Setting up Dell™ DR Series Deduplication Appliance on Dell vRanger Pro

Dell Engineering
January 2014

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release

Table of contents

Executive Summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for vRanger Pro® Backup & Replication software. 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 other data management application best practices whitepapers for additional information.

NOTE: The DR Series Deduplication Appliance/vRanger build version and screen shots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/vRanger 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**".
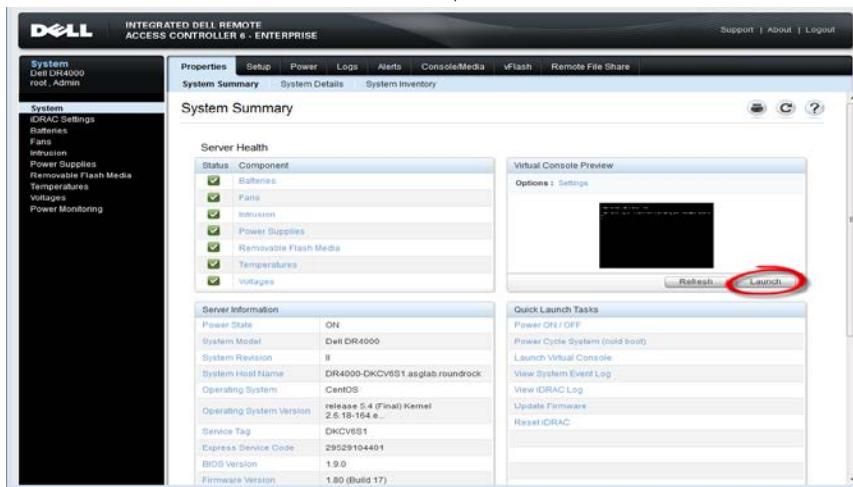
4. Launch the virtual console.
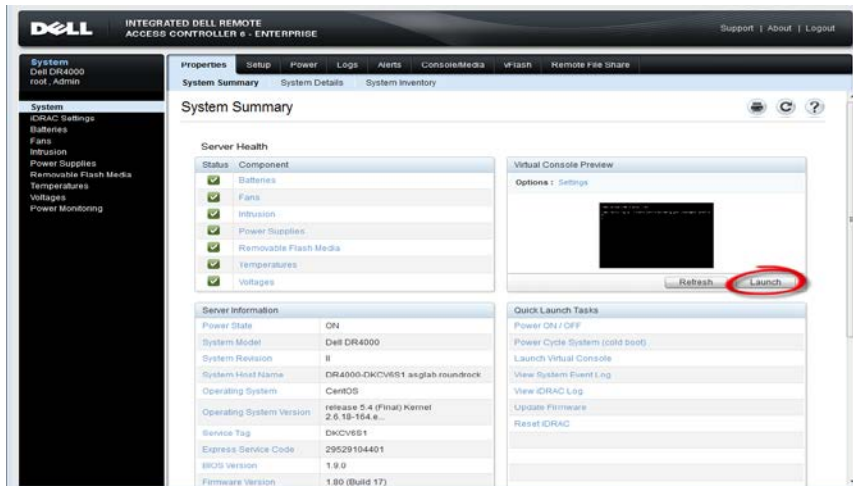
5. After the virtual console is open, log in to the system as user **administrator** and the password **St0r@ge!** (The "0" in the password is the numeral zero).

```
Ocarina release 1 (EAR-1.00.00) Build: 32850
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.).
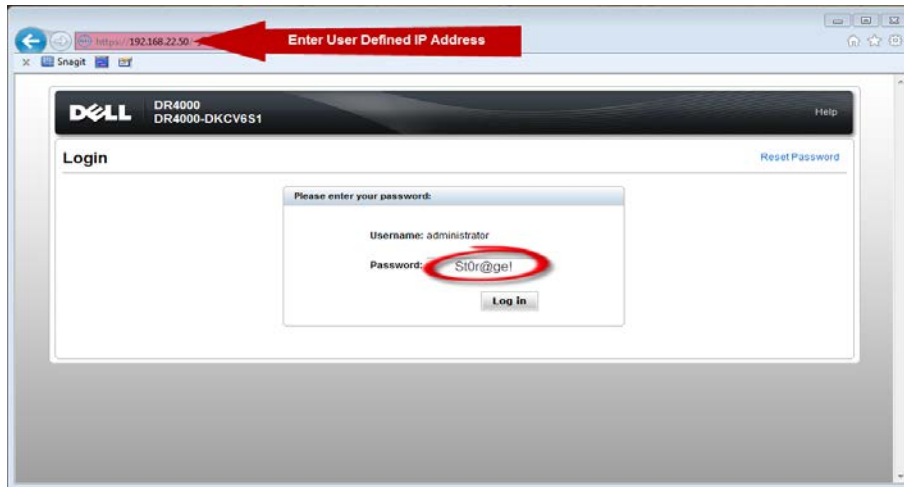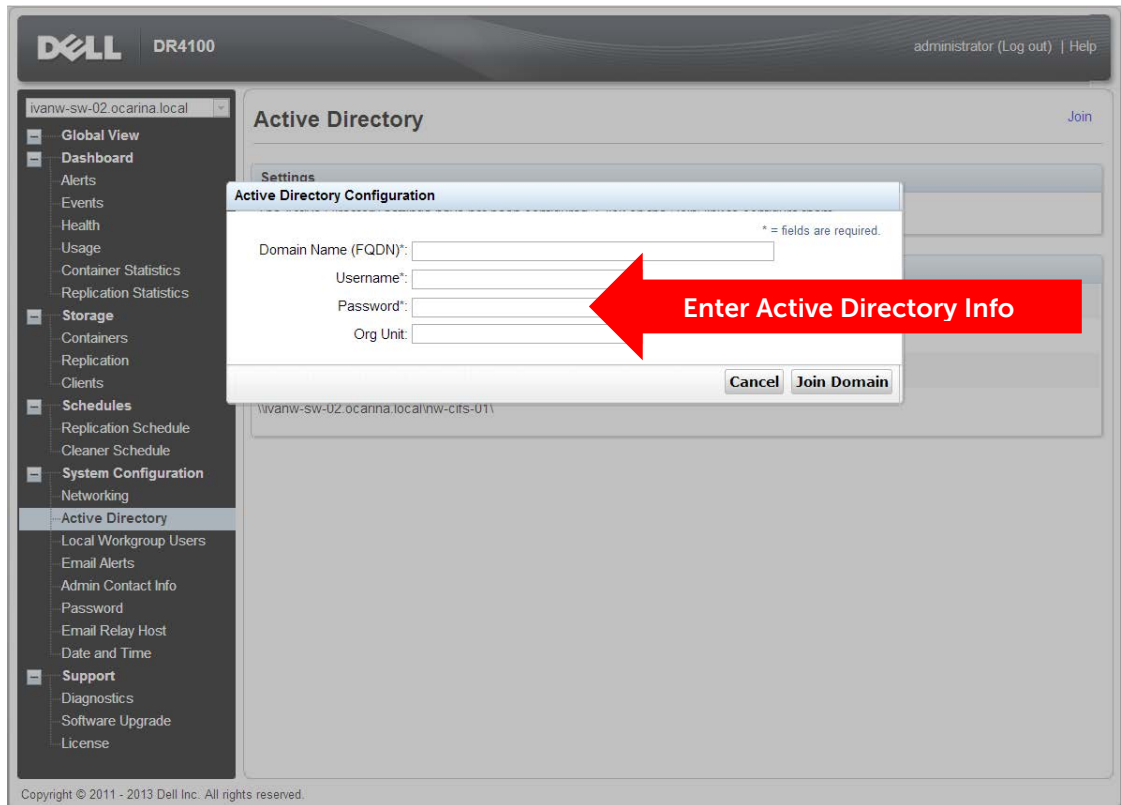

> **Note:** if you do not want to add DR Series Deduplication Appliance to Active Directory, please see the *DR Series Deduplication Appliance Owner's Manual* for guest login instructions.
