



Setting Up the Dell™ DR Series System as a CIFS Backup Target on EMC Networker

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.....	4
2 Configure the Networker Storage Node	11
3 Set up Networker	13
4 Set up DR Native Replication & Restore from Replication Target	25
4.1 Create Replication Session between Two DR Appliances.....	25
4.2 Restore from Replication Target Container	29
5 Set up the DR Series Deduplication Appliance Cleaner.....	33
6 Monitoring Dedupe, Compression & Performance.....	34



Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for EMC NetWorker™ software. This document is a quick reference guide and does not include all DR Series system deployment best practices.

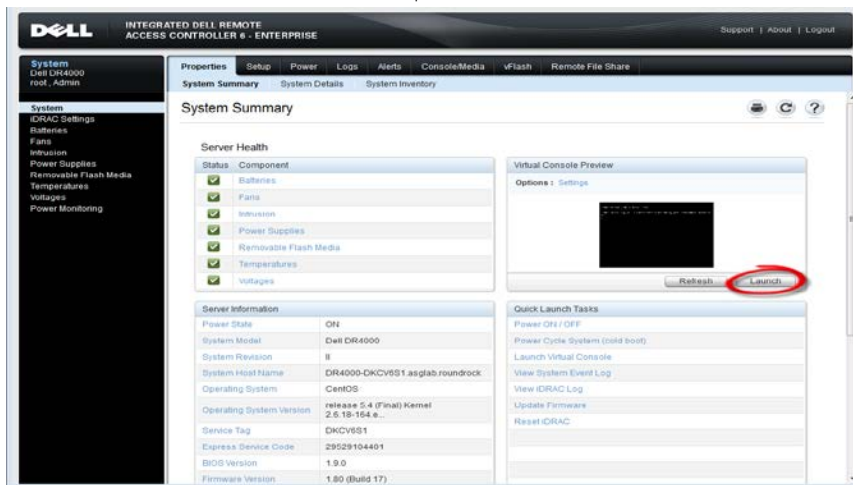
For additional data management application (DMA) best practice whitepapers, see the DR Series system documentation at <http://www.dell.com/support/Manuals/us/en/19/Product/powervault-dr4100>.

Note: The DR Series system and NetWorker screenshots used in this document may vary slightly, depending on the DR Series system firmware version and NetWorker version used.

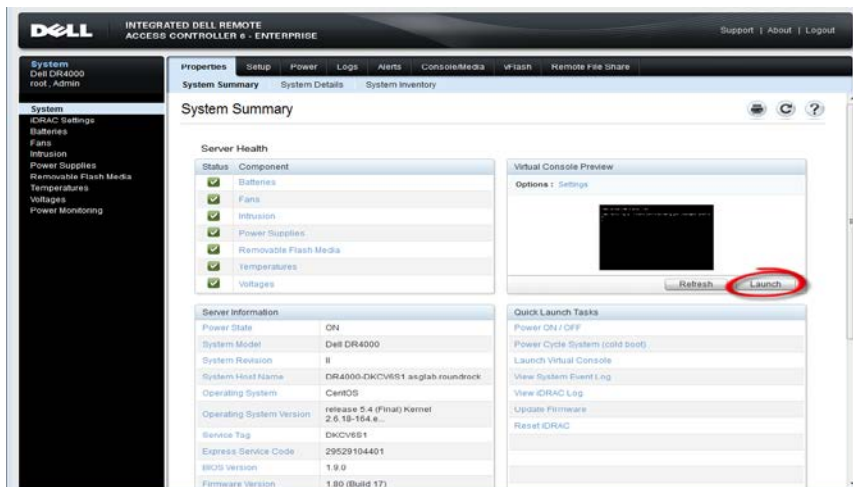


1 Install and configure the DR system

1. Rack and cable the DR Series system and power it on.
2. Initialize the DR Series system. Refer to the *Dell DR Series System Administrator Guide* under the following topics: "iDRAC Connection," "Logging in and Initializing the DR Series System," and "Accessing iDRAC6/iDRAC7 Using RACADM".
3. Log in to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use the user name and password of "**root/calvin**".



4. Launch the virtual console.



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

```
Dearina 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:
```

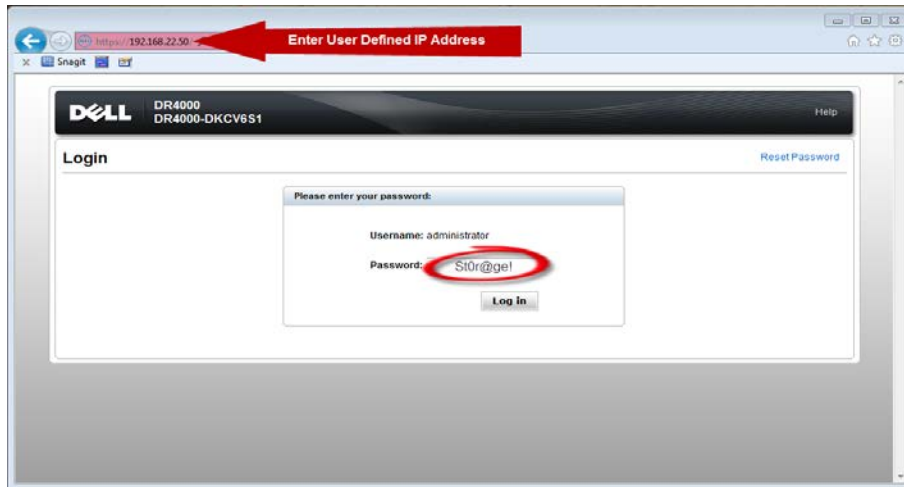
7. View the summary of preferences and confirm that it is correct.

```
=====
                          Set Static IP Address
IP Address      : 10.10.86.100
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) ? _
```



