



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

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

Revisions.....	2
Executive Summary	4
1 Install and Configure the DR Series Deduplication Appliance.....	5
2 Set up vRanger	12
3 DR Native Replication Setup & Restore from Target Container.....	20
3.1 Build Replication Relationship between DRs	20
3.2 Restore data from target DR	24
4 Set up the DR Series Deduplication Appliance Cleaner.....	25
5 Monitoring Dedupe, Compression & Performance.....	26



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.

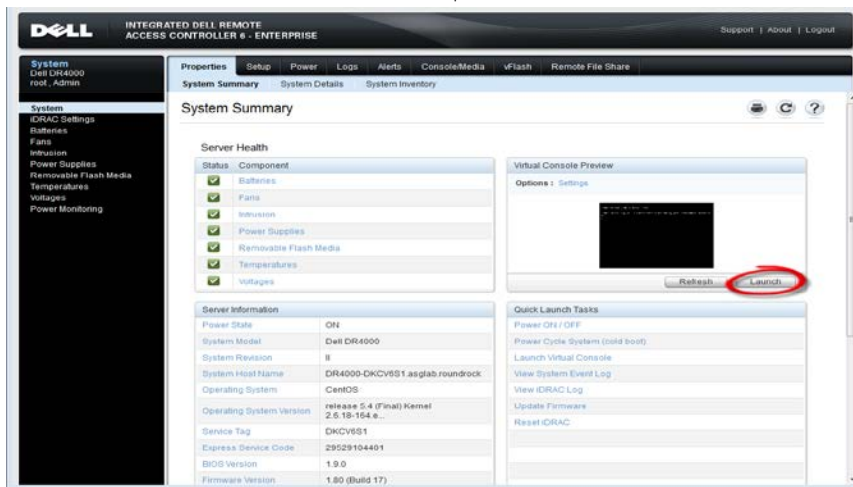
See the DR Series Deduplication Appliance documentation other data management application best practices whitepapers for additional information.

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.

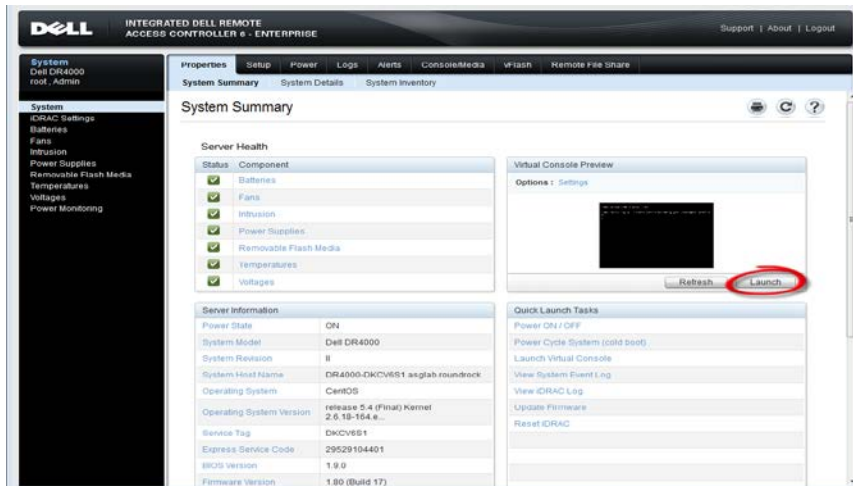


1 Install and Configure the DR Series Deduplication Appliance

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).

```
Debarina 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:
```

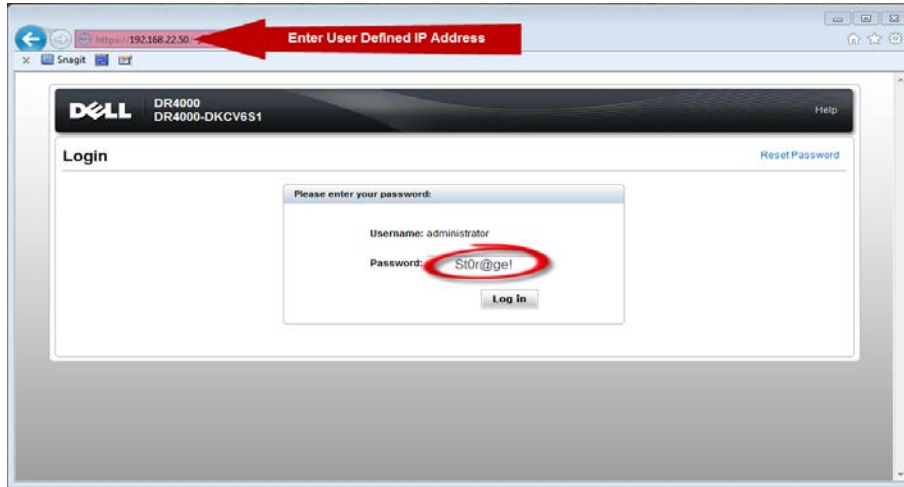
7. View the summary of preferences and confirm that it is correct.

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

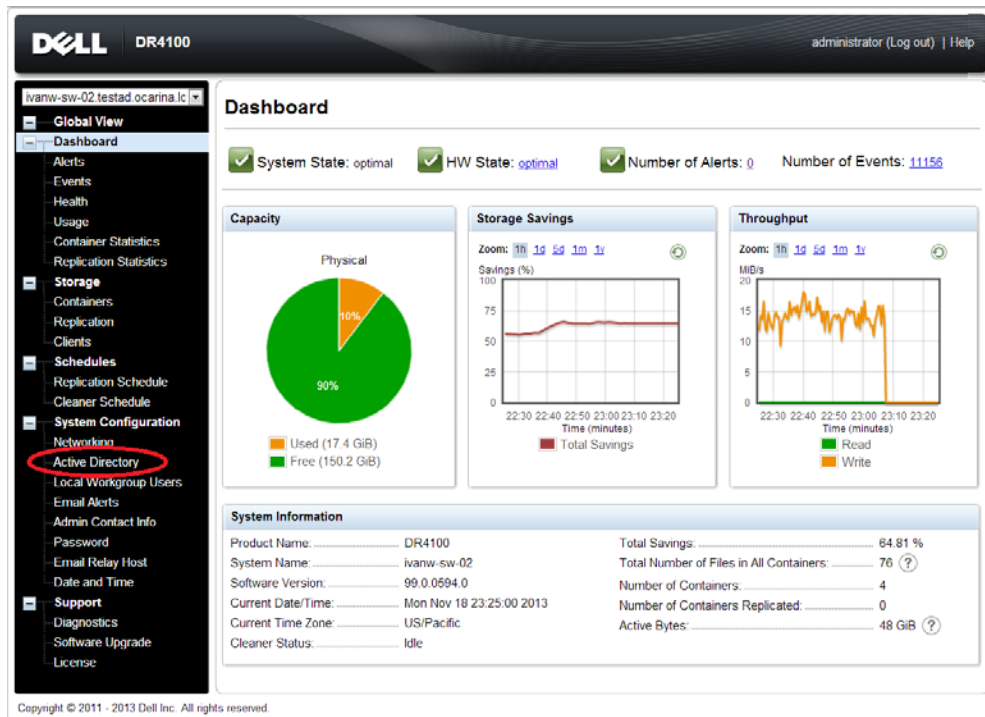


8. Log on to DR Series Deduplication Appliance administrator console, using the IP address you just provided for the DR Series Deduplication Appliance, with username **administrator** and password **St0r@ge!** (The "0" in the password is the numeral zero).