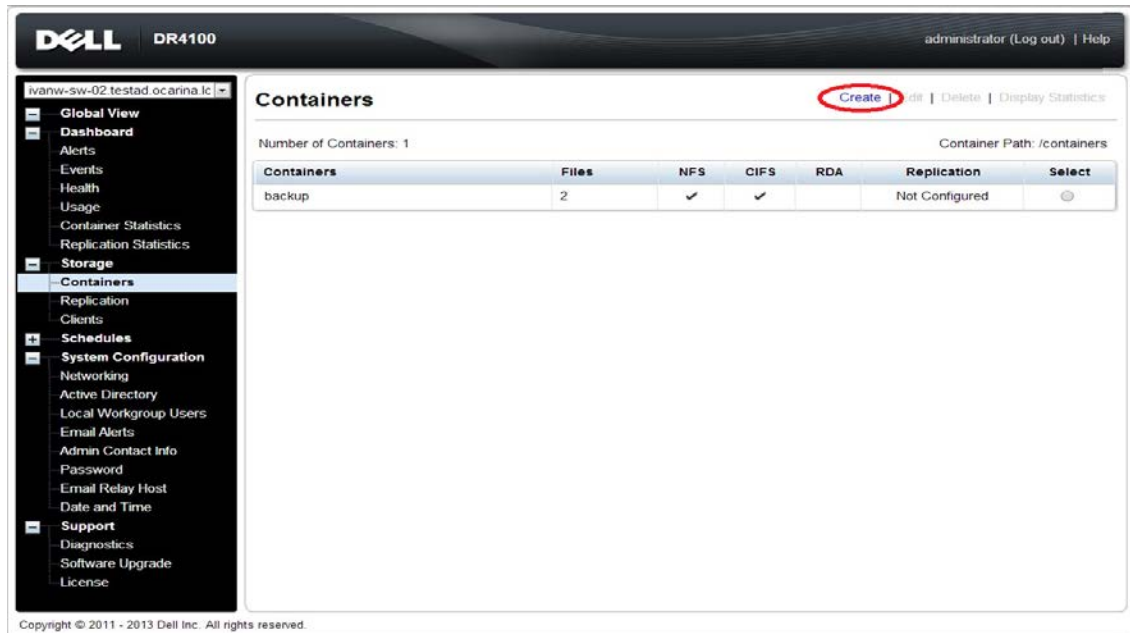
9. Join the DR into Active Directory domain.

- Select **Active Directory** from the menu panel on the left side of the management interface.
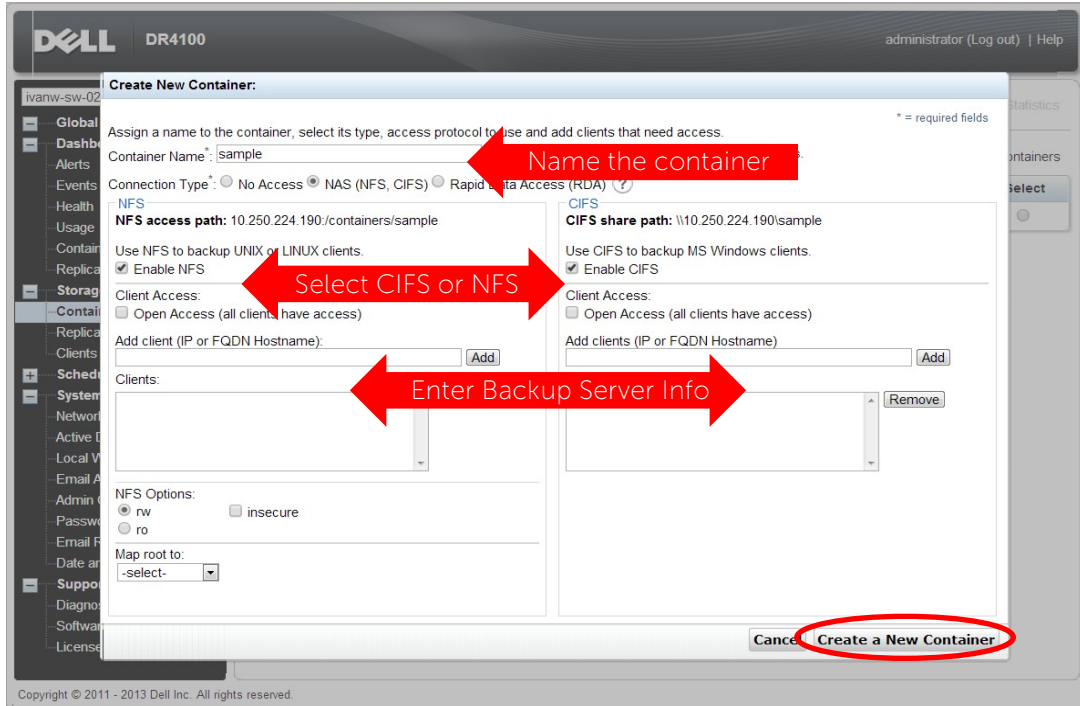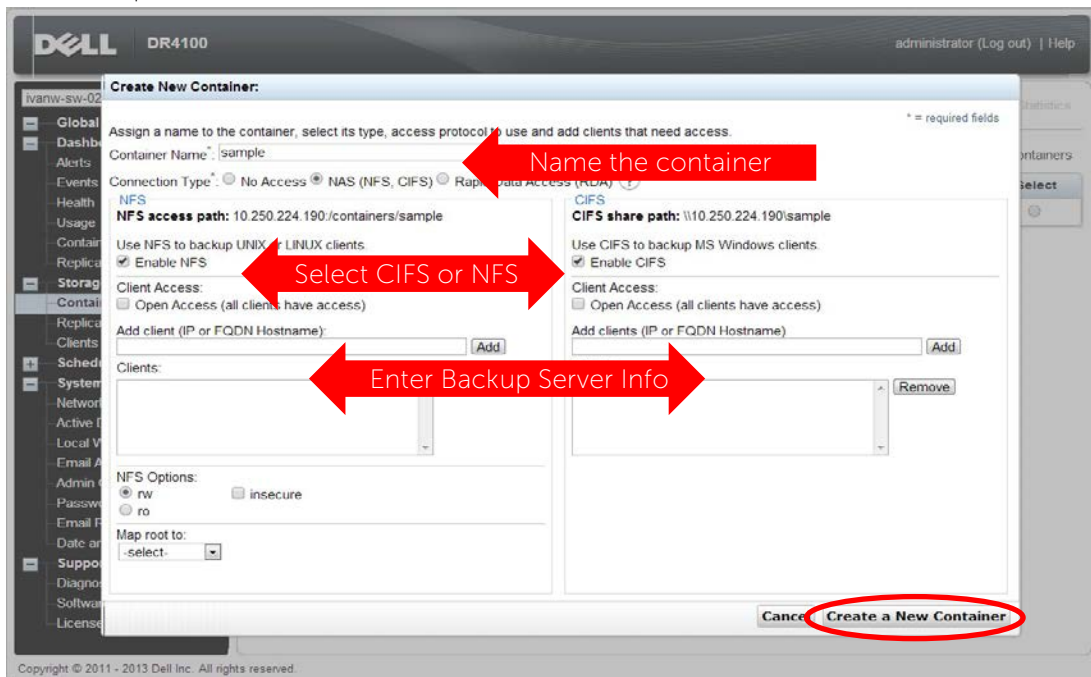
- Enter your Active Directory credentials.