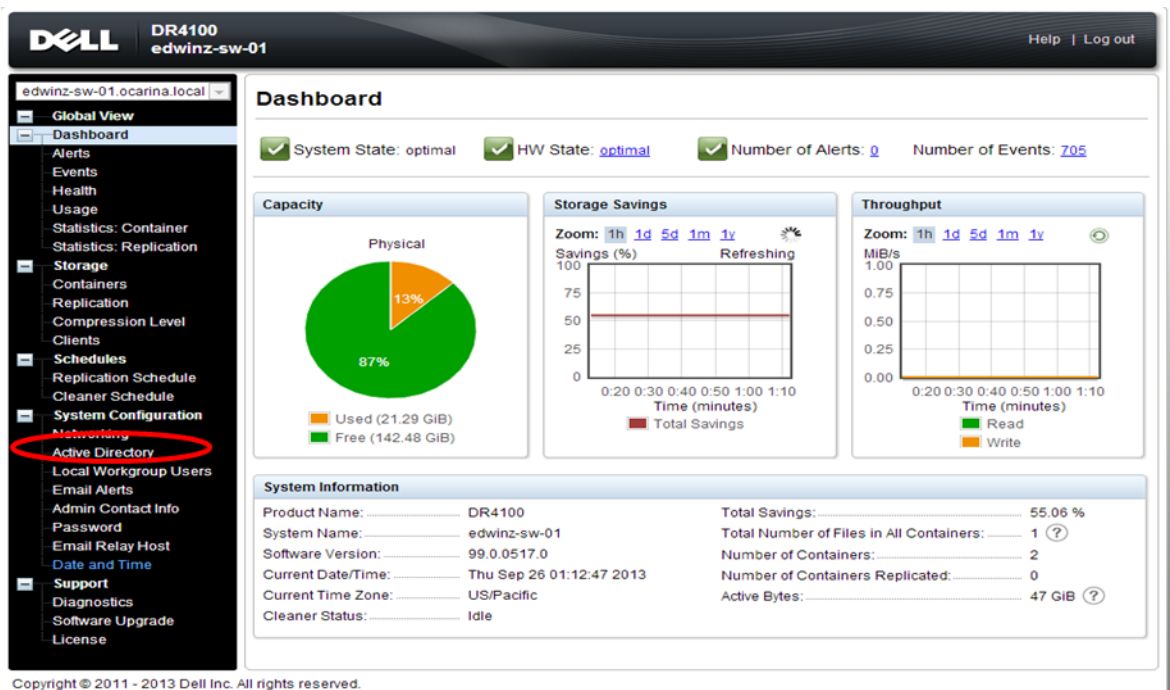
8. Log on to the DR Series system administrator console using the IP address you just provided for the DR Series system, the username **administrator**, and the password **St0r@ge!** (the "0" in the password is the numeral zero).



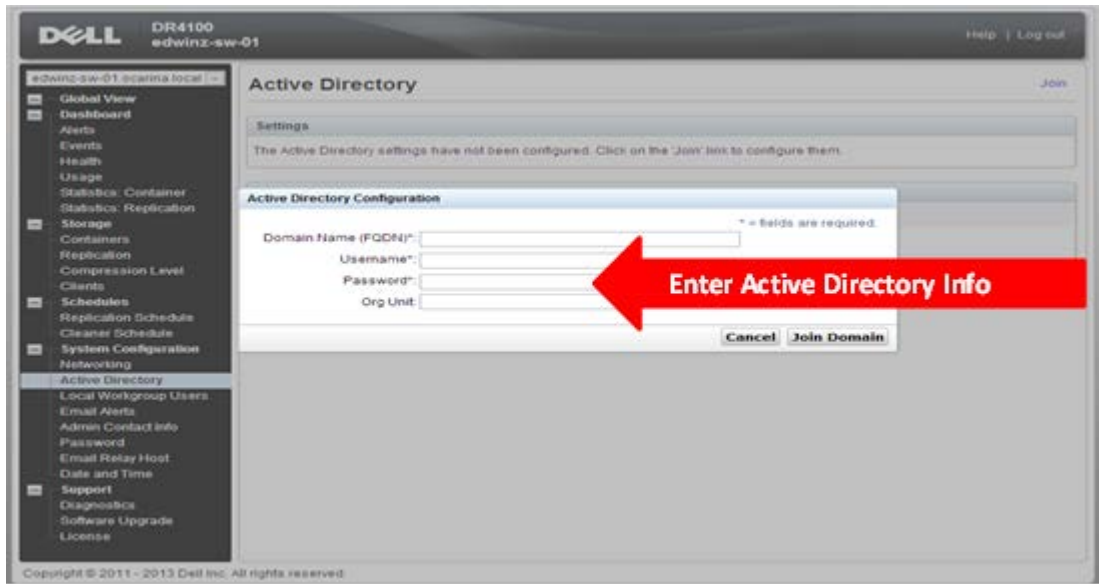
9. Join the DR Series system to Active Directory.

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

- a. Select **Active Directory** from the navigation panel on the left side of the management interface (also known as the dashboard).