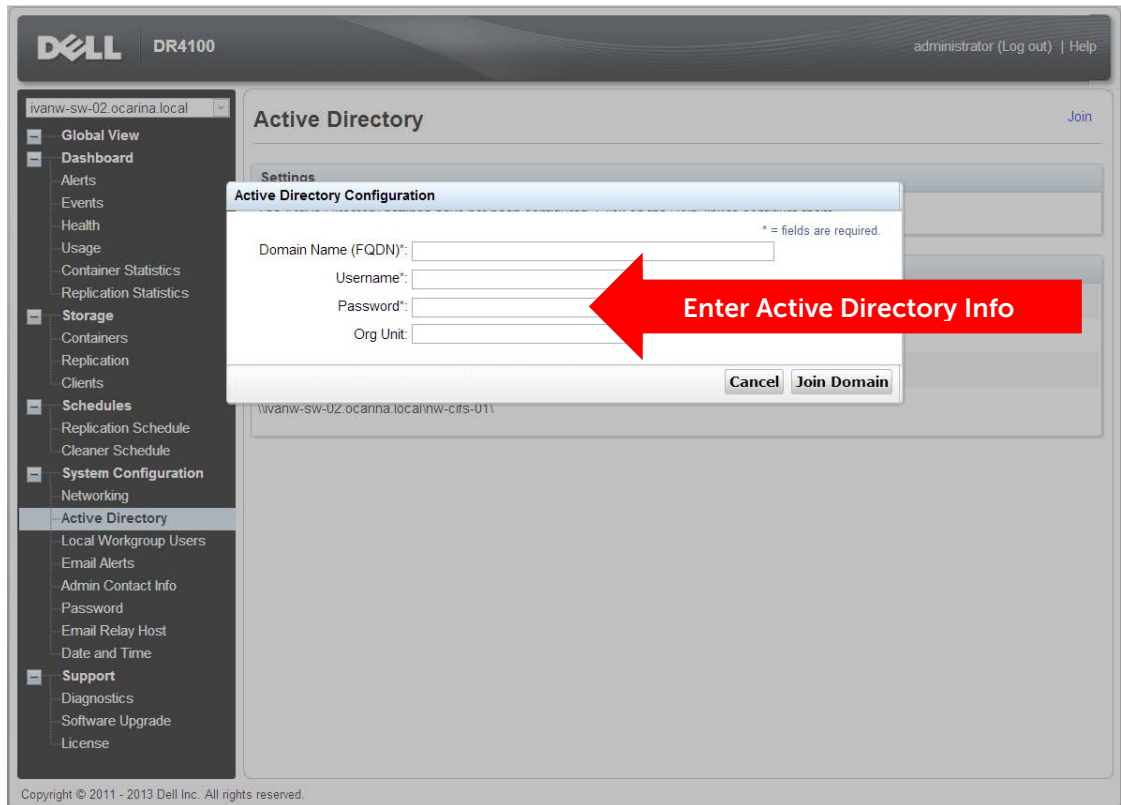


Note: if you do not want to add DR Series Deduplication Appliance to Active Directory, please see the *DR Series Deduplication Appliance Owner's Manual* for guest login instructions.

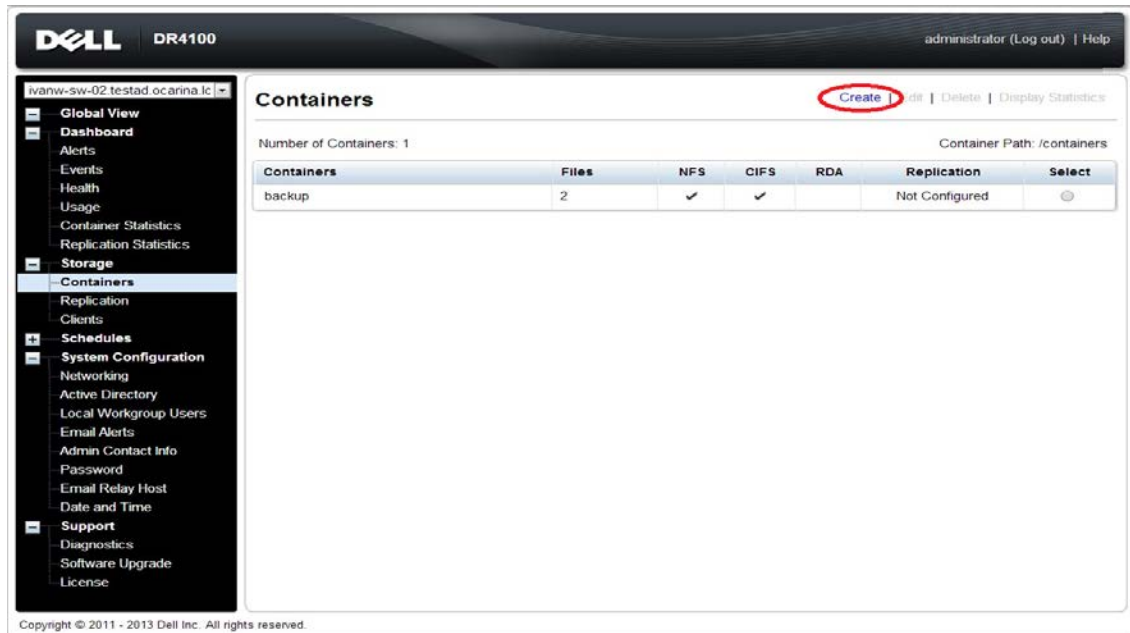
9. Join the DR into Active Directory domain.
 - Select **Active Directory** from the menu panel on the left side of the management interface.



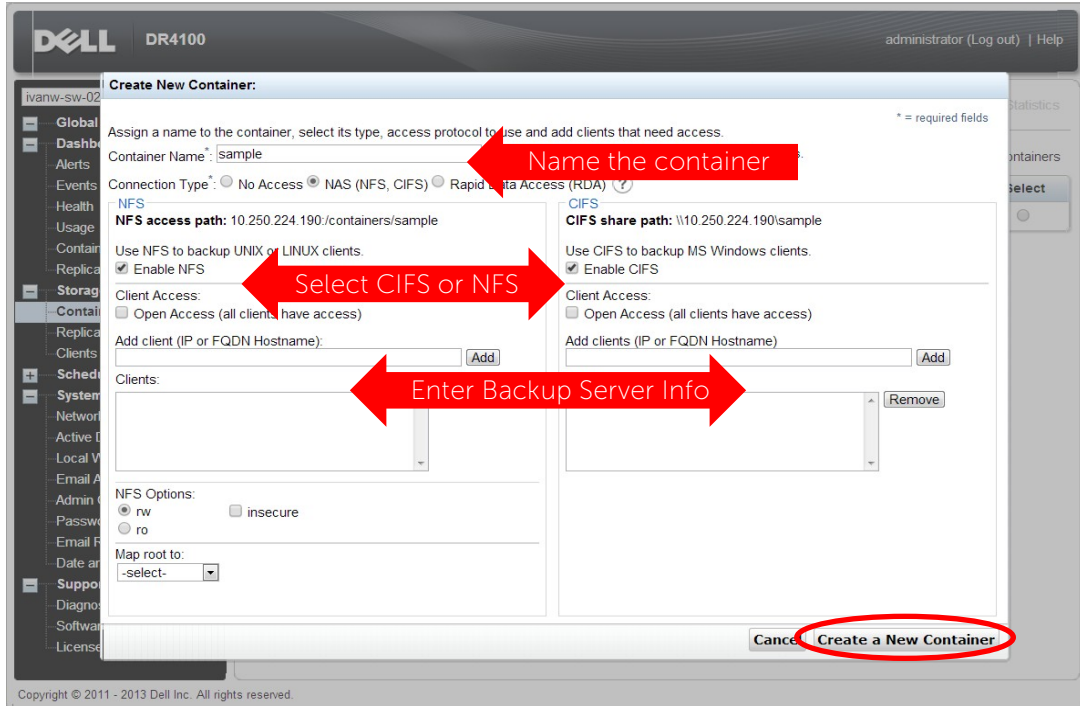
- Enter your Active Directory credentials.



