder Properties

Local Path

Folder: []

Network Path

Connect As: []

Password: []

Verify Password: []

Folder: []

Preferred

Read Only

OK Cancel Help

Select the name of MediaAgent accessing this mount path

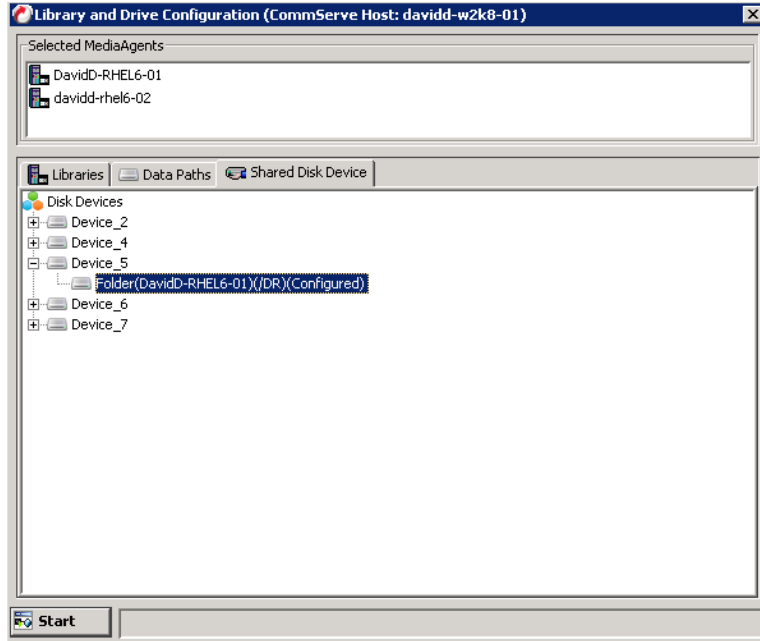
Linux MediaAgent can only select local path

Windows MediaAgent can select both local and network path

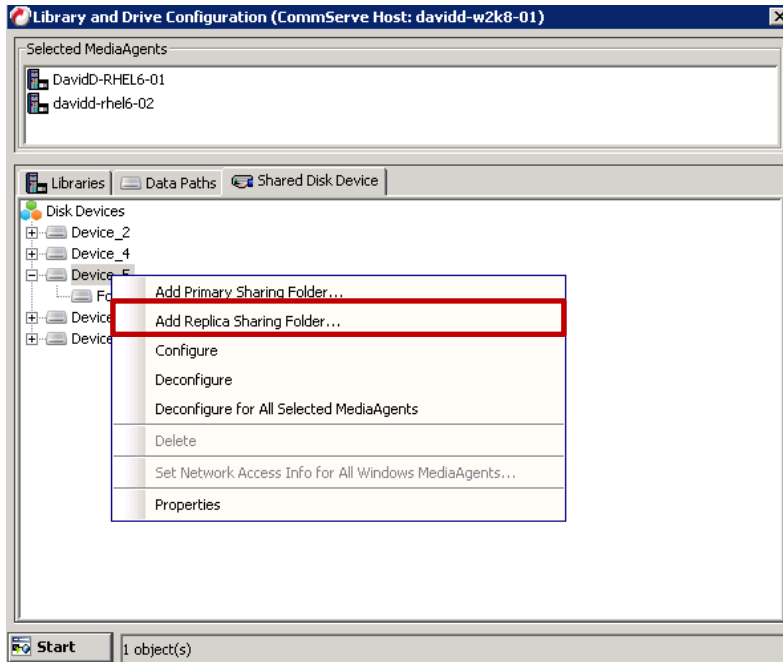
Note: This Device is replication source. Device information is based on which protocol the container is exposed to the MediaAgents.



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 **Add Sharing Folder** dialog box, enter target DR container share/export information and then Click **OK**.

The screenshot shows the 'Add Sharing Folder' dialog box. The 'Device Name' is 'Device_5' and the 'MediaAgent' is 'davidd-rhel6-02'. Under 'Sharing Folder Properties', the 'Local Path' radio button is selected. The 'Folder' field is empty with a browse button. The 'Network Path' section is unselected and contains fields for 'Connect As:', 'Password:', 'Verify Password:', and 'Folder:'. At the bottom, the 'Preferred' checkbox is unchecked and the 'Read Only' checkbox is checked. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

Select the name of MediaAgent accessing this mount path

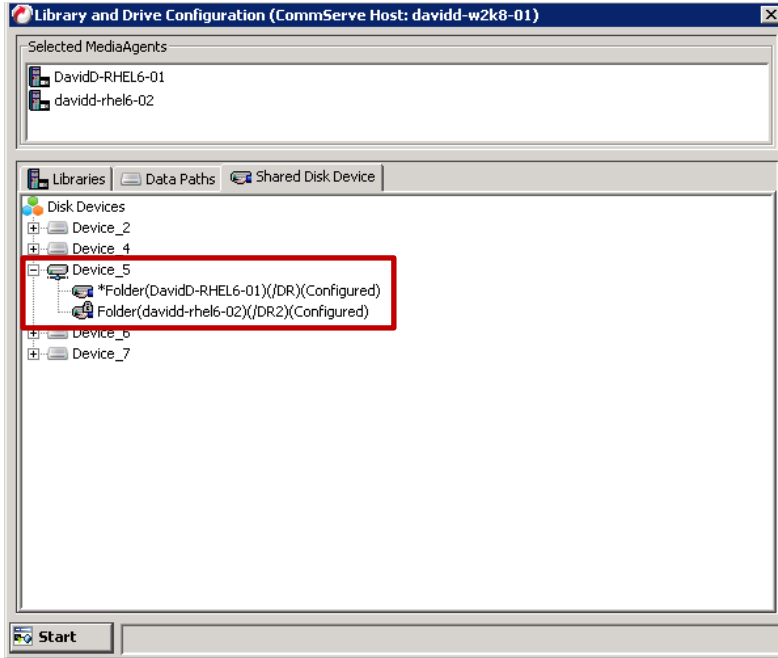
Linux MediaAgent can only select local path

Windows MediaAgent can select both local and network path

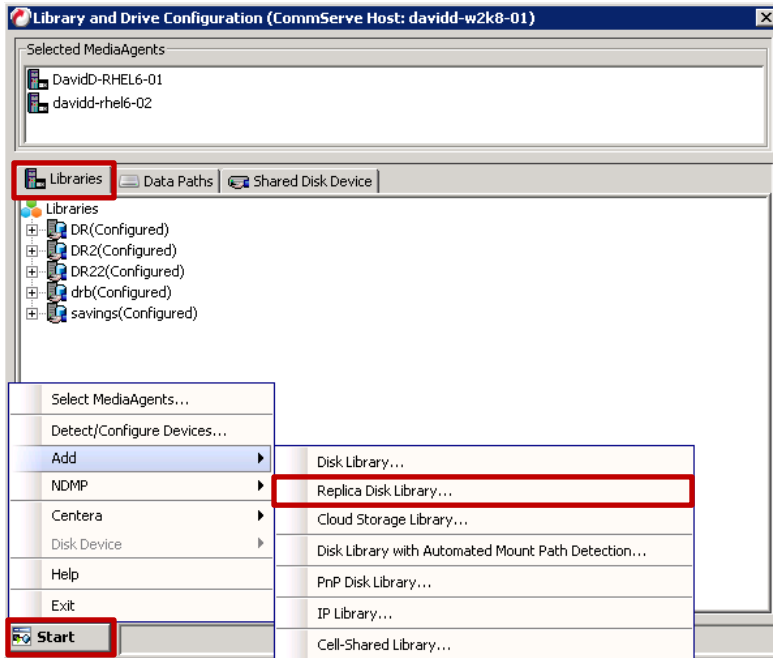
Note: This Device is the destination of replication. Device information is based on which protocol the container is exposed to the MediaAgents.