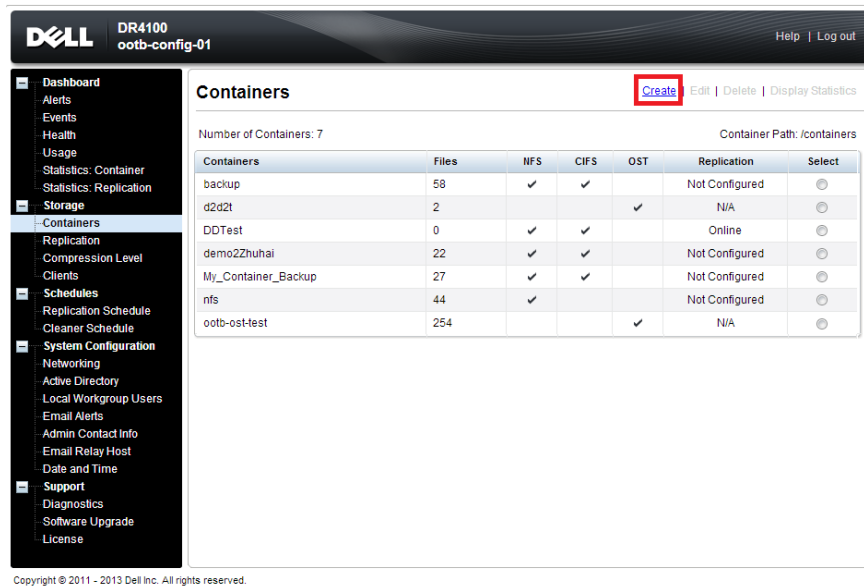


b. Enter your Active Directory credentials.



10. Create and mount the container.

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



- b. Enter a **Container Name**, select **Networker** as **Marker Type**, and select the **NFS/CIFS** check box for **Connection Type**.

Create New Container:

Choose the type of container to create ((NFS and/or CIFS) or OST) and add clients that need access. * = required fields

Container Name*: Max 32 characters and only letters, numbers, - and _ characters.

Marker Type*: None Auto CommVault Networker TSM ARCserve

Connection Type*: None NFS/CIFS OST

NFS

NFS access path:
10.250.242.206/containers/My_Container_Backup

Use NFS to backup UNIX or LINUX clients.

 Enable NFS

CIFS

CIFS share path: \\10.250.242.206\My_Container_Backup

Use CIFS to backup MS Windows clients.

 Enable CIFS

- c. Under **CIFS** section, note down the **CIFS share path** (this will be used in configuring device on Networker server), and select **Enable CIFS**. For **Client Access** section, choose either **Open Access** or manually add clients into the allow list

Create New Container:

Choose the type of container to create ((NFS and/or CIFS) or OST) and add clients that need access. * = required fields

Container Name*: Max 32 characters and only letters, numbers, - and _ characters.

Marker Type*: None Auto CommVault Networker TSM ARCserve

Connection Type*: None NFS/CIFS OST

NFS

NFS access path:
10.250.242.206/containers/My_Container_Backup

Use NFS to backup UNIX or LINUX clients.

 Enable NFS

CIFS

CIFS share path: \\10.250.242.206\My_Container_Backup

Use CIFS to backup MS Windows clients.

 Enable CIFS

Client Access:

 Open Access (all clients have access)

Add clients (IP or FQDN Hostname)

Clients:



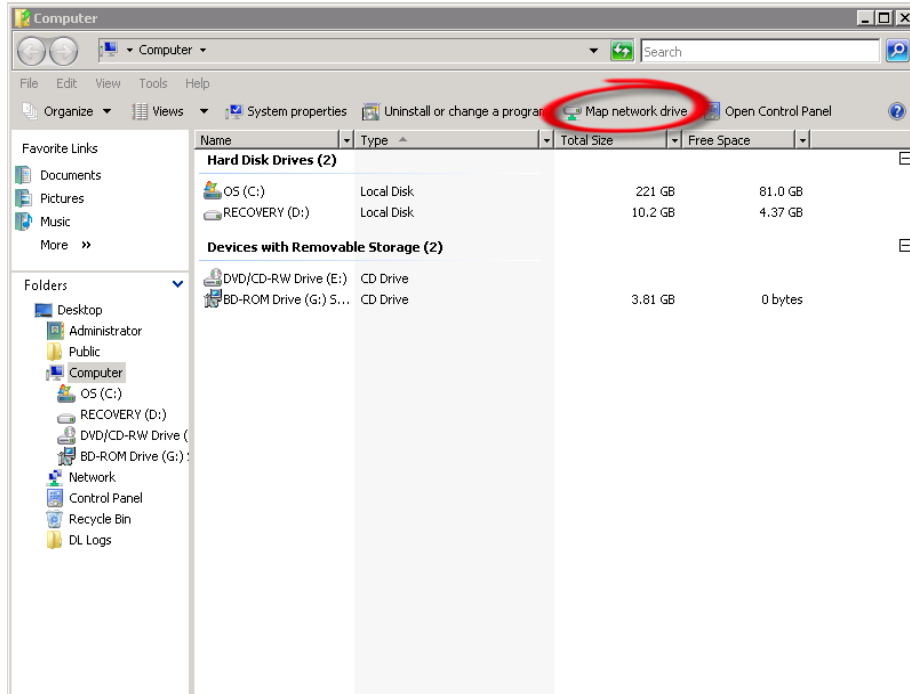
Note: For improved security, Dell recommends adding IP addresses for the backup console (Networker Server), Networker storage nodes, and Networker clients. (Not all environments will have all components.)