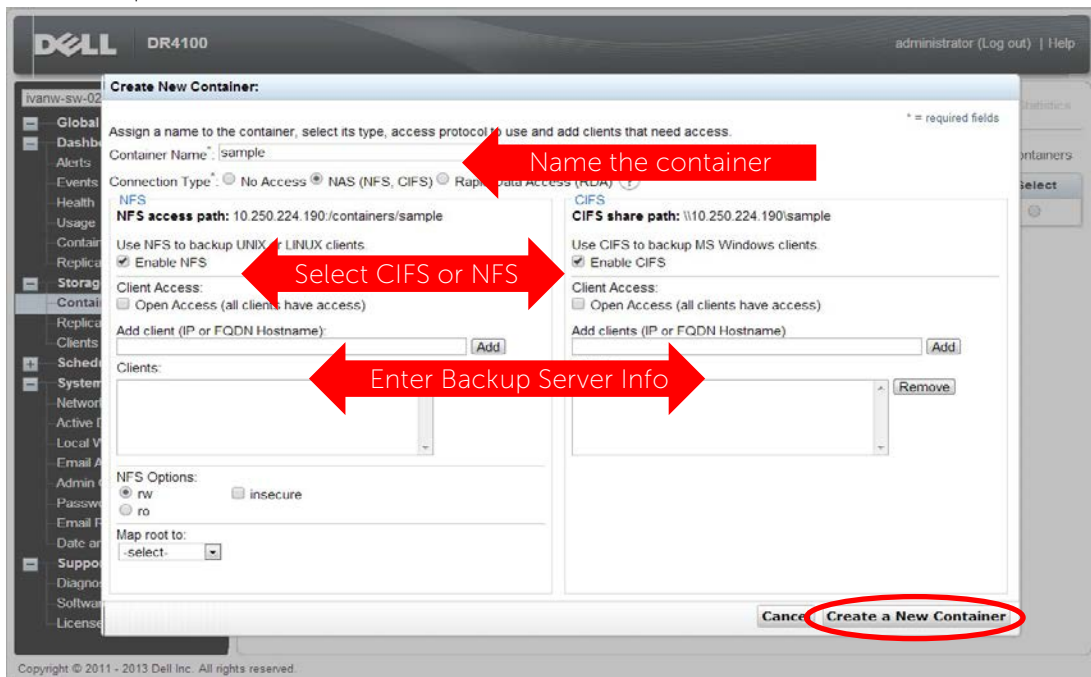
10. Create and mount the container. Select **Containers** in the tree on the left side of the dashboard, and then click the **Create** at the top of the page.



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



- 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)



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

The screenshot shows the Dell DR4100 web interface. The left sidebar contains navigation options like Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Replication, Clients, Schedules, System Configuration, and Support. The main content area is titled 'Containers' and includes a 'Message' box with a green checkmark and the following text:

- Successfully added container "sample".
- Successfully added NFS connection for container "sample".
- Successfully added CIFS connection for container "sample".

Below the message, it states 'Number of Containers: 2' and 'Container Path: /containers'. A table lists the containers:

Containers	Files	NFS	CIFS	RDA	Replication	Select
backup	2	✓	✓		Not Configured	<input type="radio"/>
sample	0	✓	✓		Not Configured	<input type="radio"/>

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

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

The screenshot shows the 'Edit Container: sample' dialog box in the Dell DR4100 web interface. The 'Connection Type' is set to 'NAS (NFS, CIFS)'. The 'RDA' field is circled in red. The dialog is divided into two sections: NFS and CIFS.

NFS Section:

- Connection Type: No Access NAS (NFS, CIFS) Read-Only Data Access (RDA) ?
- NFS access path: 10.250.224.190/containers/sample
- Use NFS to backup UNIX or LINUX clients. Enable NFS
- Client Access: Open Access (all clients have access)
- NFS Options: rw insecure
- Map root to: root

CIFS Section:

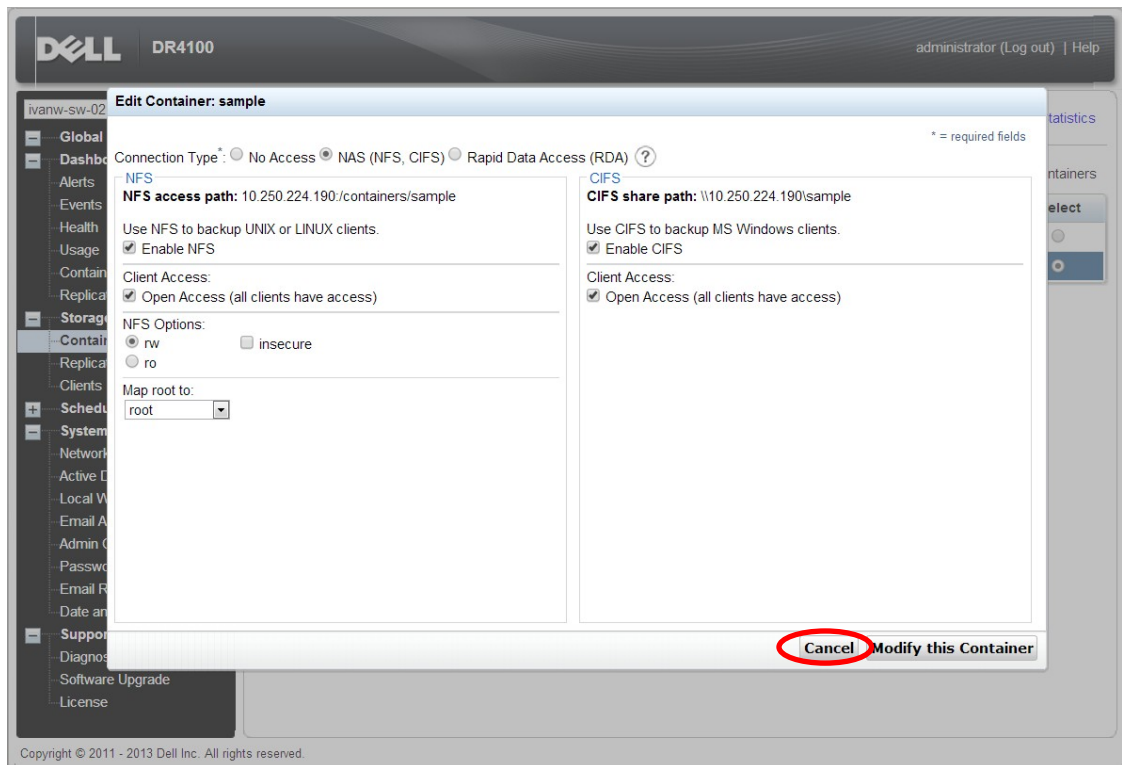
- CIFS share path: \\10.250.224.190/sample
- Use CIFS to backup MS Windows clients. Enable CIFS
- Client Access: Open Access (all clients have access)

Buttons at the bottom: Cancel, Modify this Container

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



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.

```
root@RHEL60-Base:~#  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]# mount -t nfs swsys-63:/containers/backup /mnt/mntpt  
[root@RHEL60-Base ~]#  
[root@RHEL60-Base ~]# mkdir /mnt/mntpt/bt
```