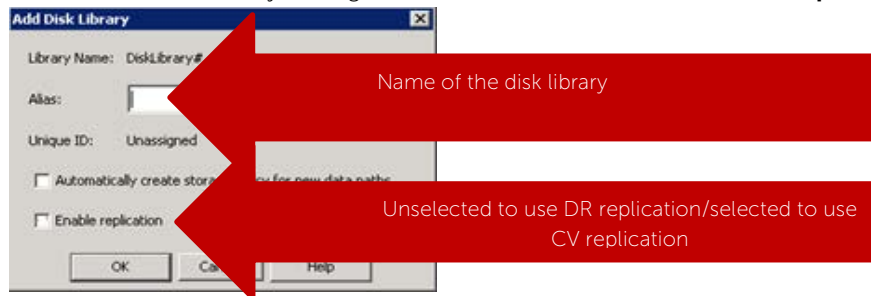
10. The system displays the device information with which MediaAgent can access the device in **Library and Drive Configuration** window.



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



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

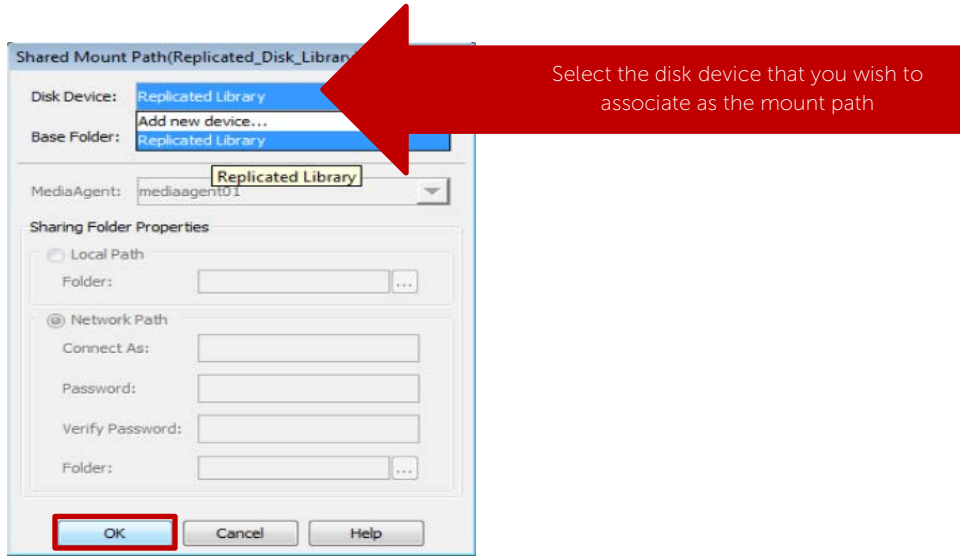


NOTE:

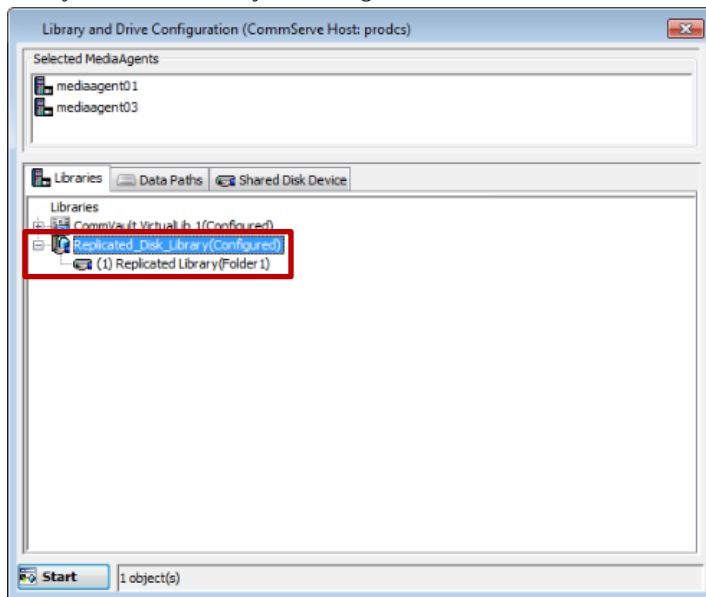
Enable Replication:

- For 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 don't want CommVault to manage replication between the two DRs.
- 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**.
- If this option is not selected, use DR native replication between two separate disk libraries. There may exist issues when CommVault tries to restore from the target DR disk library, because CommVault doesn't have catalog information for that disk library.

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



14. Verify the disk Library is configured.



2.4 Use Continuous Data Replicator to replicate client data to a DR container

NOTE:

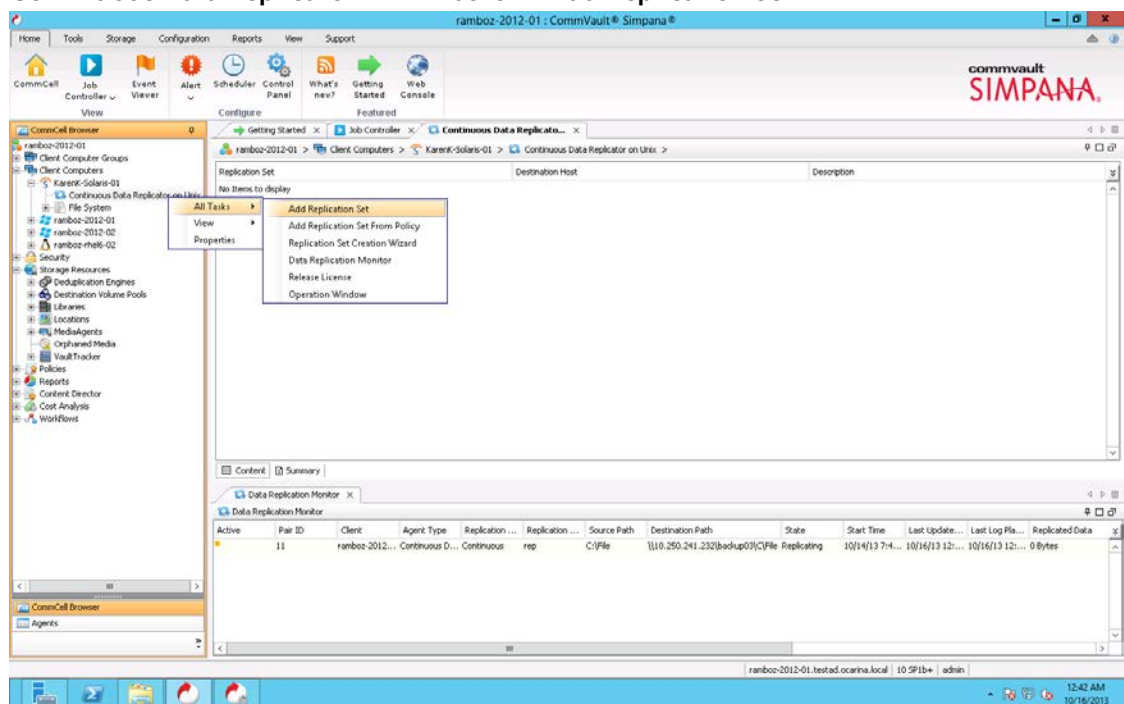
ContinuousDataReplicator (CDR) replicates data from a source computer to a destination computer, with both computers support same network transfer protocol.

In this configuration, CDR replicates between a client and a DR container. CDR package should be installed on both media agents associated with this configuration.

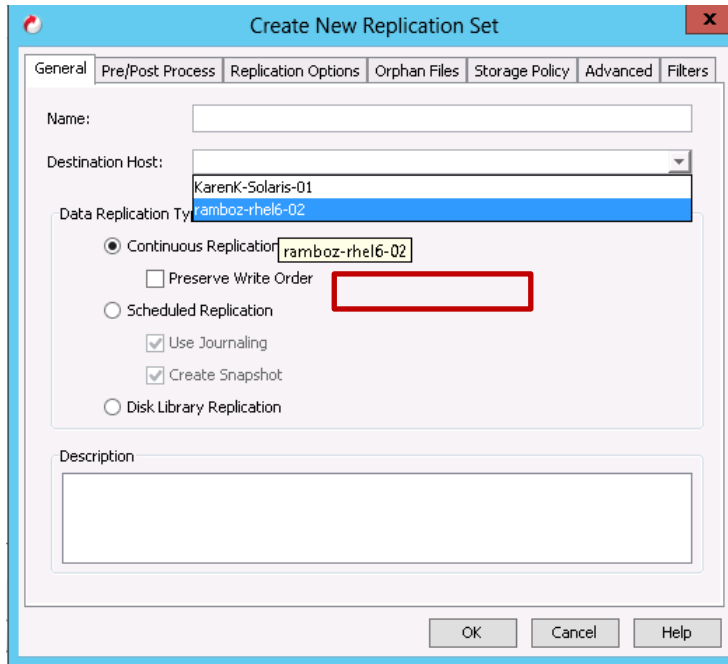
For more details, please refer to Commvault books online :

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

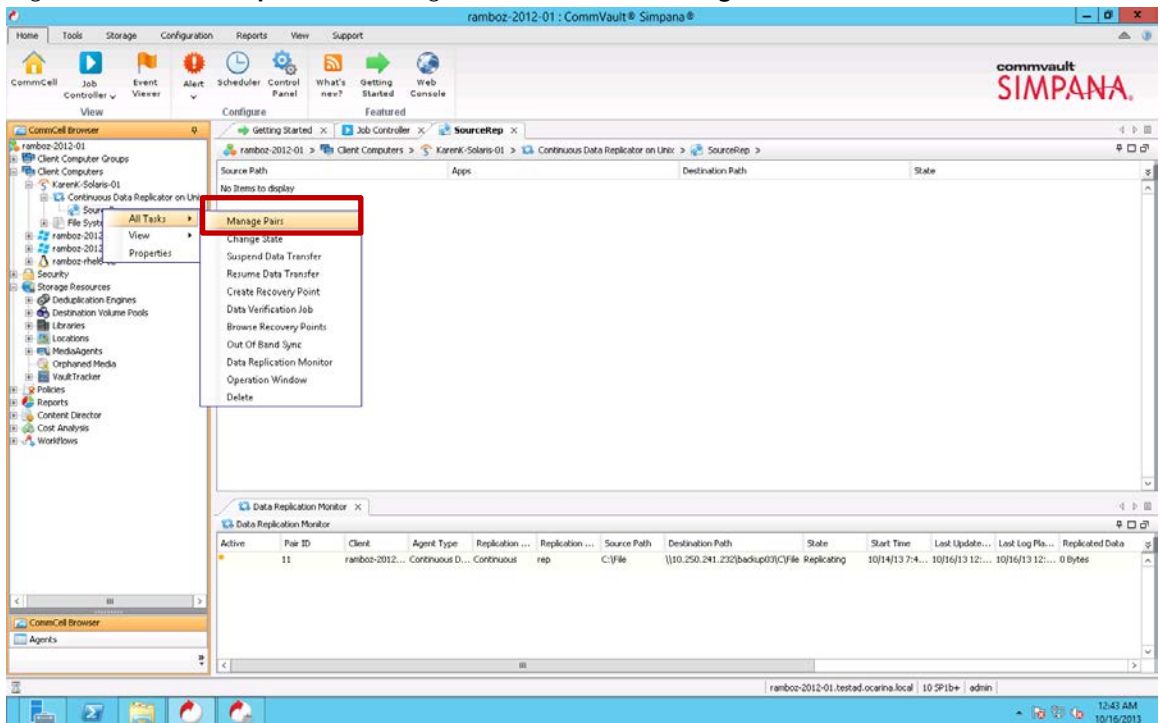
1. From **CommCell Console**, pick the client that a dataset needs to be replicated to DR. Right click **Continuous Data Replicator -> All Tasks -> Add Replication Set**.