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

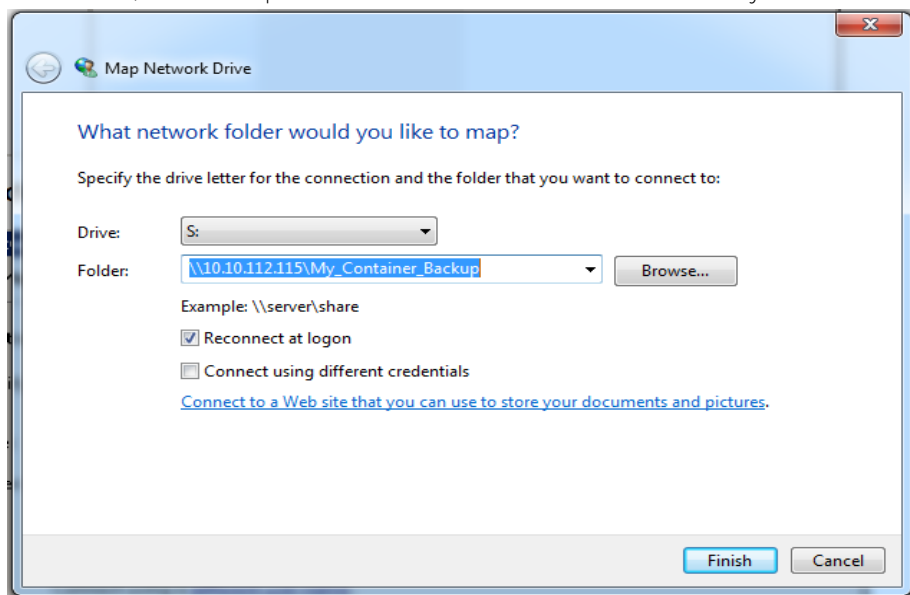


2 Configure the Networker storage node

1. Log into the storage node and click **Start→My Computer**.
2. Click **Map network drive**.



3. For **Folder**, enter the path to the container on the DR Series system.



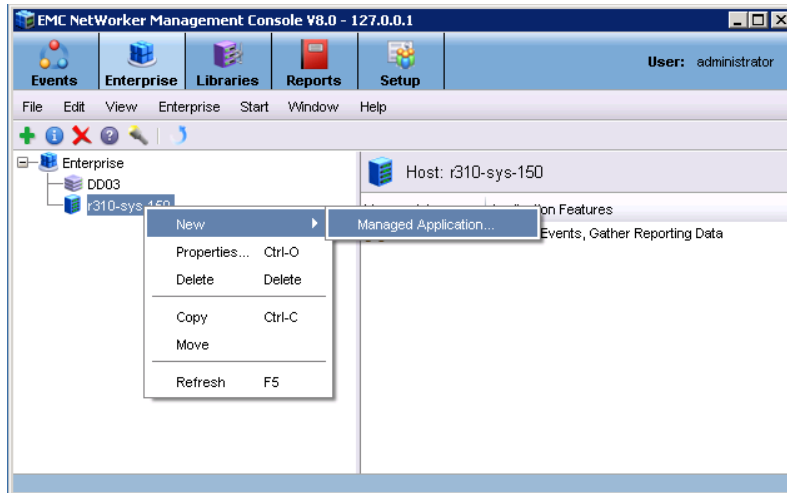
4. Select the **Reconnect at logon** checkbox.
5. When prompted, enter the CIFS credential to authenticate on the Active Directory domain. The DR Series system container is now mounted to your backup server.
6. If Client Direct will be used, make sure all of the clients can access the same DR container share using this path. Otherwise separate **Client Direct Paths** will need to be filled in with the actual paths that clients use to access the DR container share (please refer to step 10 in the next section **Set up Networker**)

Note: On DR4x00 systems, the maximum supported CIFS connections per appliance is 32; on the DR6000 system the maximum is 64. Therefore, there should not be more than 32 and 64 corresponding clients connected/mapped to a single DR Series system for backup at the same time. For details, see the *Dell DR Series System Interoperability Guide*.