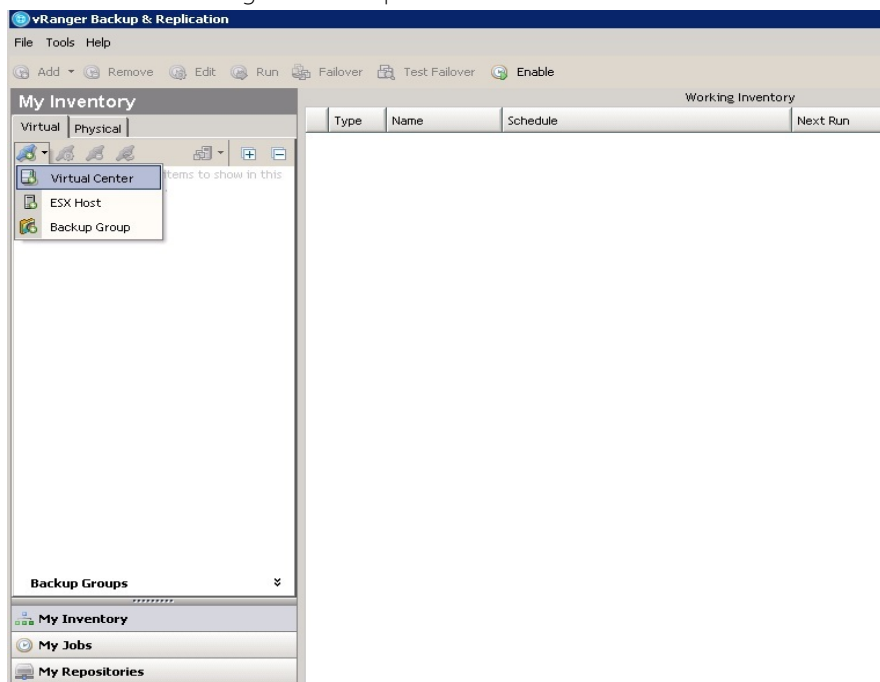


2 Set up vRanger

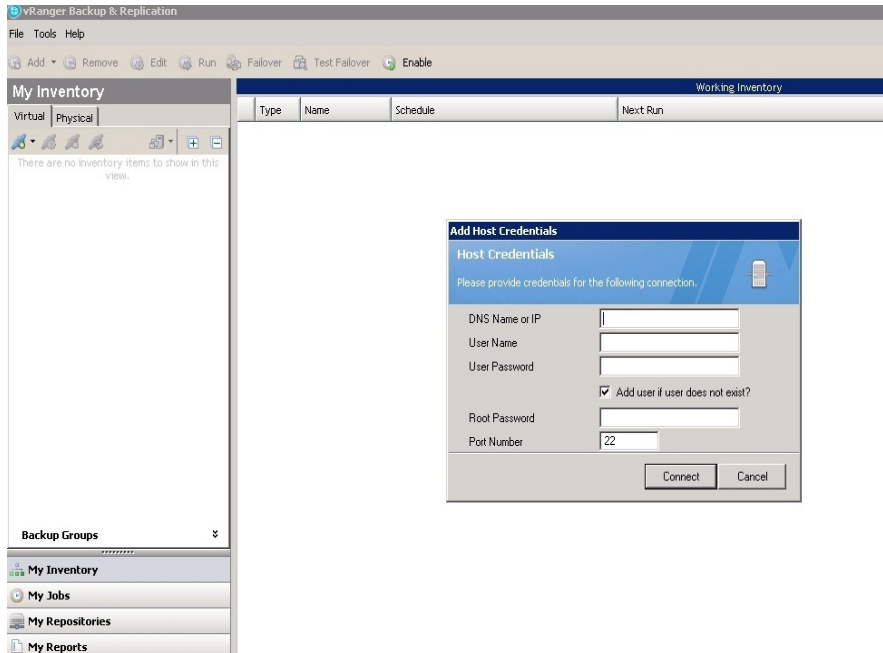
NOTES:

- 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.

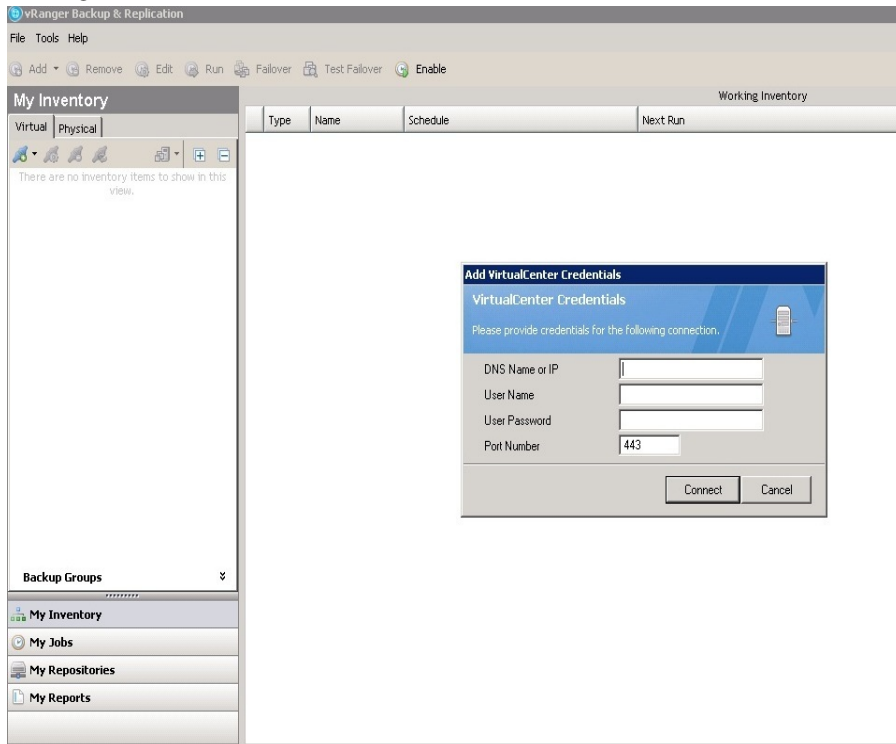
1. For backing up virtual machines, open **vRanger Backup & Replication** Console. Goto **My Inventory** -> **Virtual** -> **Add**, and add either your **Virtual Center** or **ESX Host**. While adding **Virtual Center** provide IP/Hostname, and credentials of accessing the virtual center. While adding **ESX Host** provide root credentials to access the ESX host.