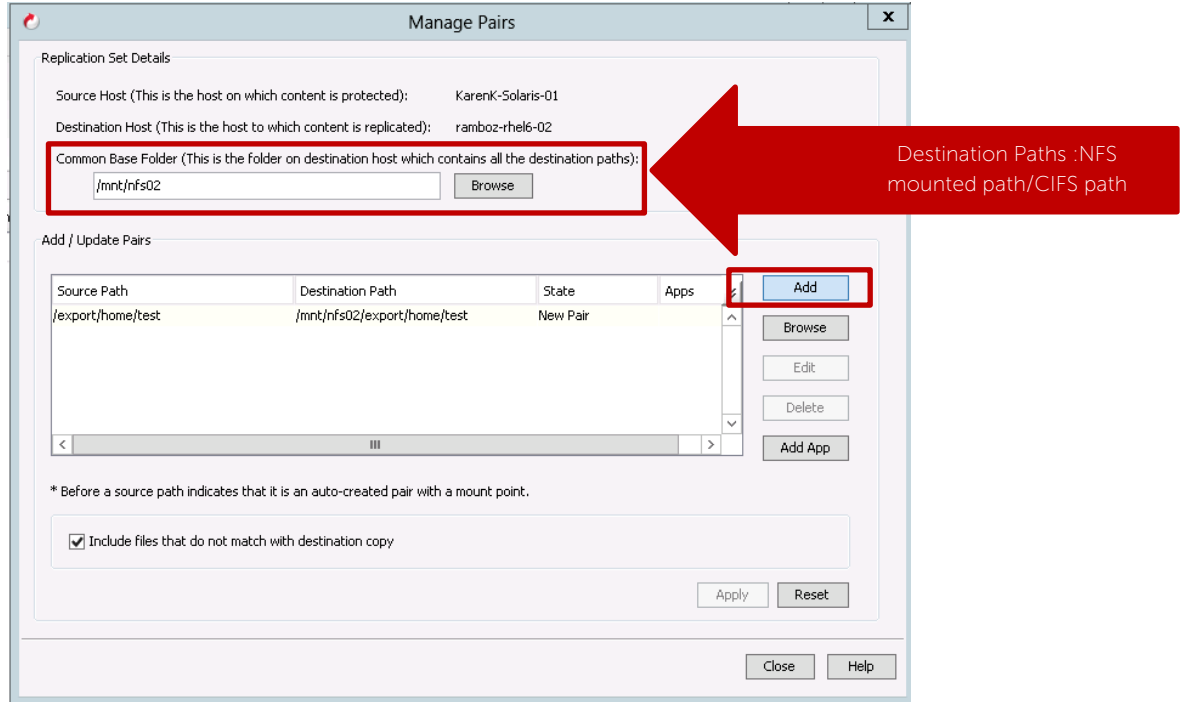
- In **Create New Replication Set** window, Enter **Name** for the Replication Set, select **Destination Host** from dropdown list. That's the client machine that has DR container mounted (CIFS or NFS). Click **OK**.



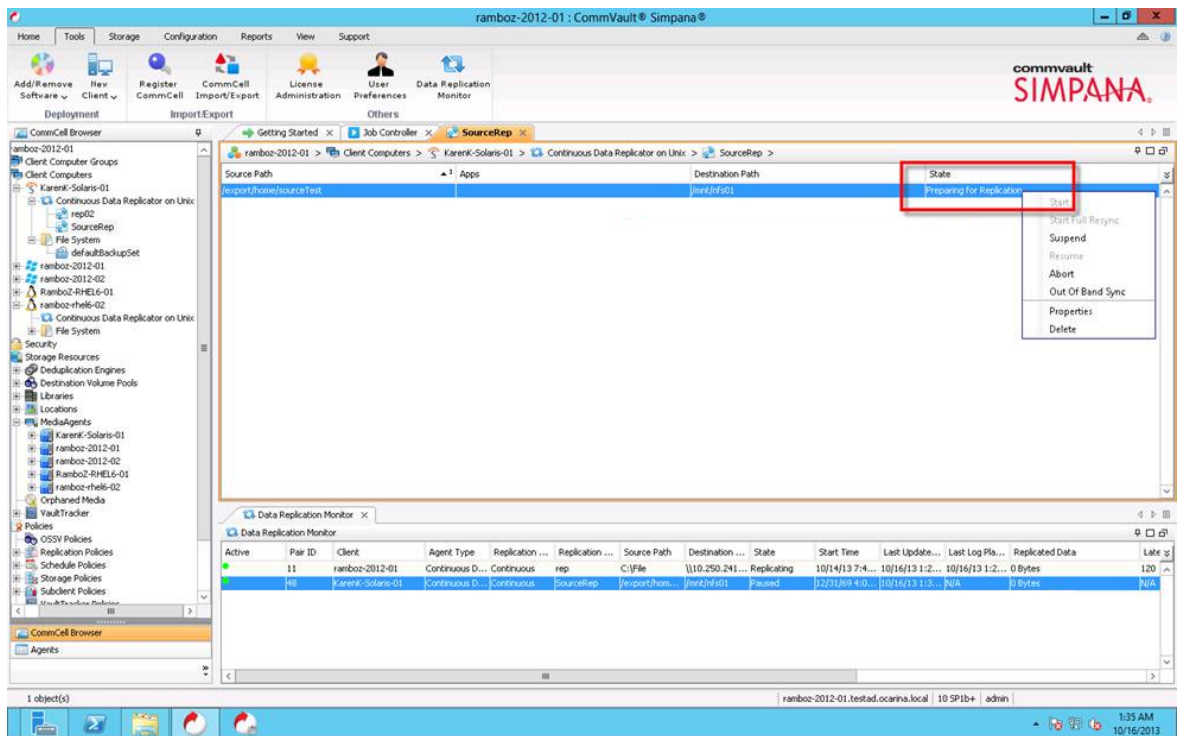
- Right click on the **Replication Set**, go to **All Tasks -> Manage Pairs**



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

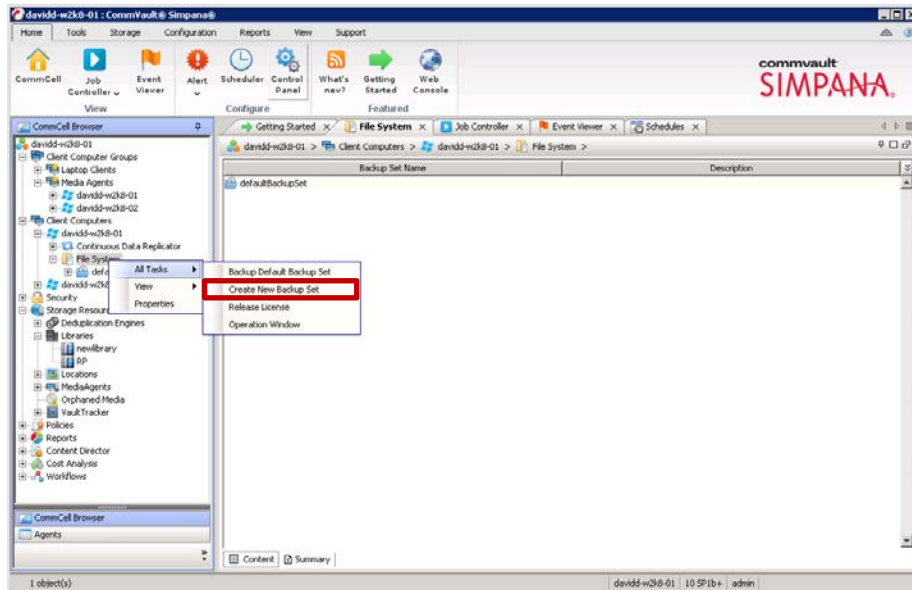


- Right click on the managed pairs under the replication set. Choose **Start/Start Full Resync**. Monitor the **State**.