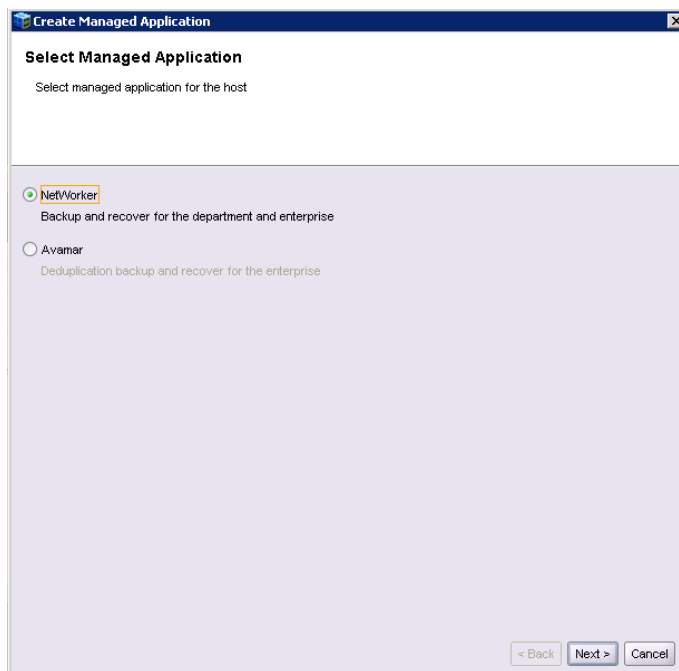


3 Set up Networker

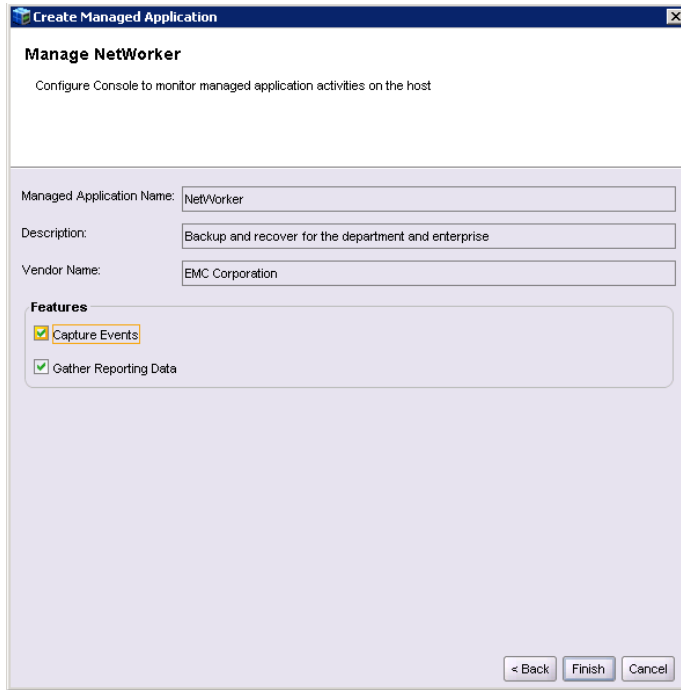
1. Open the **Networker Management Console (NMC)**.
2. Click the **Enterprise** menu button, select the storage node that the DR Series system share will be configured as a backup device, right-click on the host and click **New > Managed Application**.



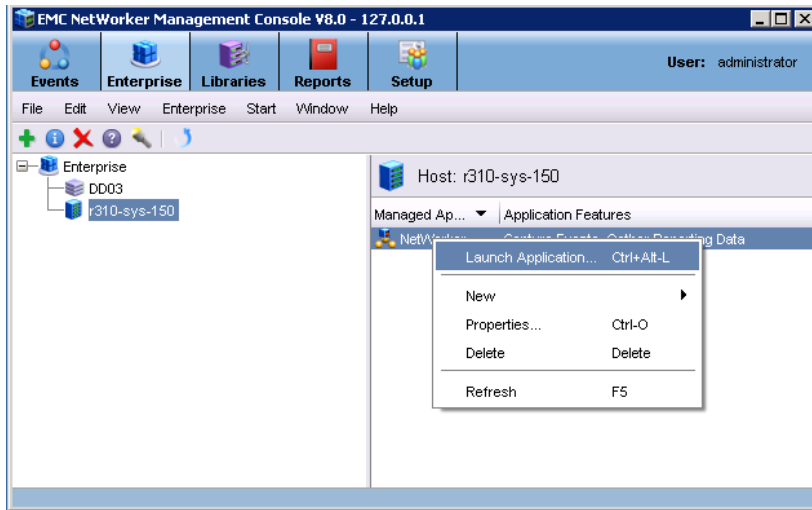
3. Select **Networker** and click **Next**.



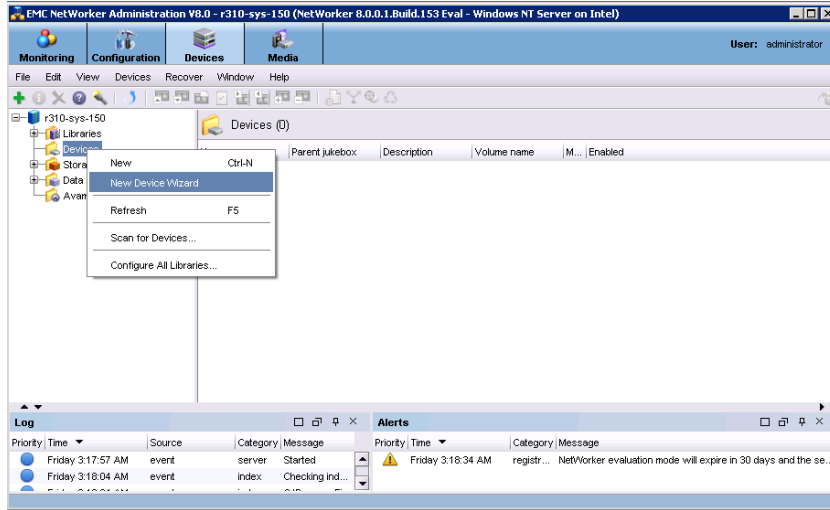
4. Click **Finish**.