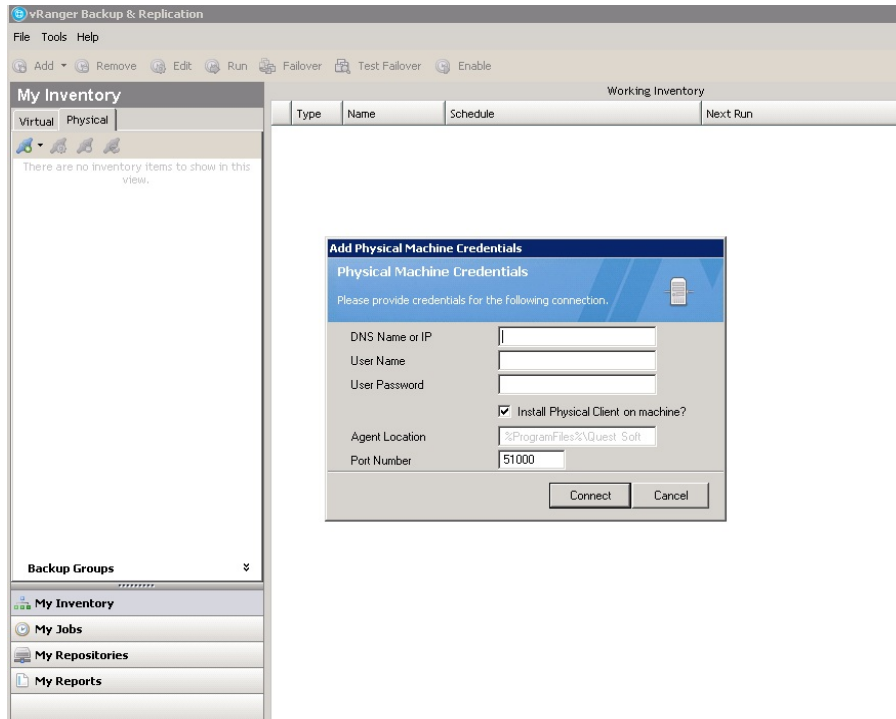
- Adding ESX host



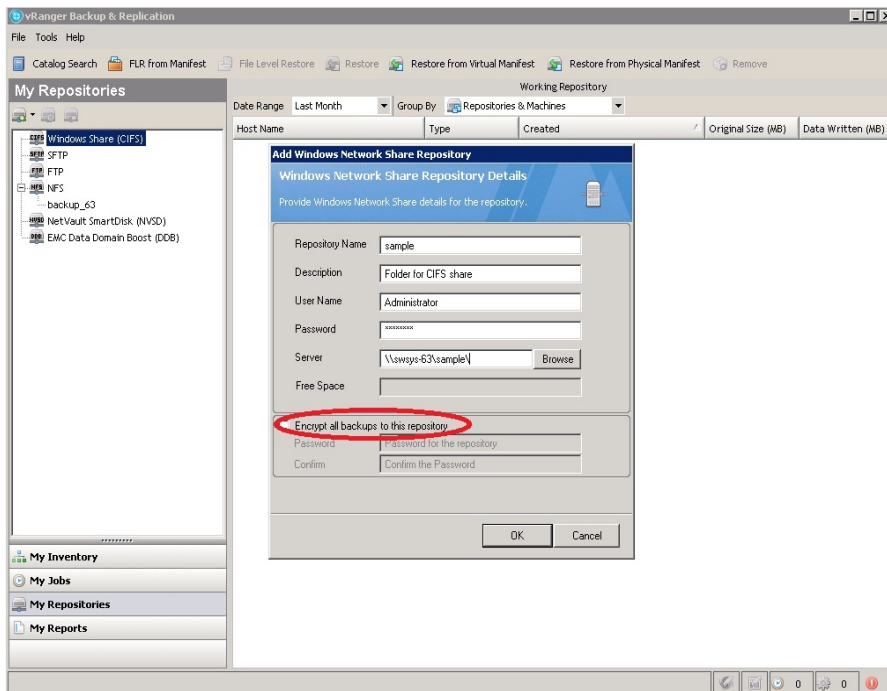
- Adding Virtual Center



- 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\'.

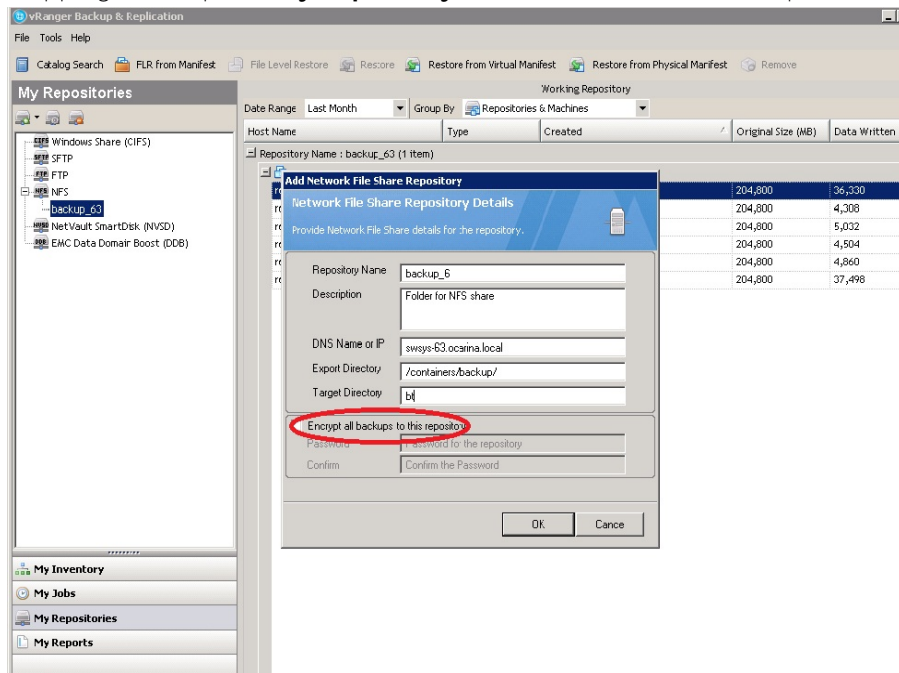


- Mapping CIFS/NFS share to vRanger. vRanger supports both CIFS and NFS protocols.
 - Mapping CIFS share : **My Repository** -> **Add** -> **Windows Share (CIFS)** -> Enter required details and then **OK**.



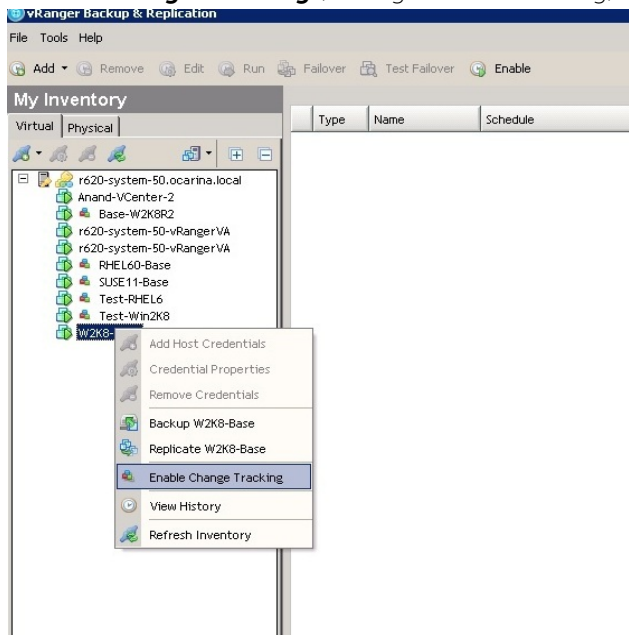
NOTE : While creating repository (CIFS/NFS), for better savings **DO NOT** enable encryption.

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

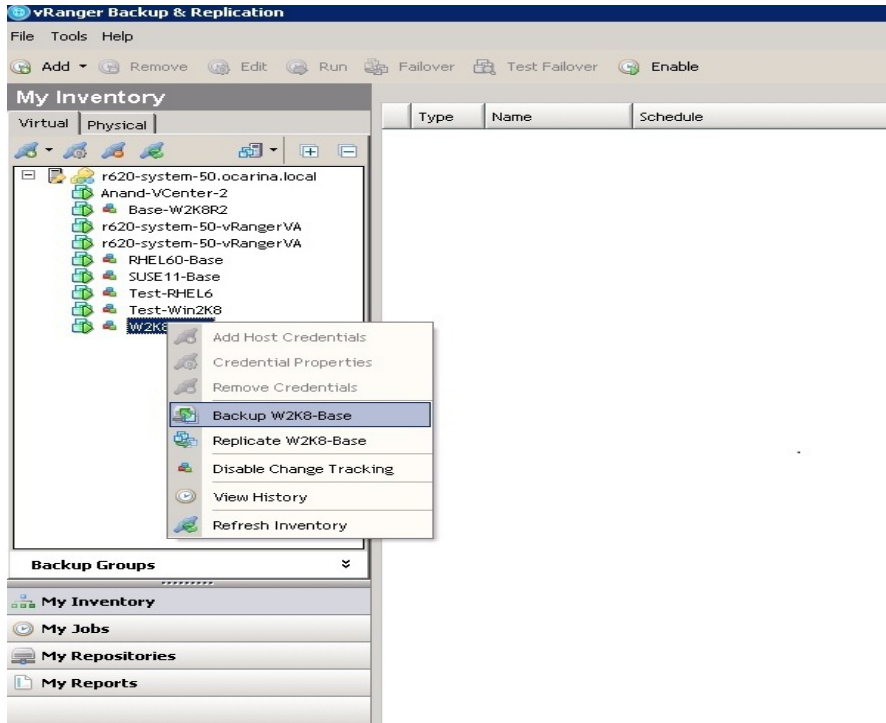


NOTE : In 'Export Directory' just mention export directory and not the whole share path [i.e should not provide IP/hostname of DR Series Deduplication Appliance]. And in 'Target directory' just mention the target directory name which was created under share directory [Mentioned above in chapter 2].