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.

11. Enter a **Container Name**, select **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 (vRanger Server, vRanger client machines)

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

14. Click **Edit.** Note down the container share/export path, which you will use later to target the DR Series Deduplication Appliance.
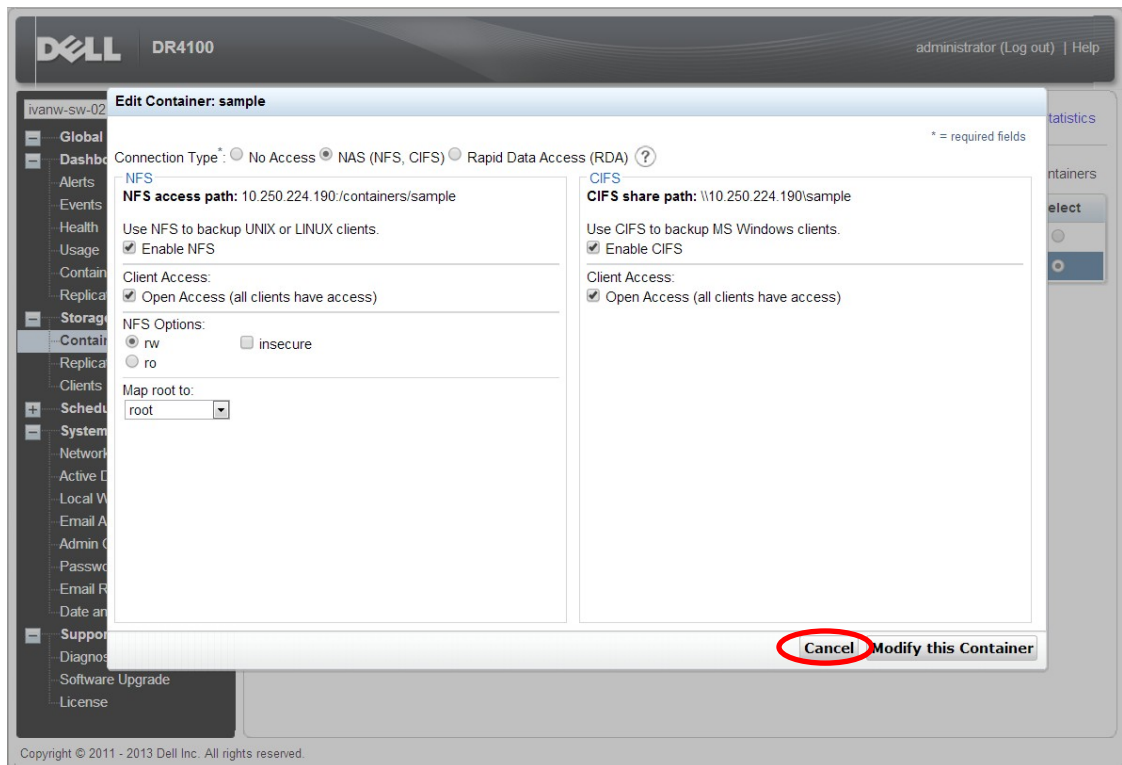
15. Click Cancel to exit.

NOTE: For NFS backup using vRanger, a target folder needs to be created under NFS share directory. This is a sub-directory of the DR container NFS Export directory. This is the location to which savepoints will be written. This is not required while adding CIFS share. Mount the NFS share onto any of the NFS clients available in the environment. Create a directory using mkdir command inside the mounted directory.

2 Set up vRanger

<u>**NOTES:**</u>

- To maximize the DR Series Deduplication Appliance-vRanger storage capacity savings, it is highly recommend following the exact below setup settings.
- The backup formats differ completely when setup settings are changed. Hence, all savings on vRanger installations that had settings changed in between are null and void.
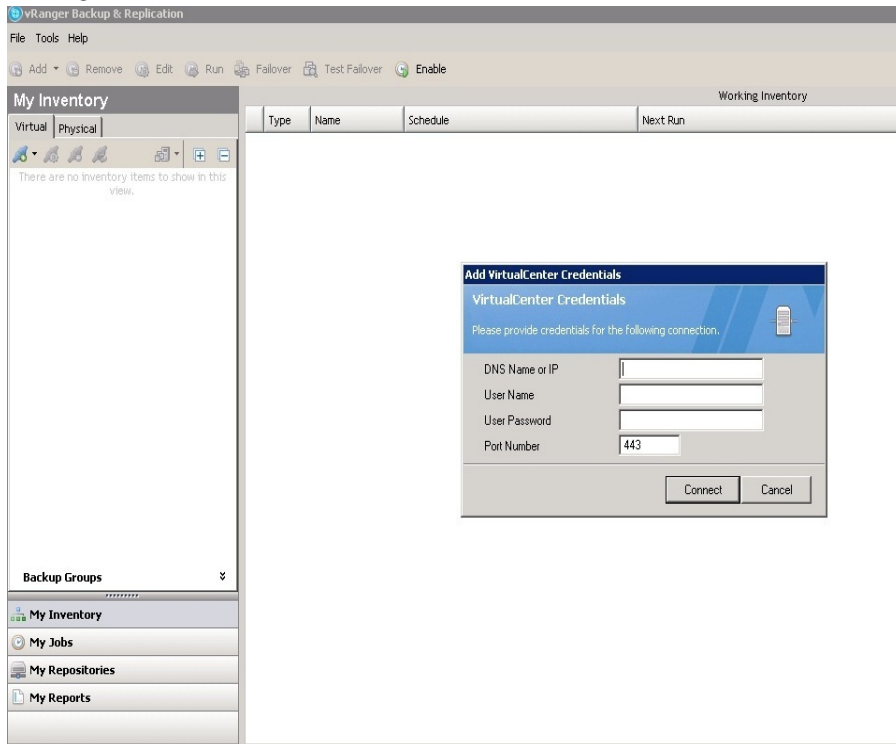
1. For backing up virtual machines, open **vRanger Backup & Replication** Console. Goto **My Inventory** - > **Virtual** - > **Add,** and add either your **Virtual Center** or **ESX Host**.
While adding **Virtual Center** provide IP/Hostname, and credentials of accessing the virtual center. While adding **ESX Host** provide root credentials to access the ESX host.