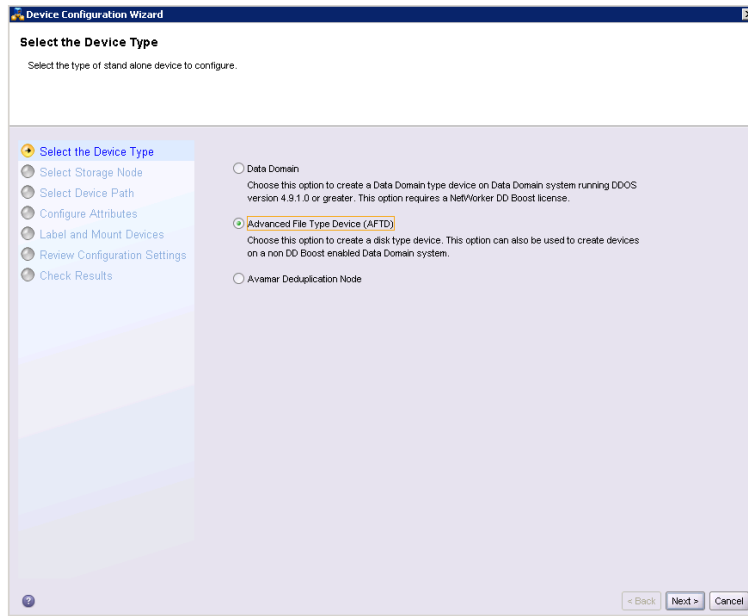
5. Select the newly created NetWorker application, right-click on the application, and click **Launch Application**.



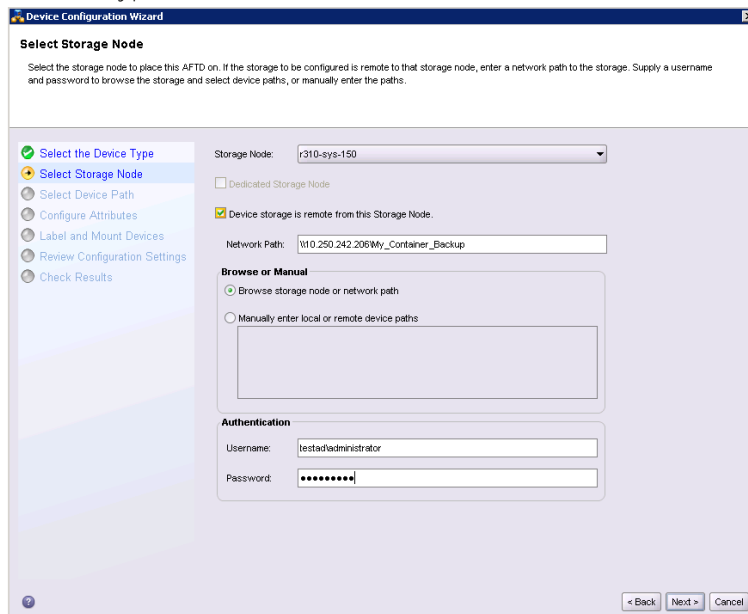
6. In the Devices window, right-click **Device** in the left panel and click **New Device Wizard**.



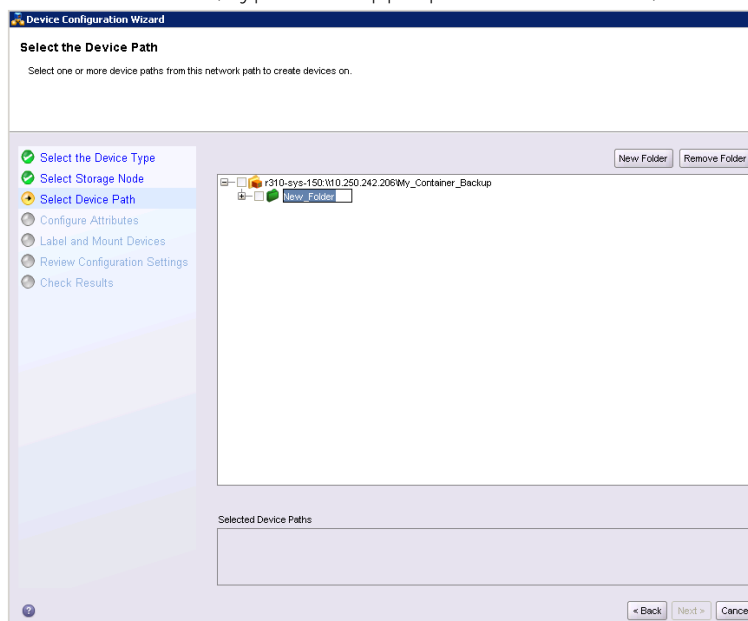
7. Select **Advanced File Type Device (AFTD)**.

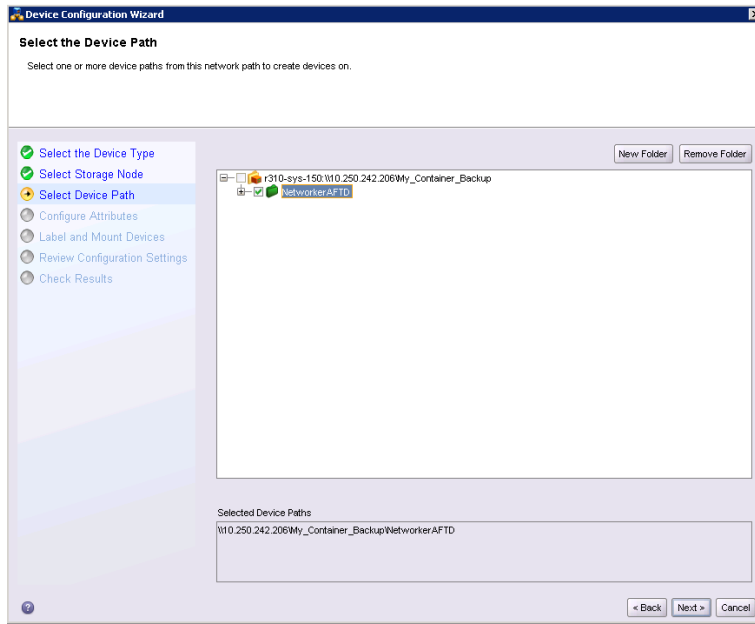


8. In the next dialog box, select **Device storage is remote from this Storage Node**, type in the network path of the DR Series system container share location (if name resolution works, the hostname or FQDN can be used in the server portion of the network path). In the **Authentication** section, type in the CIFS credentials to access the DR Series system share. Click **Next**.