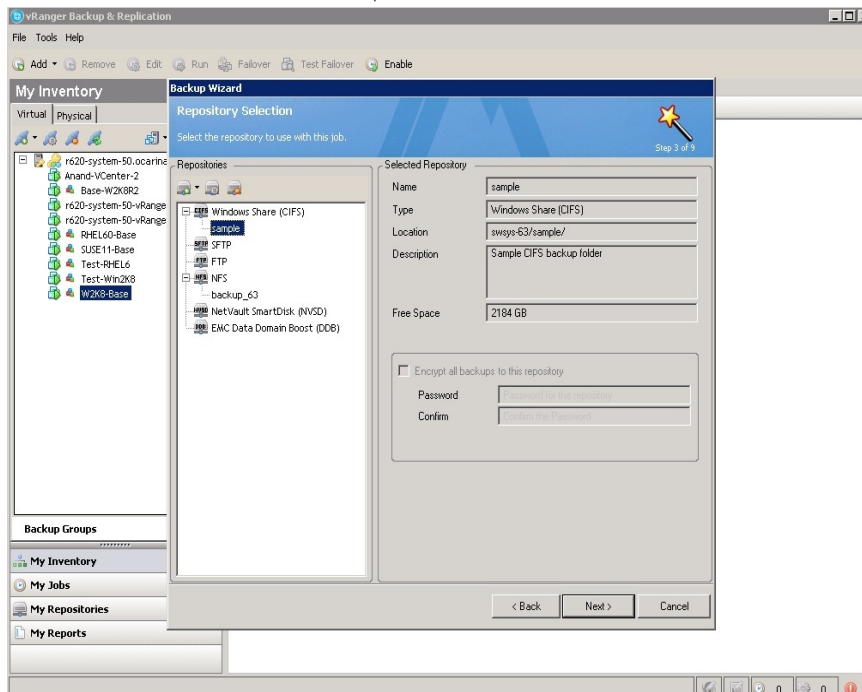
4. **Enable Change Tracking** (Change Block Tracking) on the VM you want to backup.



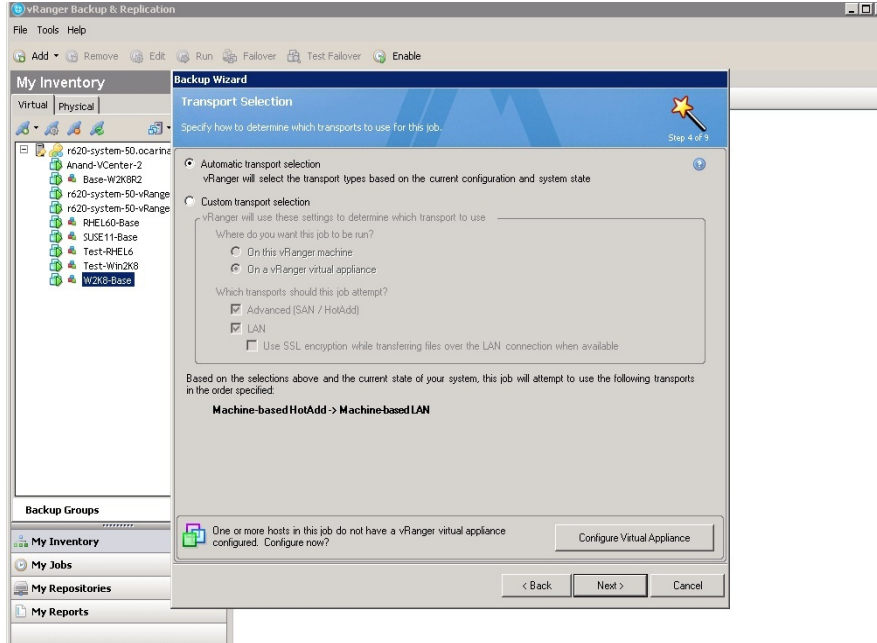
5. Selecting a **Virtual** or **Physical** machine for backup



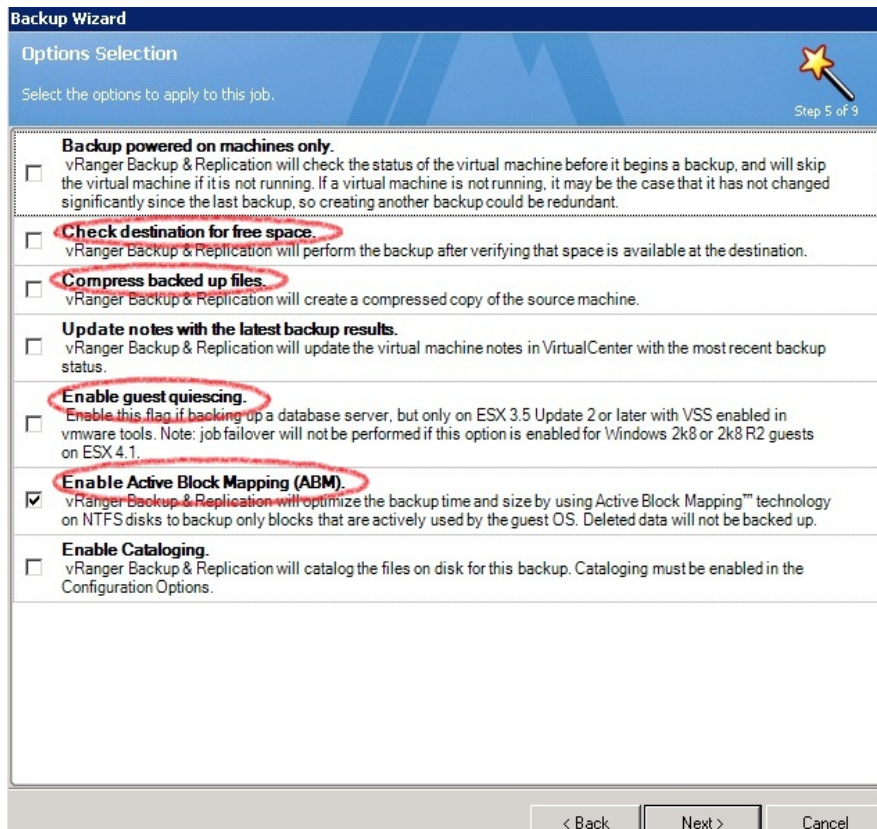
6. This opens the **Backup Wizard**. Select **Included Hard Disks** in **Virtual Machine Hard Disk Inclusion**. Then click **Next** to get to **Repository Selection**. Select the repository to which the machine is to be backed up.



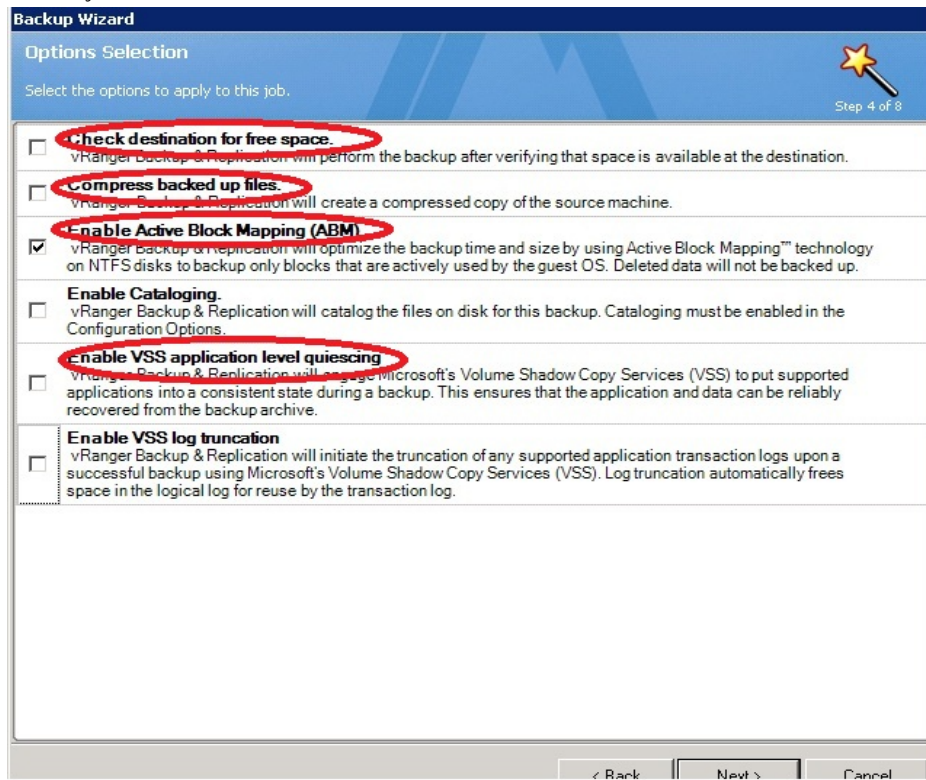
7. Select the appropriate Transport type according to the set up. If not sure, select **'Automatic Transport Selection'**



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**.