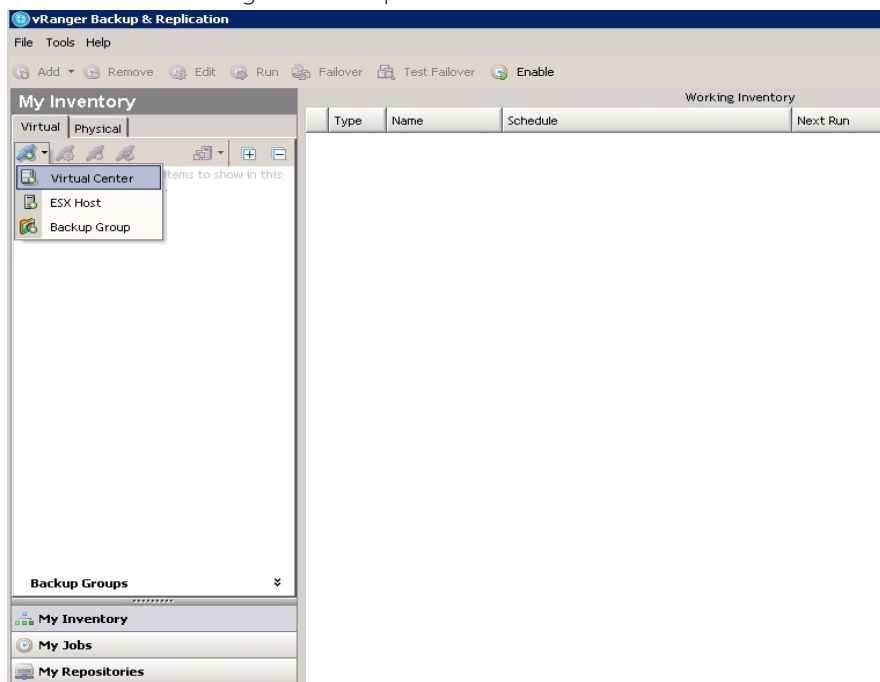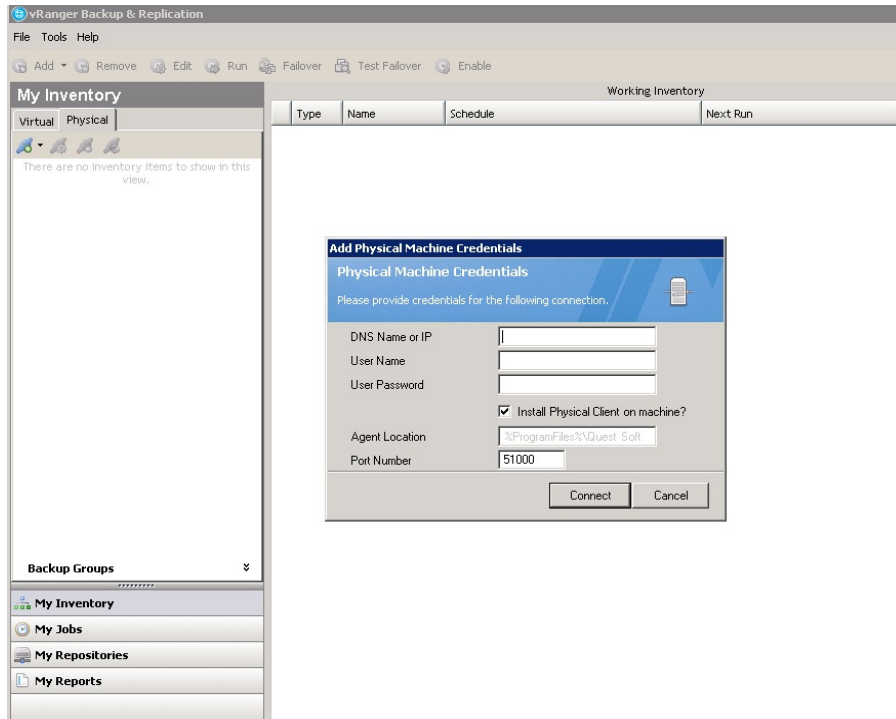
- Adding ESX host
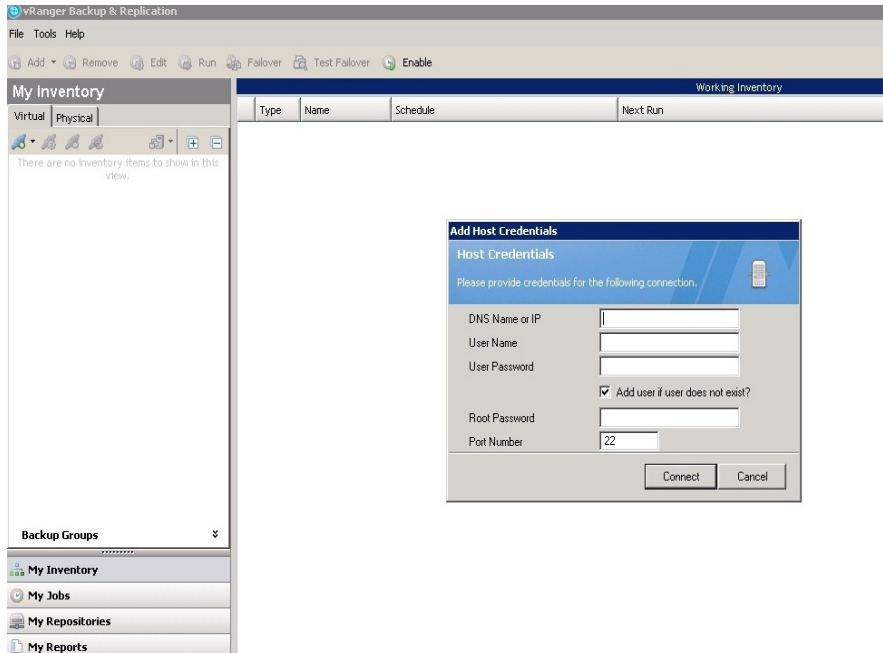
- Adding Virtual Center

2. For backing up physical machines, go to **My Inventory** -> **Physical** -> **Add**
   Select '**Install Physical Client on machine?**' flag. By default Physical client is installed on
   the physical machine at 'c:\programs Files\Quest Software\'.

3. Mapping CIFS/NFS share to vRanger. vRanger supports both CIFS and NFS protocols.
- Mapping CIFS share : **My Repository** -> **Add** -> **Windows Share (CIFS)** -> Enter required
 details and then **OK**.
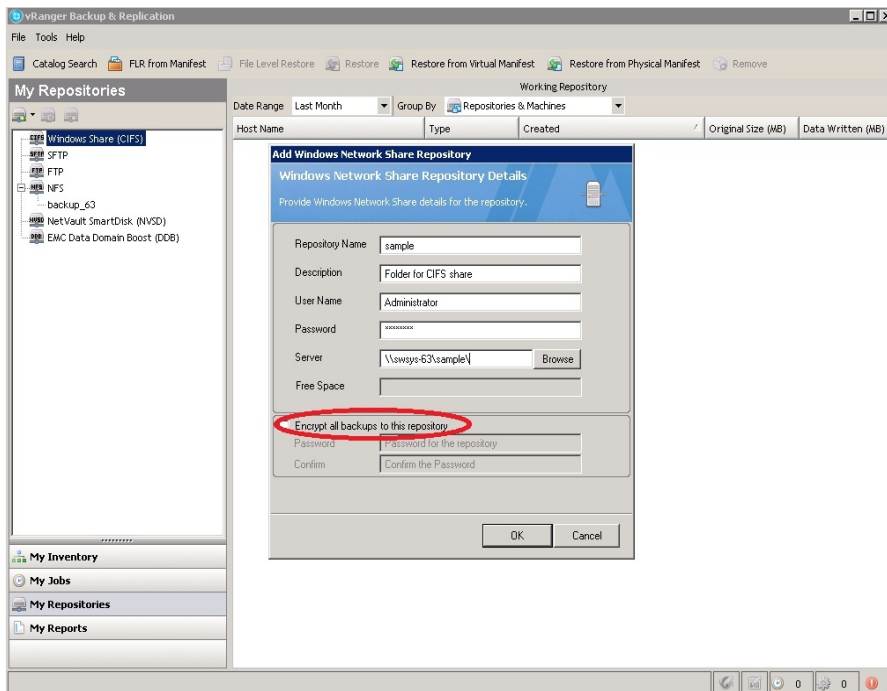
> **NOTE** : While creating repository (CIFS/NFS), for better savings **DO NOT** enable encryption.