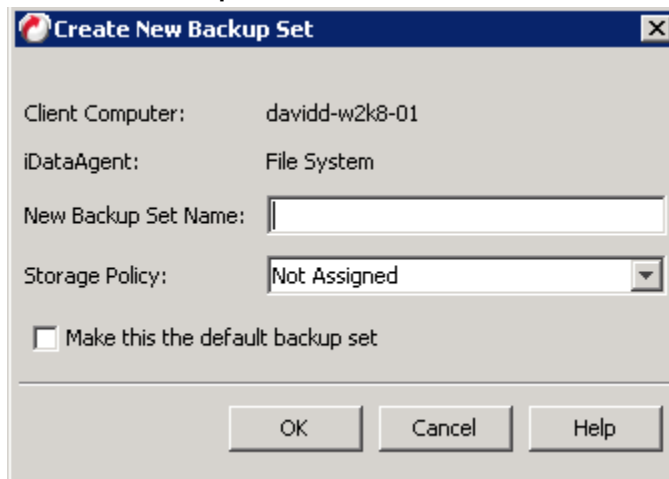


2.5 Create backup job with DR Series Deduplication Appliance as the target

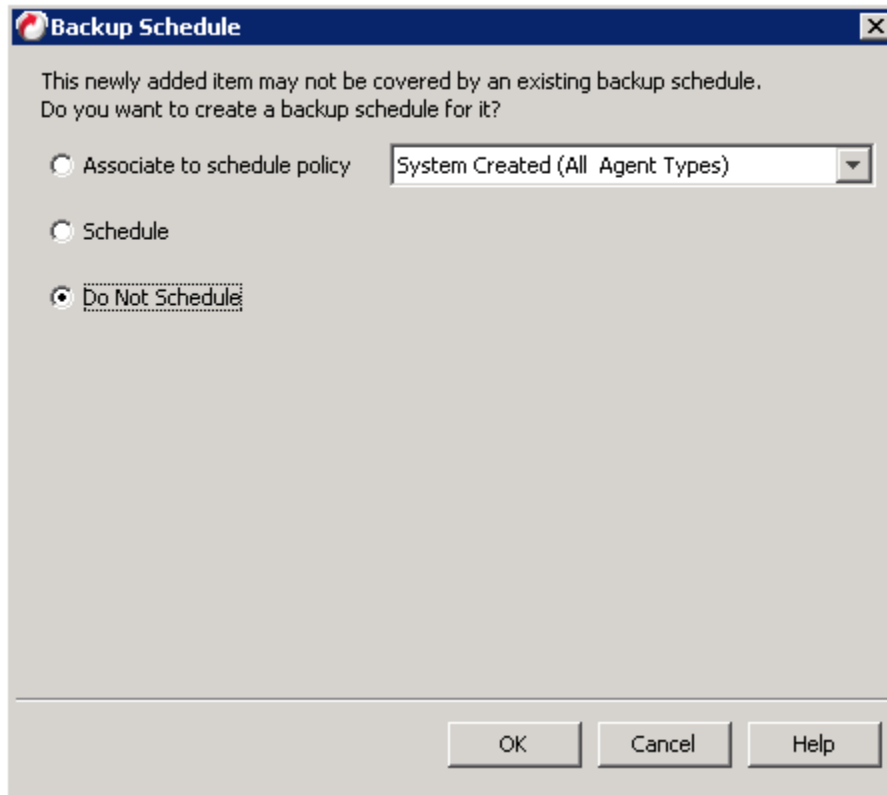
1. Expand the client to be backed up, right-click the target iDataAgent, select **All Tasks** –> **Create New Backup Set**



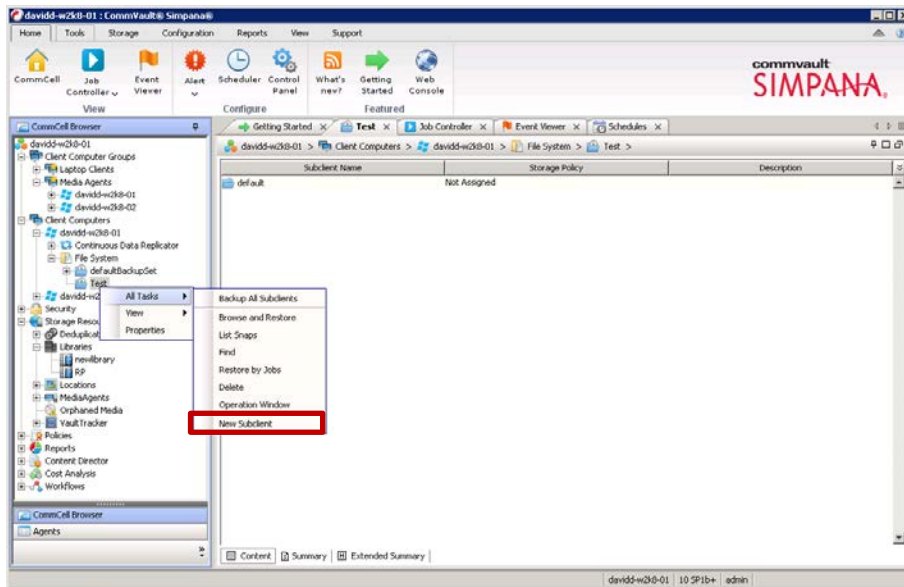
2. Enter **New Backup Set Name**.