Backup Wizard
Retention Policy Selection

Specify the retention policy and space saving settings for this job. Step 6 of 9

Retention Policy
Savepoint Count: The minimum number of savepoints that will be stored.

Space Saving Technology

- None**
Perform a full backup each time this job is run.
- Incremental**
Perform an incremental backup unless the threshold count has been exceeded.
- Differential**
Perform a differential backup unless the count threshold or the size threshold has been exceeded.

< Back Next > Cancel

10. Schedule the backup and then provide mail server details for sending mail.

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

Backup Wizard
Summary

Please examine the job settings below and confirm your selections before clicking Finish. Step 9 of 9

Name	Backup 'W2K8-Base'
Description	
Inventory Node	W2K8-Base
Repositories	sample
Type	Windows Share (CIFS)
Location	\\swsys-63\sample\
Retention Policy	Retain 7 savepoints
Space Saving Technology	None (Only full backups will be performed)
Recurrence Schedule	Scheduled
Frequency	Occurs every day effective 5/7/2013 at 12:29 AM
Transport Selection	Automatic
Option Flags	2 options set
Enable Active Block Mapping (ABM)	
Enable Cataloging	

Run the job after Finish is clicked.

< Back Finish Cancel



3 DR Native Replication Setup & Restore from Target Container

3.1 Build Replication Relationship between DRs

1. Create a source container on source DR

The screenshot shows the Dell DR4100-VM web interface. The left sidebar contains a navigation menu with categories: Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Schedules, System Configuration, and Support. The 'Containers' section is selected. The main area displays a table of containers for the source DR. The table has columns: Containers, Files, NFS, CIFS, RDA, Replication, and Select. The 'rep-source' container is highlighted with a red border.

Containers	Files	NFS	CIFS	RDA	Replication	Select
backup	2	✓	✓		Not Configured	○
cifs1	6		✓		Not Configured	○
cifs11	0		✓		Not Configured	○
kknfs	0	✓			Not Configured	○
nbu-cifs-01	14		✓		Not Configured	○
nvbu	7	✓	✓		Stopped	○
nvbu1	7		✓		Online	○
nw-cifs-01	21		✓		Not Configured	○
rep-source	0		✓		Not Configured	○
sample	12		✓		Not Configured	○

2. Create a target container on target DR

The screenshot shows the Dell DR4100-VM web interface for a target DR. The left sidebar is the same as in the previous screenshot. The main area displays a table of containers for the target DR. The table has columns: Containers, Files, NFS, CIFS, RDA, Replication, and Select. The 'rep-target' container is highlighted with a red border.

Containers	Files	NFS	CIFS	RDA	Replication	Select
backup	0	✓	✓		Not Configured	○
cifs1	11		✓		Not Configured	○
cifs2	0		✓		Not Configured	○
kknfs	0	✓			Not Configured	○
kknfs2	0	✓			Not Configured	○
nfs-01	0	✓			Not Configured	○
nfs1	0	✓			Not Configured	○
nw-cifs-01	9		✓		Not Configured	○
rep-target	0		✓		Not Configured	○
sample	7		✓		Not Configured	○



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

The screenshot shows the Dell DR4100-VM web interface. The top navigation bar includes the Dell logo, 'DR4100-VM', and user information 'administrator (Log out) | Help'. A left sidebar contains a menu with categories like Global View, Dashboard, Storage, Schedules, System Configuration, and Support. The 'Replication' menu item is highlighted with a red box. The main content area is titled 'Replication' and features a 'Create' button (also highlighted with a red box) and action links for 'Edit', 'Delete', 'Stop', 'Start', 'Bandwidth', and 'Display Statistics'. Below this, it states 'Number of Source Replications: 2' and displays a table:

Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nvbu	source	10.250.243.18 nvbu	Stopped	Default	<input type="radio"/>
nvbu1	source	10.250.243.18 nvbu1	Online	Default	<input type="radio"/>

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

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

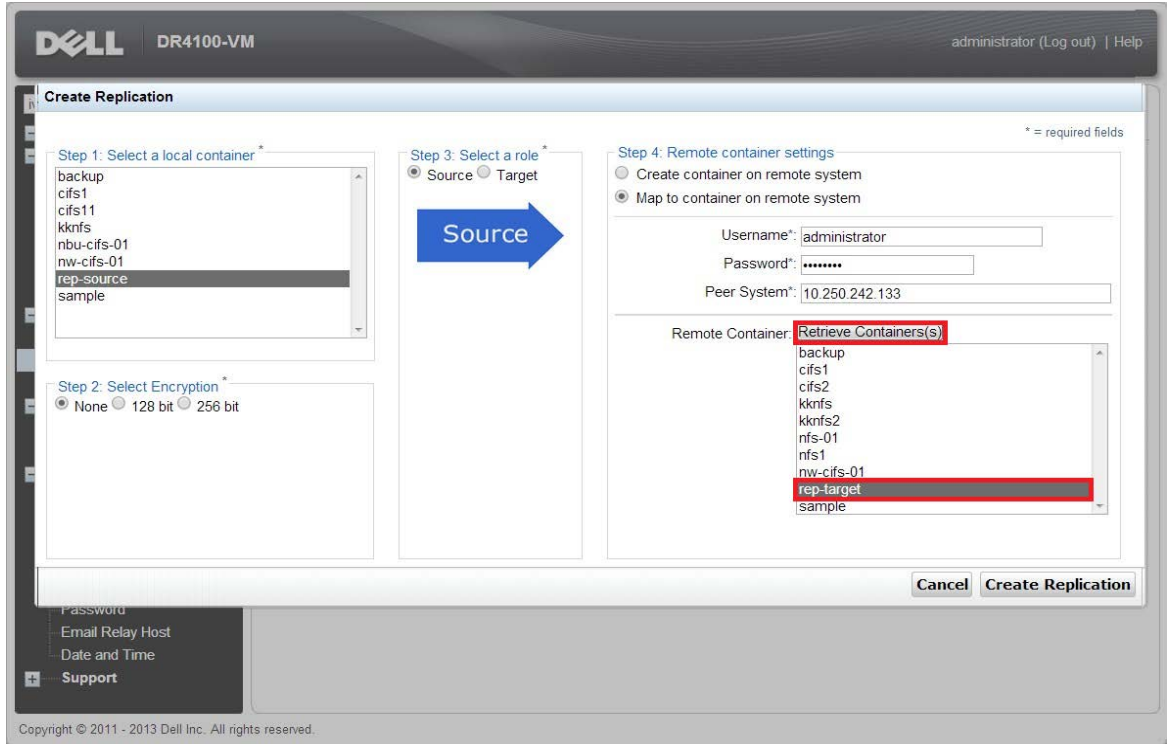
The screenshot shows the 'Create Replication' wizard in the Dell DR4100-VM web interface. The wizard is divided into four steps:

- Step 1: Select a local container ***: A list of containers is shown, with 'rep-source' highlighted by a red box.
- Step 2: Select Encryption ***: Radio buttons for 'None', '128 bit', and '256 bit' are shown, with 'None' selected.
- Step 3: Select a role ***: Radio buttons for 'Source' and 'Target' are shown, with 'Source' selected and a blue arrow pointing to the right.
- Step 4: Remote container settings ***: Radio buttons for 'Create container on remote system' and 'Map to container on remote system' are shown, with 'Map to container on remote system' selected and highlighted by a red box. Below this, there are input fields for 'Username' (administrator), 'Password' (masked with dots), and 'Peer System' (10.250.242.133). A 'Remote Container' field is also present with a dropdown menu showing 'Retrieve Containers(s)'. At the bottom right, there are 'Cancel' and 'Create Replication' buttons.