- Mapping NFS export : **My Repository** -> **Add** -> **NFS** -> Enter required Credentials -> **OK**
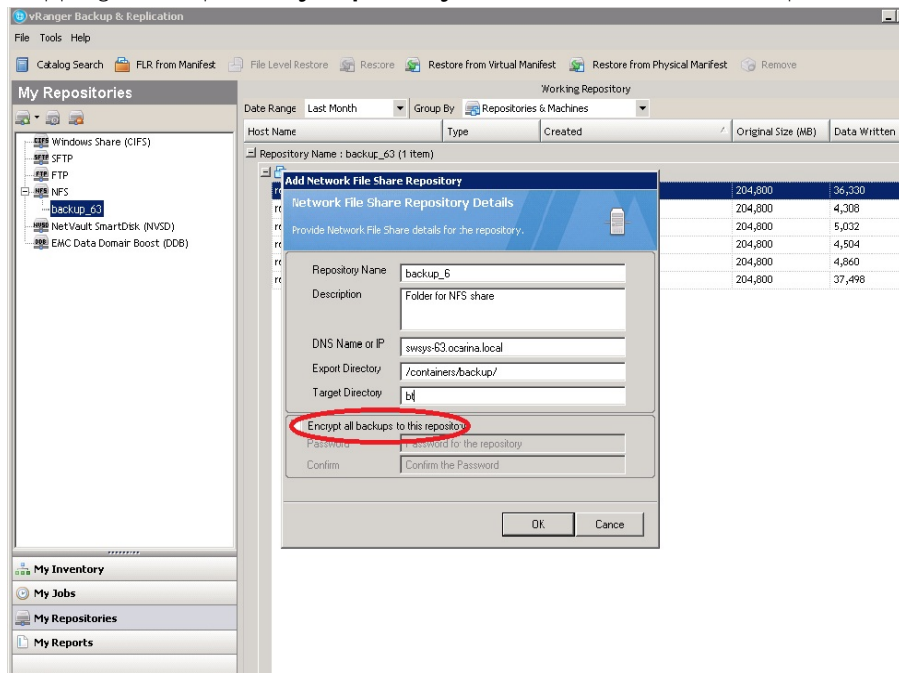

> **NOTE** : In 'Export Directory' just mention export directory and not the whole share path [i.e should not provide IP/hostname of DR Series Deduplication Appliance]. And in 'Target directory' just mention the target directory name which was created under share directory [Mentioned above in chapter 2].
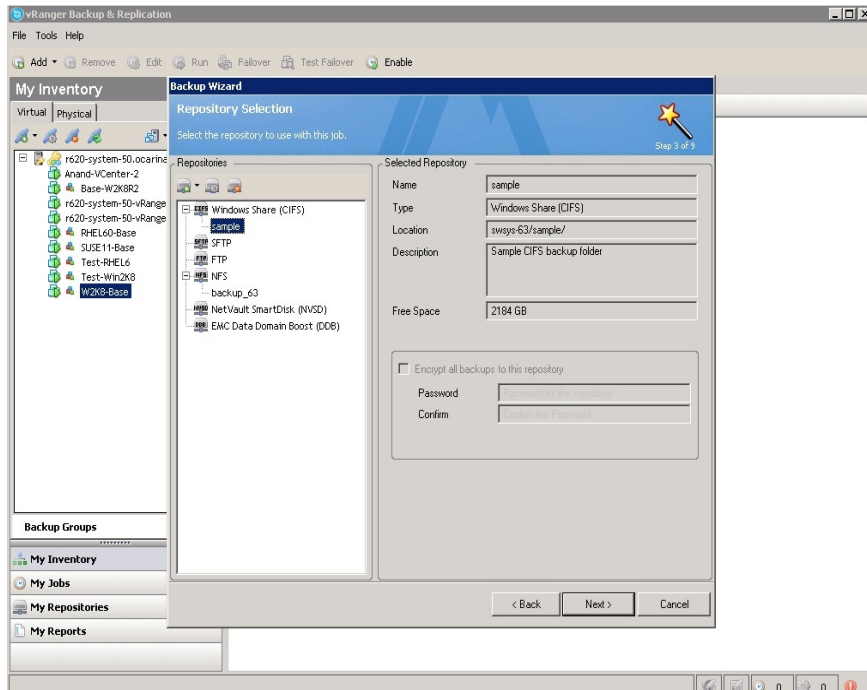
4. **Enable Change Tracking** (Change Block Tracking) on the VM you want to backup.
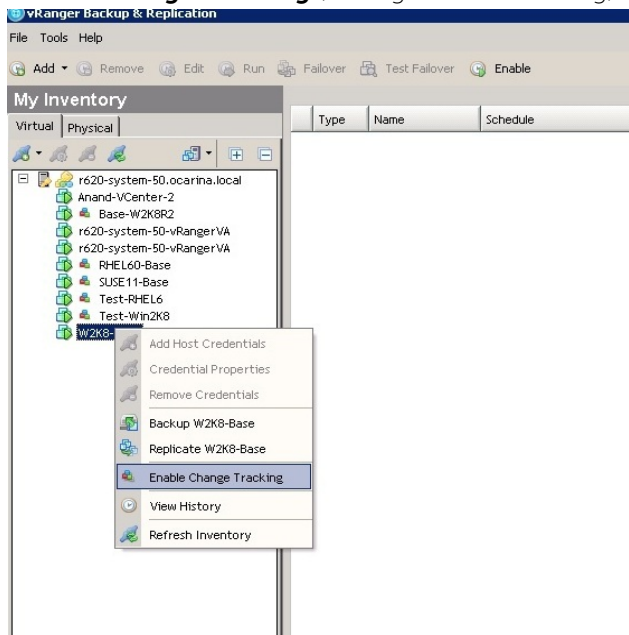
5. Selecting a **Virtual** or **Physical** machine for backup
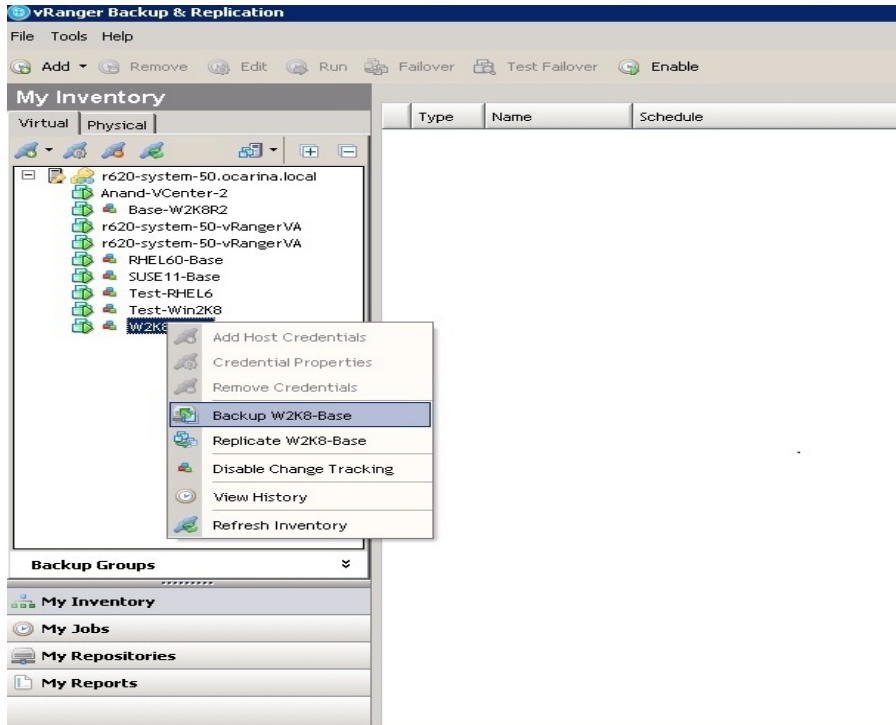
6. This opens the **Backup Wizard.** Select **Included Hard Disks** in **Virtual Machine Hard Disk Inclusion**. Then click **Next** to get to **Repository Selection**. Select the repository to which the machine is to be backed up.