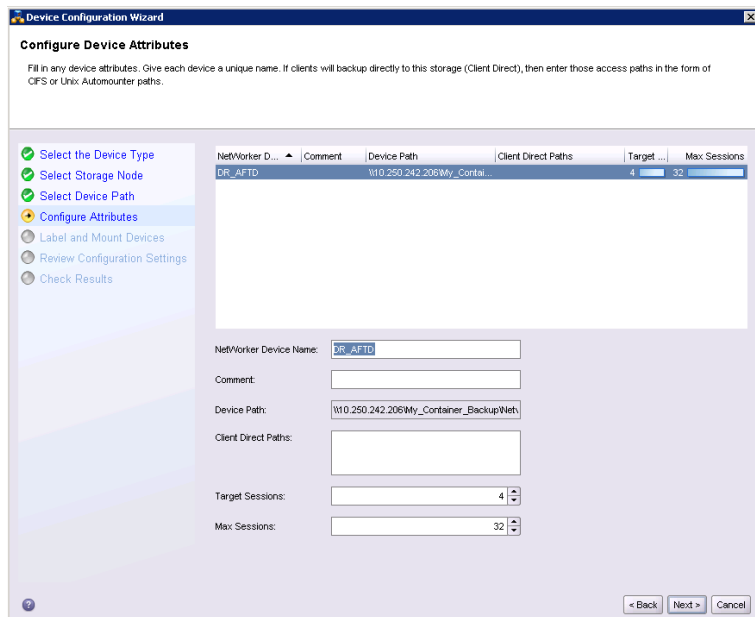
9. Click **New Folder**, type in an appropriate folder name, then select the folder and click **Next**.





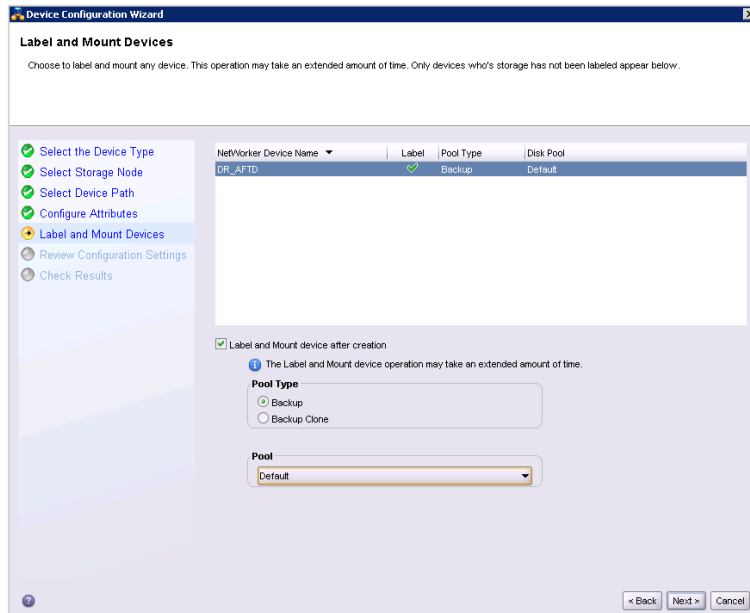
10. Set the session attributes according to the Networker administration documentation and click **Next**.

If the Client Direct feature will be used, different device path(s) that clients use to access the DR container share can be entered into the **Client Direct Paths** (please refer to step 6 in the last section **Configure Networker Storage Node**). If all of the clients are able to access the DR container share using the direct path, there is no need to enter extra client direct paths.

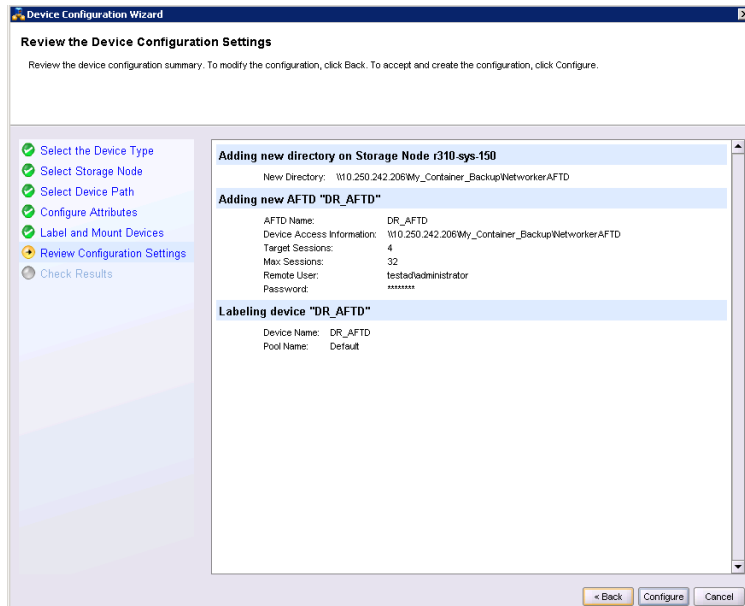


Note: On DR4x00 systems, the maximum supported CIFS connections per appliance is 32; on the DR6000 system the maximum is 64. Therefore, there should not be more than 32 and 64 corresponding clients connected/mapped to a single DR Series system for backup at the same time. For details, see the *Dell DR Series System Interoperability Guide*.