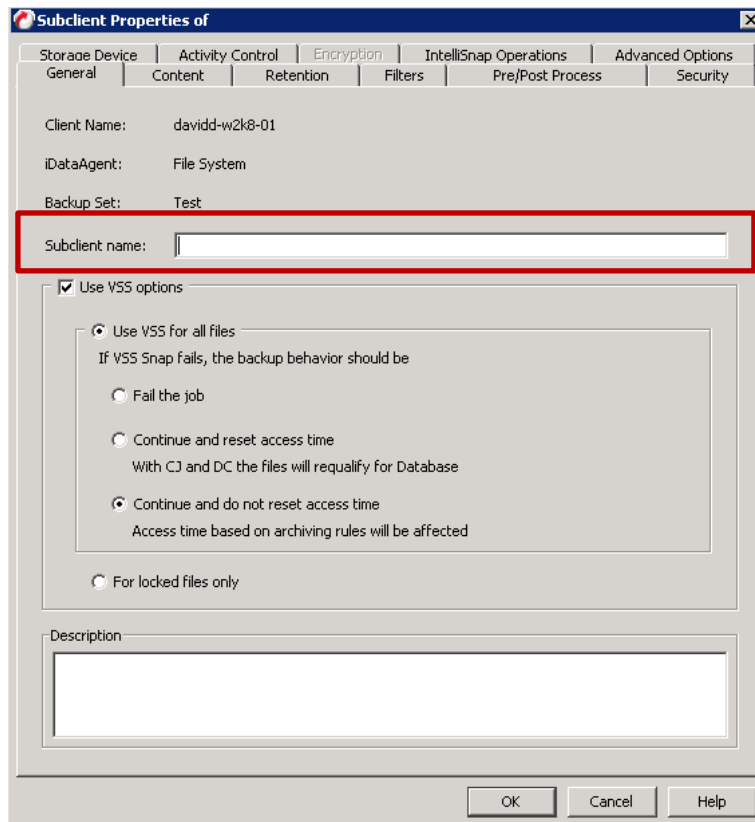
3. Set appropriate **Backup Schedule**



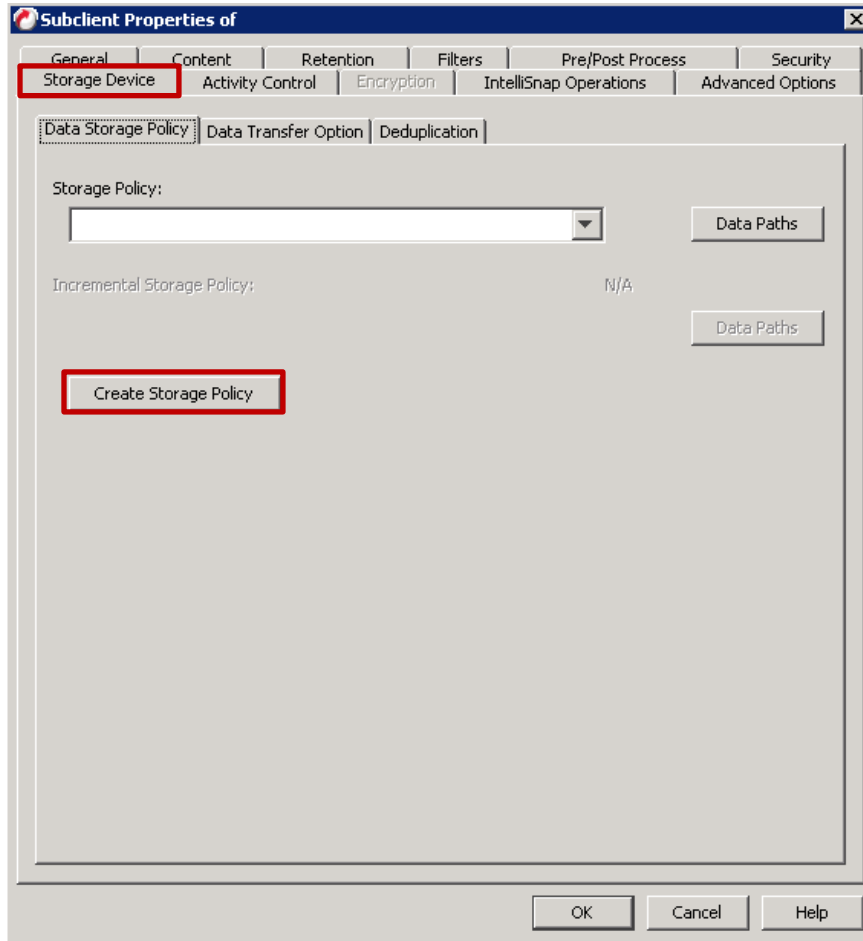
4. Right-Click on the newly created Backup Set, select **All Tasks -> New Subclient**



5. Enter **Subclient name** on **General** tab.

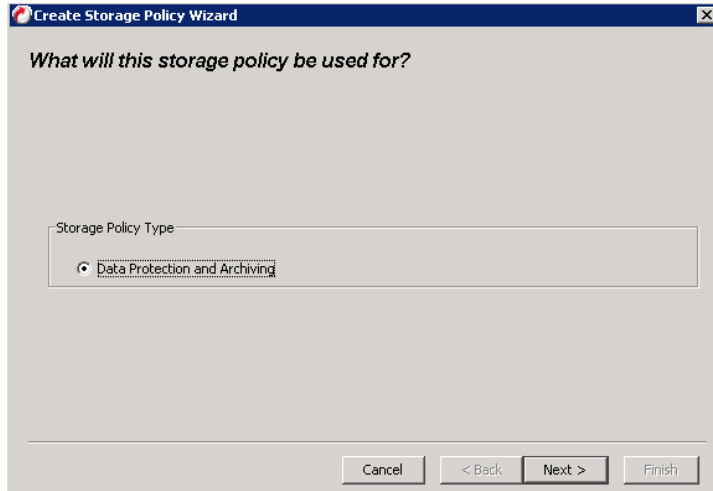


6. Select **Storage Device** tab, click **Create Storage Policy**



7. In **Create Storage Policy Wizard**

- Select Policy Type: Data Protection and Archiving



- Enter **Storage Policy Name**

Create Storage Policy Wizard

Enter the storage policy name

Storage Policy Name:

Incremental Storage Policy

Provide the DataFabric Manager Server Information

Cancel < Back Next > Finish

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

Create Storage Policy Wizard

Select a default library for this primary copy

Library:

Cancel < Back Next > Finish

- Select **MediaAgent**

Create Storage Policy Wizard

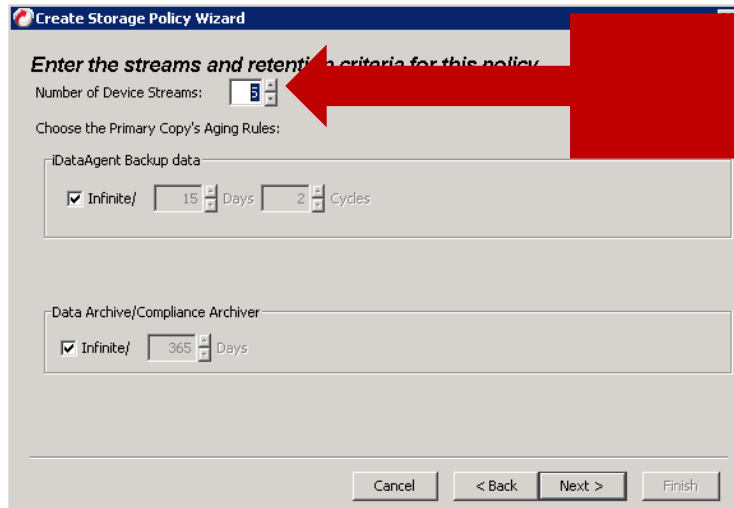
Select a MediaAgent for this copy

MediaAgent:

Cancel < Back Next > Finish

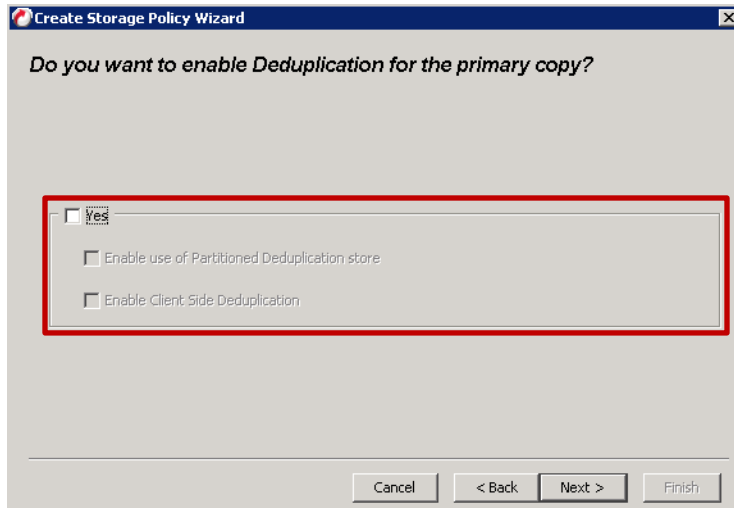


- Enter **Number of Device Streams** and retention policy



Max is 32. If each client can write backup data close to 100MB/s, this number can be set as 5 for current DR firmwersions.

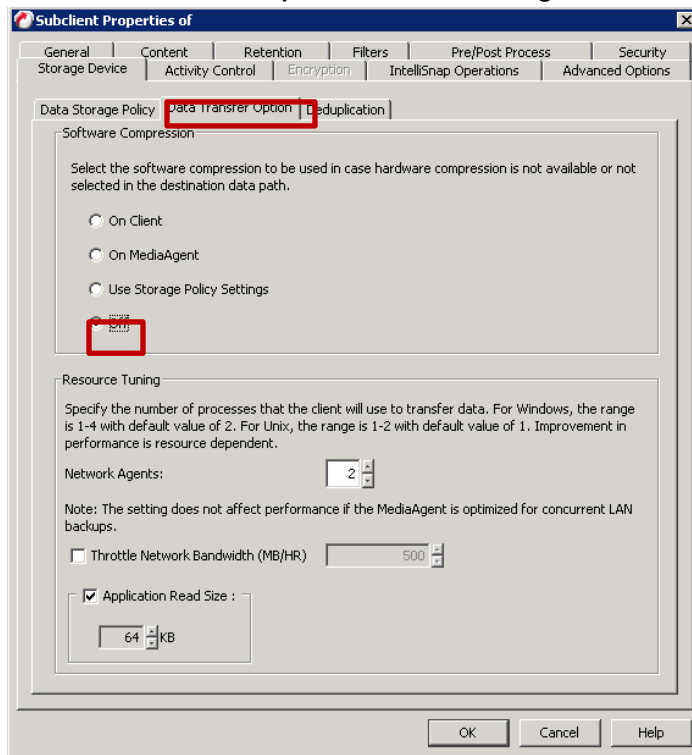
- **Disable** deduplication for the primary copy



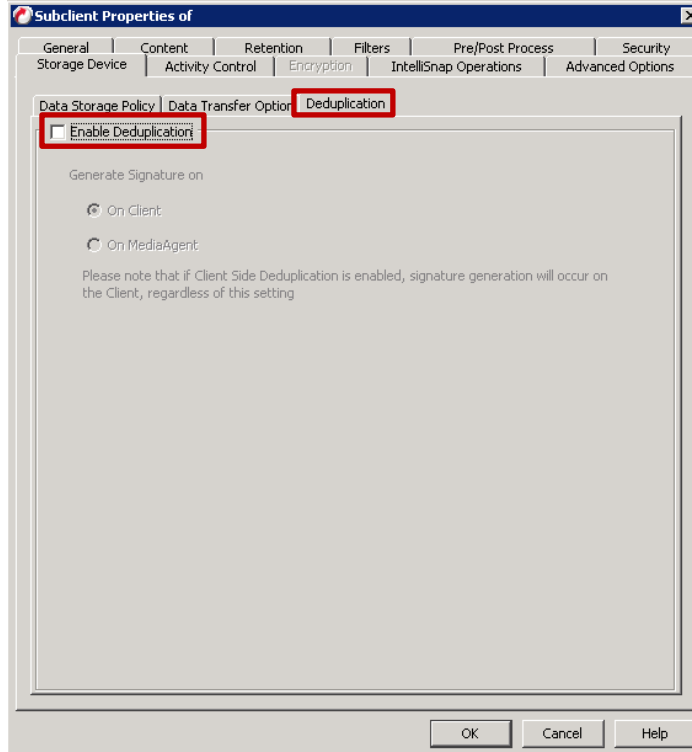
- Finish



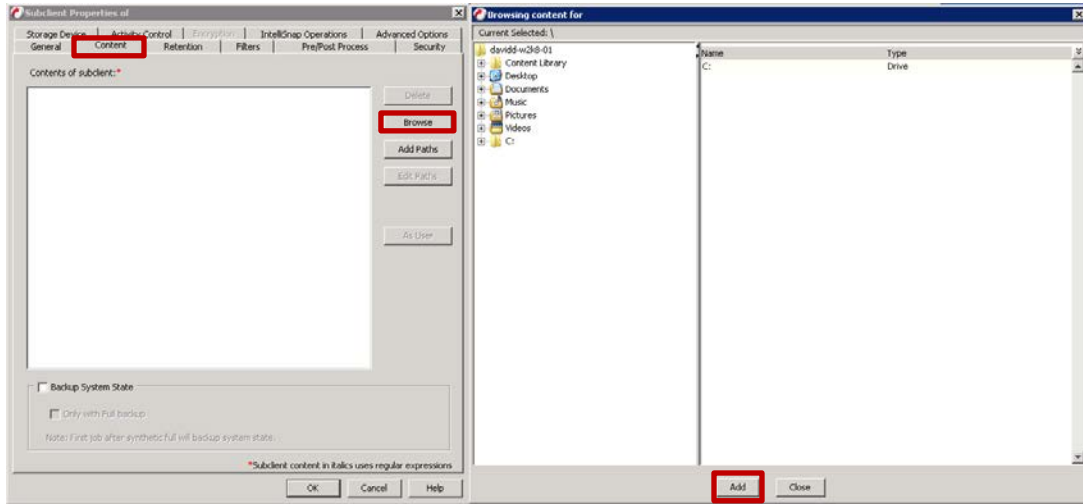
8. Disable **Software Compression** under **Storage Device** -> **Data Transfer Option**