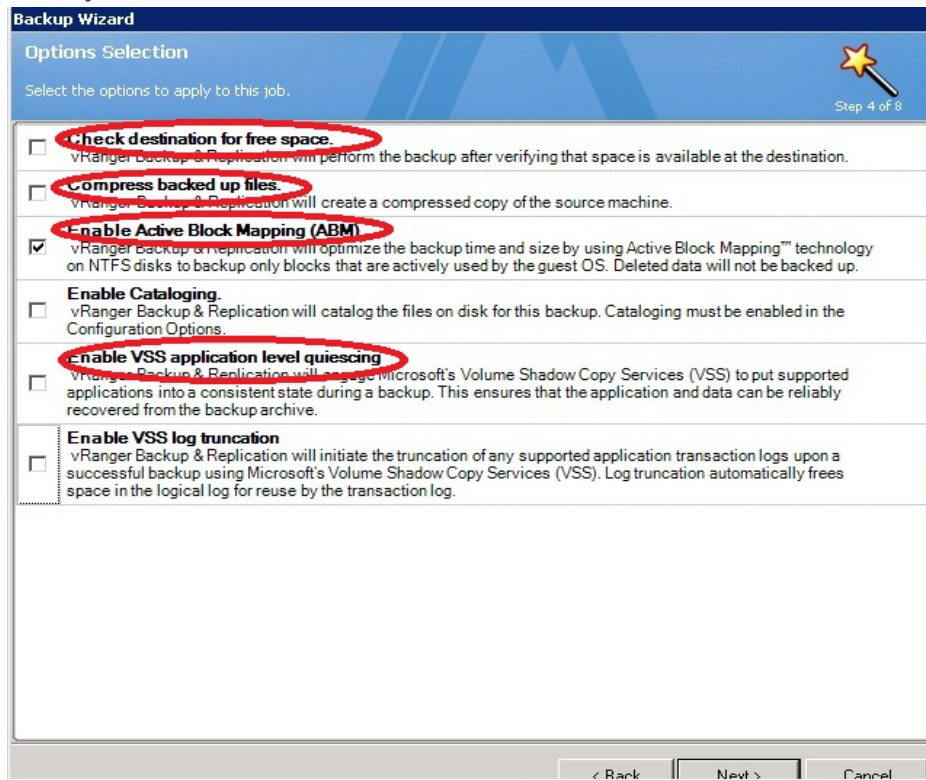
7. Select the appropriate Transport type according to the set up. If not sure, select '**Automatic Transport Selection**'
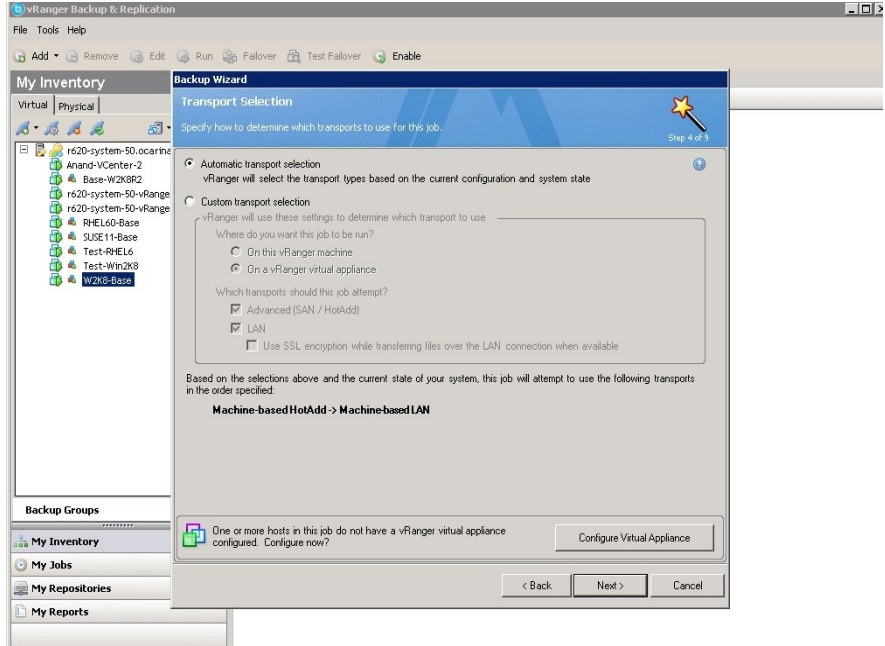
8. Select appropriate backup options in Options Selection
• For VM
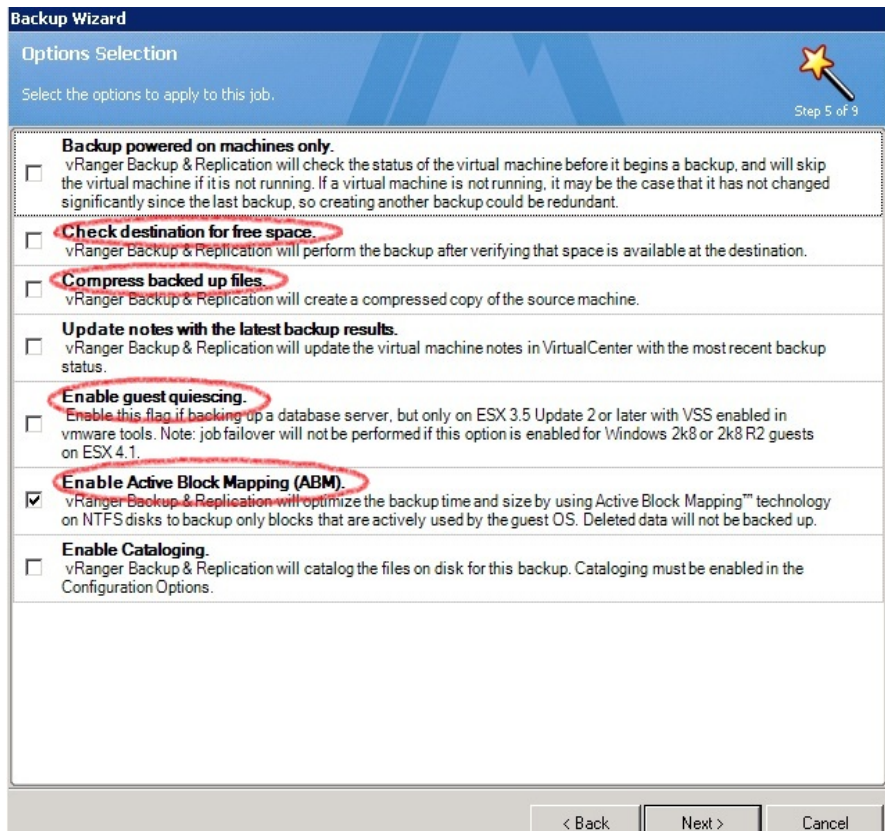
- For Physical Machine

> **NOTE**:
>
> Always Disable **'Check destination for free space'** as DR Series Deduplication Appliance supports deduplication and so overall space occupied is lesser.
>
> Always enable **ABM** (**Active Block Mapping**) for better overall results from both vRanger and DR.
>
> vRanger recommends to Enable **'Guest quiescing'** on VM backups, in case of backing up a database (Eg : Exchange server).