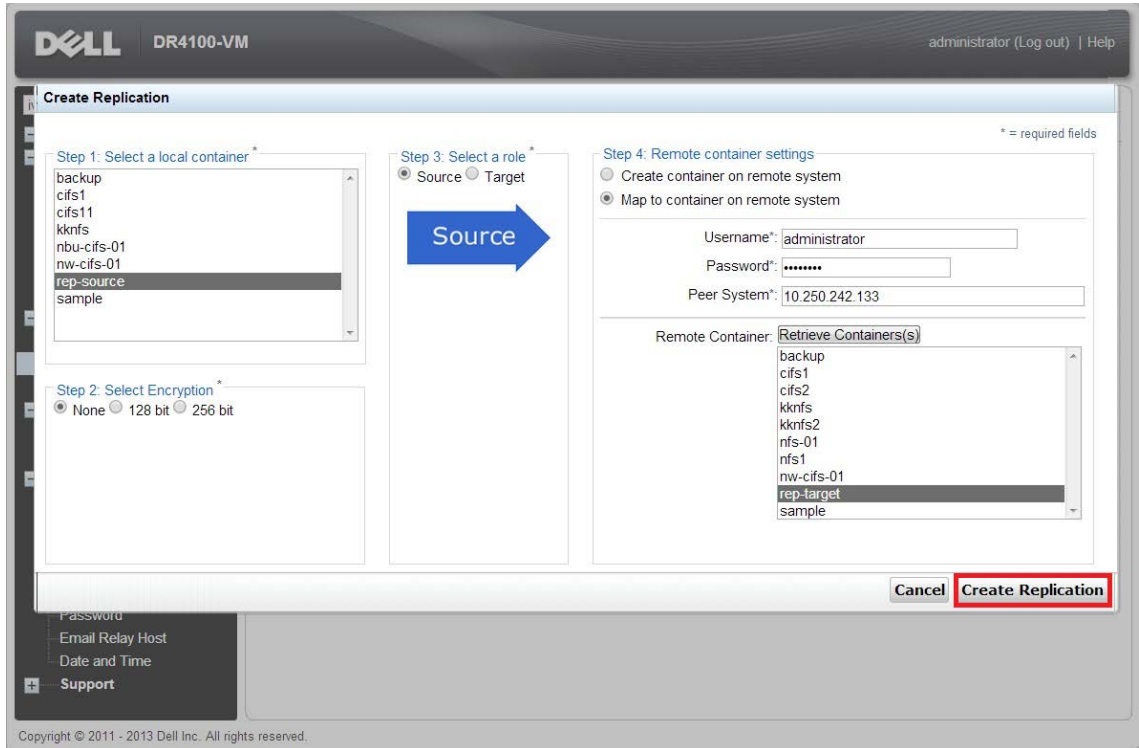
Copyright © 2011 - 2013 Dell Inc. All rights reserved.



5. Click **Retrieve Containers**, then select the target container on the list



6. Click **Create Replication**



- Verify the replication relation between DRs is created.

The screenshot shows the Dell DR4100-VM web interface. The top navigation bar includes the Dell logo, the product name 'DR4100-VM', and the user 'administrator (Log out) | Help'. The left sidebar contains a navigation menu with categories like Global View, Dashboard, Storage, Replication, Schedules, System Configuration, and Support. The main content area is titled 'Replication' and shows 'Number of Source Replications: 3'. Below this is a table with the following data:

Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nvbu	source	10.250.243.18 nvbu	Stopped	Default	<input type="radio"/>
nvbu1	source	10.250.243.18 nvbu1	Online	Default	<input type="radio"/>
rep-source	source	10.250.242.133 rep-target	Online	Default	<input checked="" type="radio"/>

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

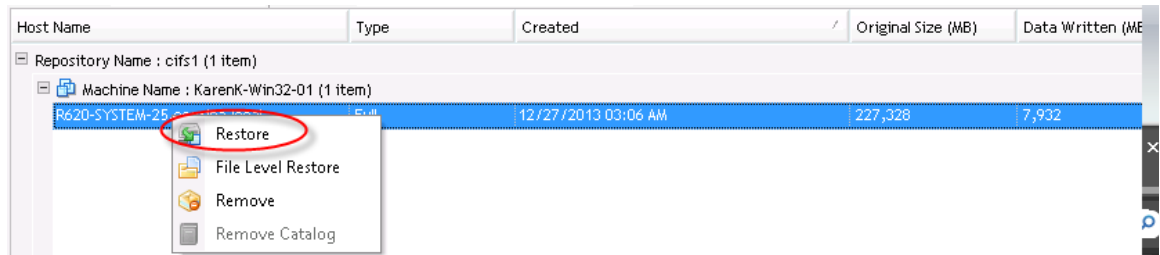
NOTE:

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.

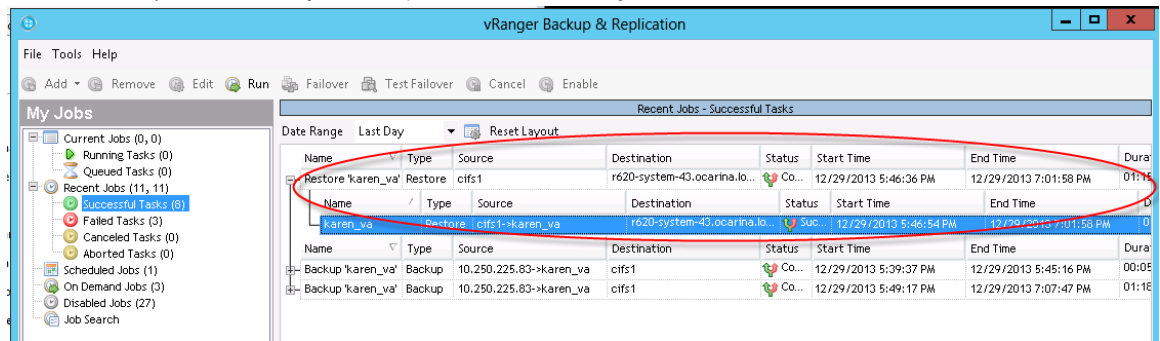


3.2 Restore data from target DR

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 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 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.

The screenshot displays the Dell DR4000 Deduplication Appliance Cleaner configuration interface. The top header shows the Dell logo, model numbers (DR4000, DR4000-DKCV6S1), and 'Help | Log out' links. The left sidebar menu includes categories like Dashboard, Alerts, Events, Health, Usage, Statistics, Storage, Schedule, Replication, Cleaner (highlighted), System Configuration, and Support. The main content area is titled 'Cleaner Schedule' and shows the system time zone as 'US/Central, Mon Jan 23 15:18:49 2012'. A table lists the days of the week (Sun through Sat) with columns for 'Start Time' and 'Stop Time', all currently showing '--'. A red arrow points to a 'Schedule Cleaner' button, and a red circle highlights a 'Schedule' link. A note at the bottom states: 'Note: When no schedule is set, the cleaner will run as needed.'

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

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.