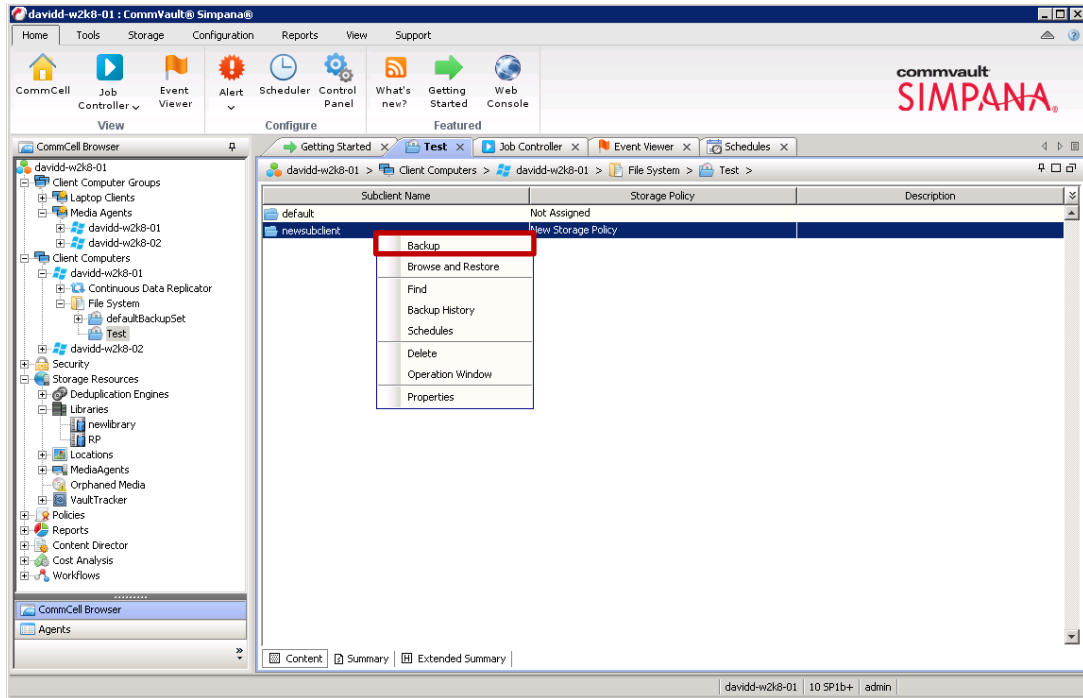
9. **Uncheck Enable Deduplication** under **Storage Device** -> **Deduplication**



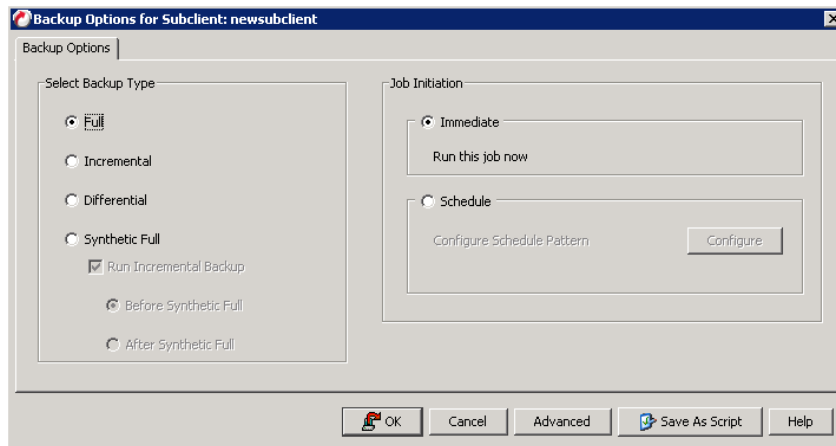
10. Under **Content** tab, select data for backup by clicking **Browse**.



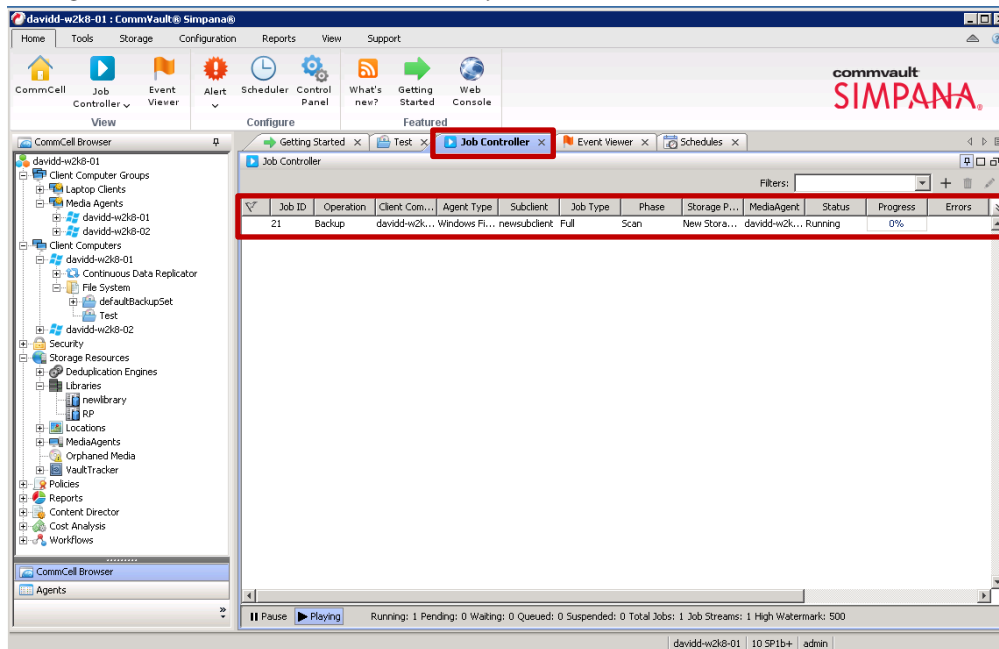
11. Right-click the newly created subclient, and select **Backup**



12. Make selection under **Select Backup Type** and Click **OK**.



13. Navigate to **Job Controller** to monitor job **Status**



3 Set Up the DR Series Deduplication Appliance Cleaner

The cleaner will run 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 which will force it to run during that scheduled time.

If necessary you can do the following procedure described in the screenshot to force the cleaner to run. Once all the backup jobs are setup the DR4x00 cleaner can be scheduled. The DR Series Deduplication Appliance cleaner should run at least 6 hours per week when backups are not taking place, generally after a backup job has completed.

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 screenshot shows the Dell DR4100 web interface. The header includes the Dell logo, system ID 'DR4100 EdwinZ-SW-01', and 'Help | Log out' links. The sidebar menu on the left has 'Cleaner Schedule' highlighted with a red box. The main content area is titled 'Cleaner Schedule' and shows the system time zone as 'US/Pacific, Fri Jul 5 05:00:41 2013'. A note states: 'Note: When no schedule is set, the cleaner will run as needed.' Below this is a table with columns 'Day', 'Start Time', and 'Stop Time'. All cells in the table are empty, indicating no schedule is currently set. A red arrow labeled 'Schedule Cleaner' points to the 'Edit Schedule' button in the top right corner of the main content area.

Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--



4 Monitoring Deduplication, Compression and Performance

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

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 complete, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio in most cases.