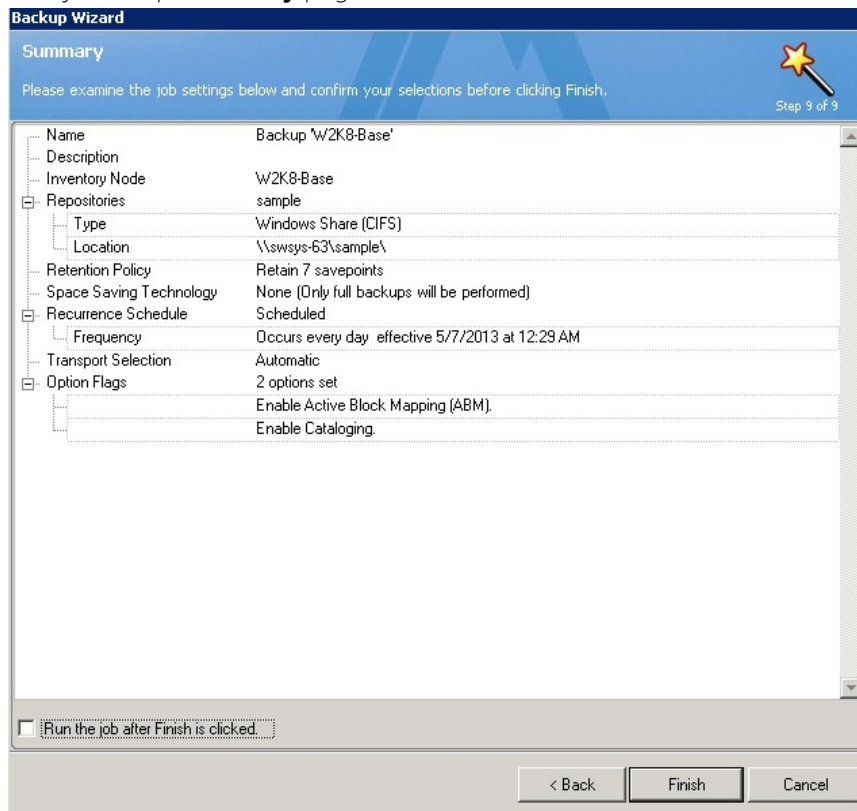>
> **Disable 'compress backed up files'** for better savings.

9. **Retention Policy Selection**: Define the type of backup as **Full/Incremental/Differential**, set **Retention Policy**.
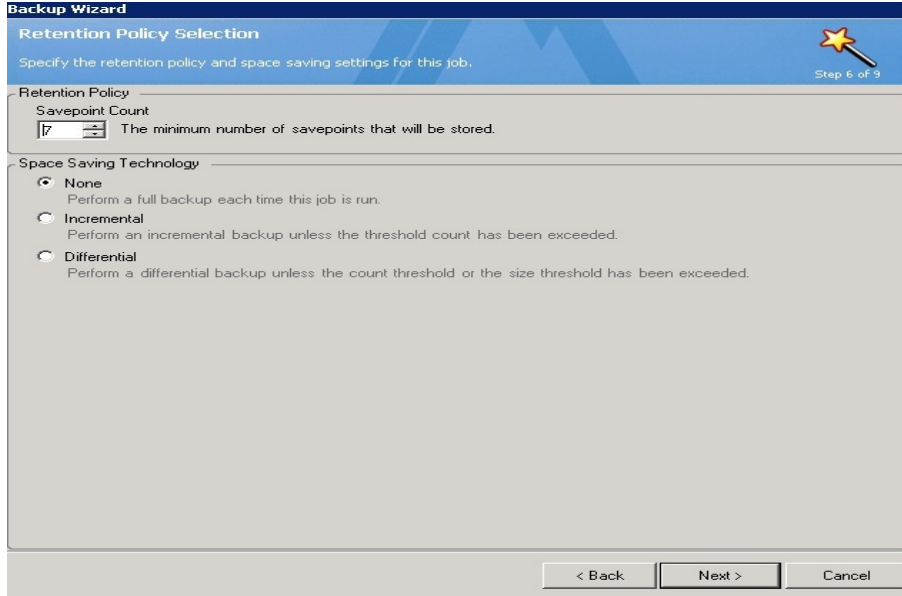
10. Schedule the backup and then provide mail server details for sending mail.

11. Verify backup **Summary** page. Click **Finish**.

3 DR Native Replication Setup & Restore from Target Container

3.1 Build Replication Relationship between DRs

1. Create a source container on source DR

2. Create a target container on target DR

3. On source DR, go to **Replication** page, and then click **Create**

4. Select the source container as source container, then enter the info of second DR

5. Click **Retrieve Containers**, then select the target container on the list
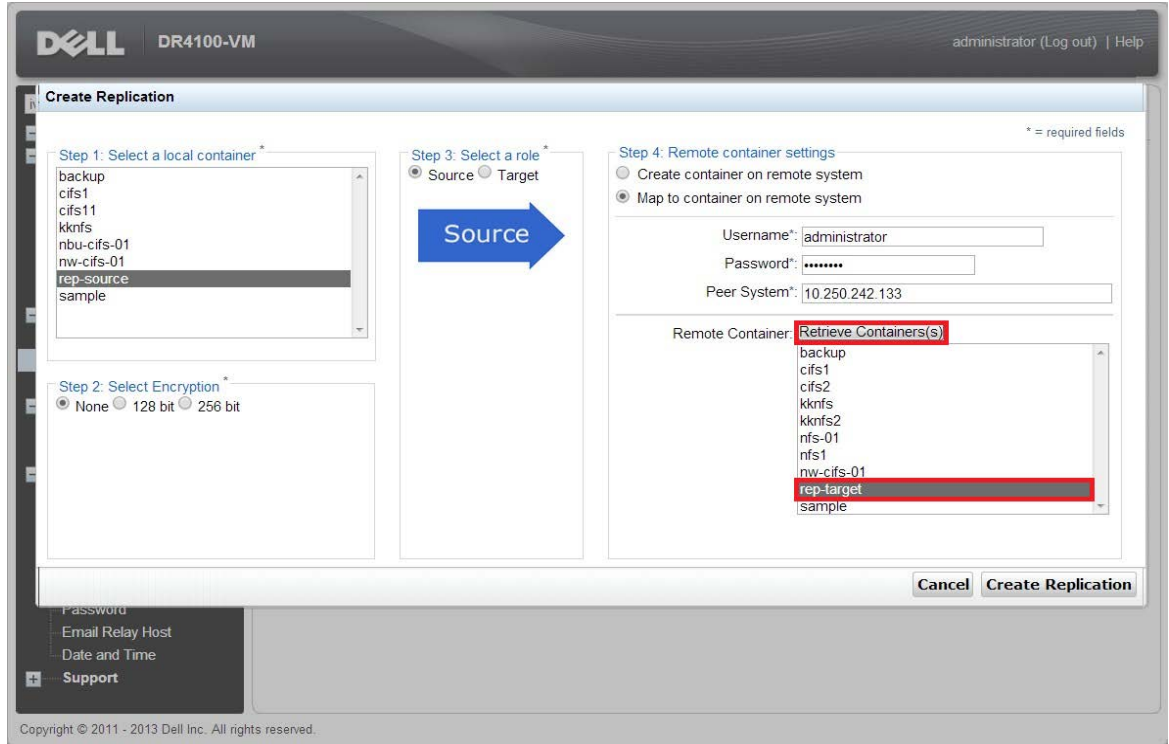
6. Click **Create Replication**
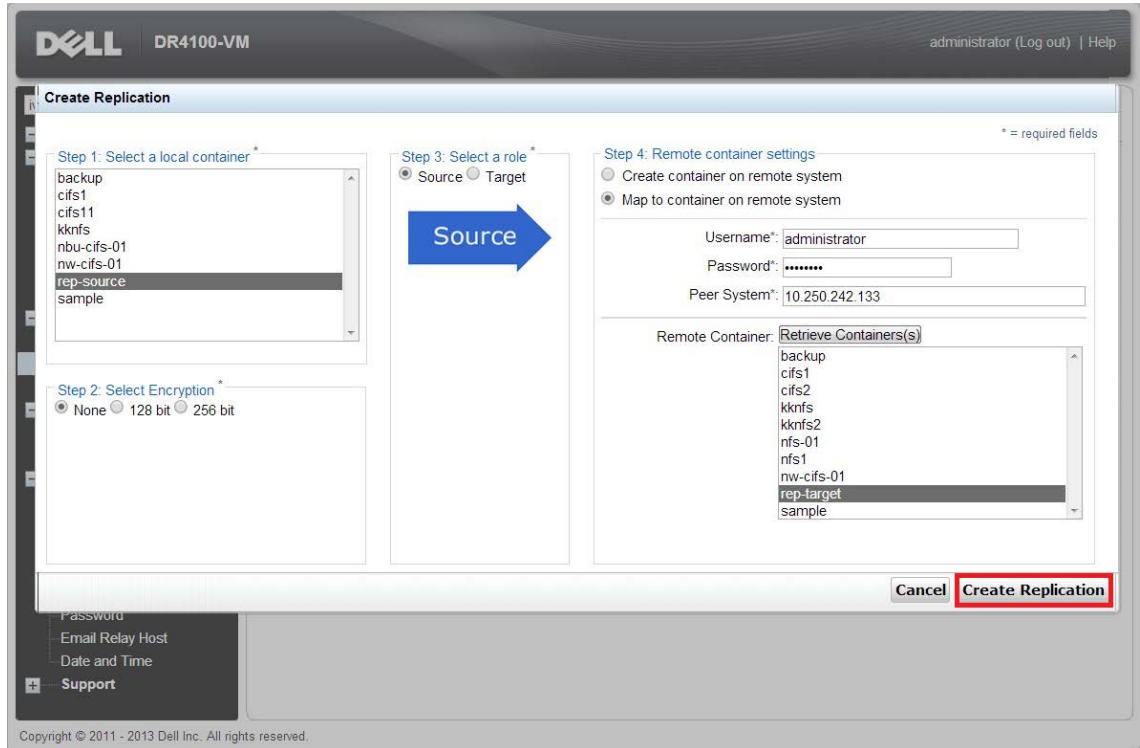
7. Verify the replication relation between DRs is created.

NOTE:
Make sure the replication session has **Peer Status** as **Online**. If restore from replication target is needed,
Make sure the replication is in **INSYNC** state from Replication Statistics menu, and Stop or Delete the replication.
Make sure the replication target has **CIFS**/**NFS** connection(s) enabled when restoring from it.

3.2   Restore data from target DR

8. Add the target DR container into vRanger repository. Follow the same steps as described under **Section 2** in **Step#3**.

9. Create a restore job from this target container. Go to **My Repositories**, select the container repository. In the **Working Repository** pane click to select a savepoint to restore. Click the **Restore** icon on the toolbar, or right-click the savepoint and click **Restore**.
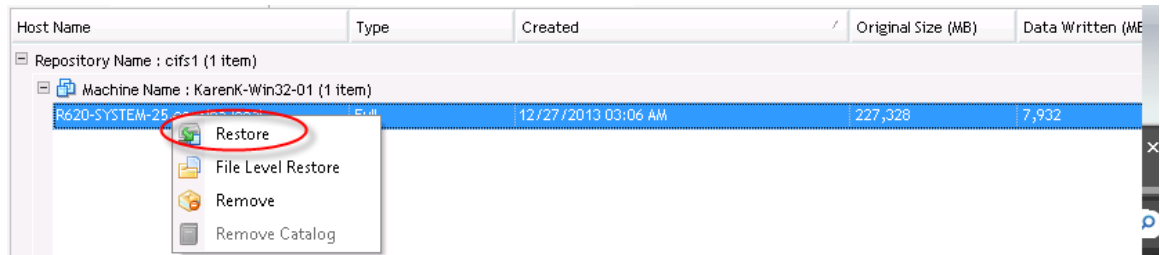
10. Monitor the job and verify it completes successfully.
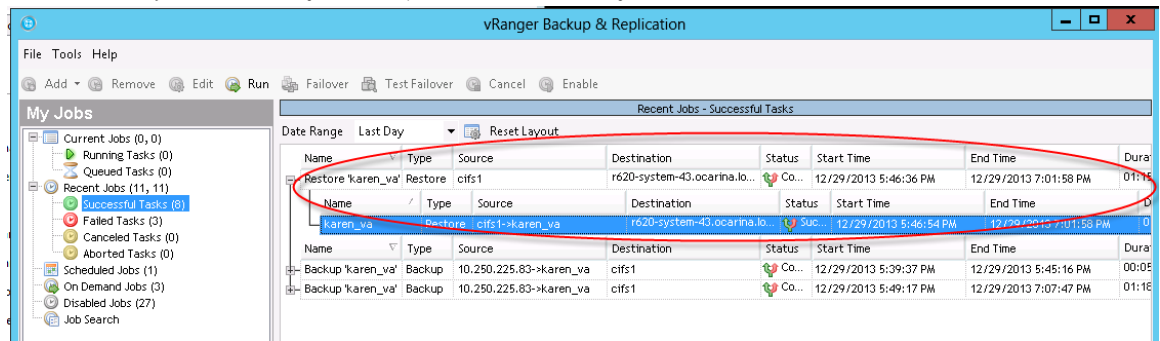
4   Set up the DR Series Deduplication Appliance Cleaner

The cleaner will run during idle time. If you 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.

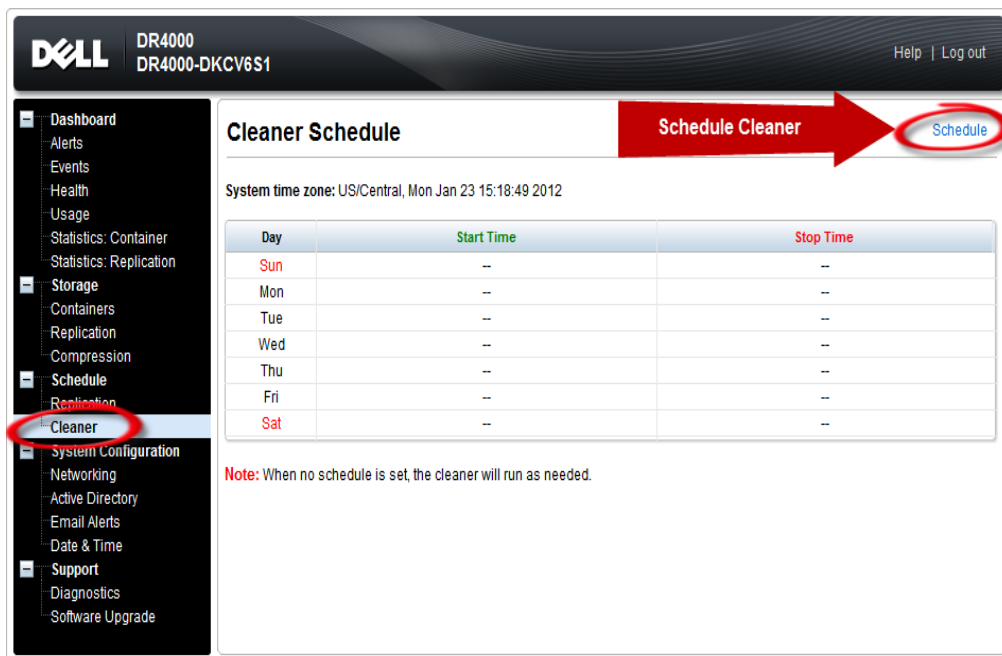If necessary you can do the following procedure as described in the screenshot to force the cleaner to run. Once all the backup jobs are setup the DR Series Deduplication Appliance cleaner can be scheduled. The DR Series Deduplication Appliance cleaner should run at least 6 hours per week when backups 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.

5   Monitoring Dedupe, Compression & Performance

After backup jobs have run the DR Series Deduplication Appliance will track 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. As mentioned before backup jobs with 12 week retention will average a 15x ratio in most cases.