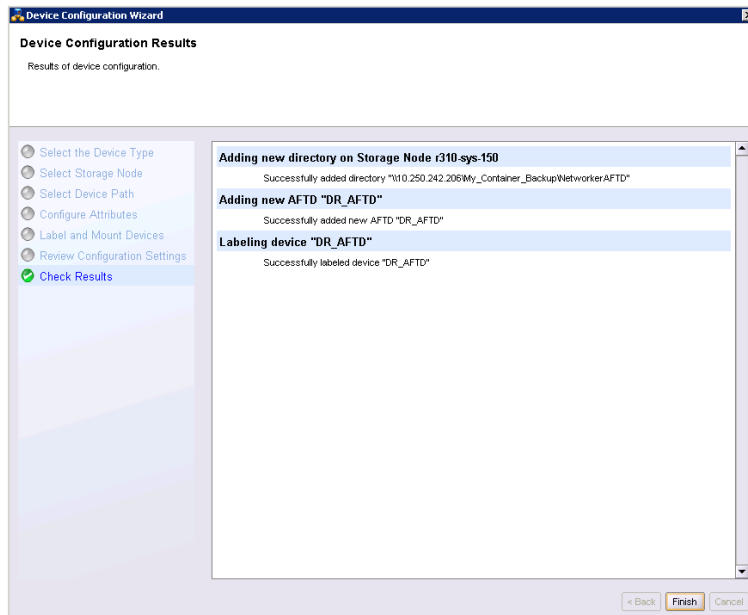
11. The new NetWorker device should have Pool Type set to **Backup**. Click **Next**.



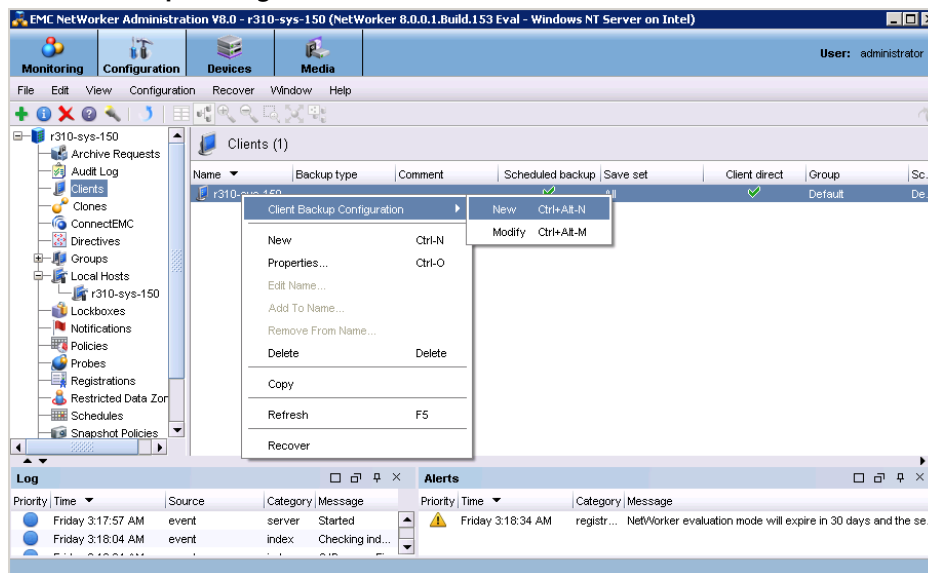
12. Review the configuration and then click **Configure**.



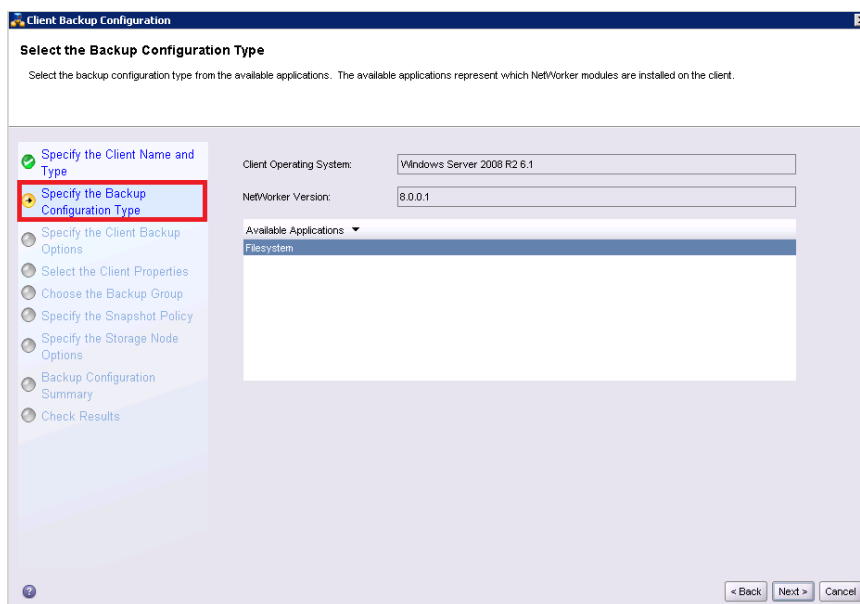
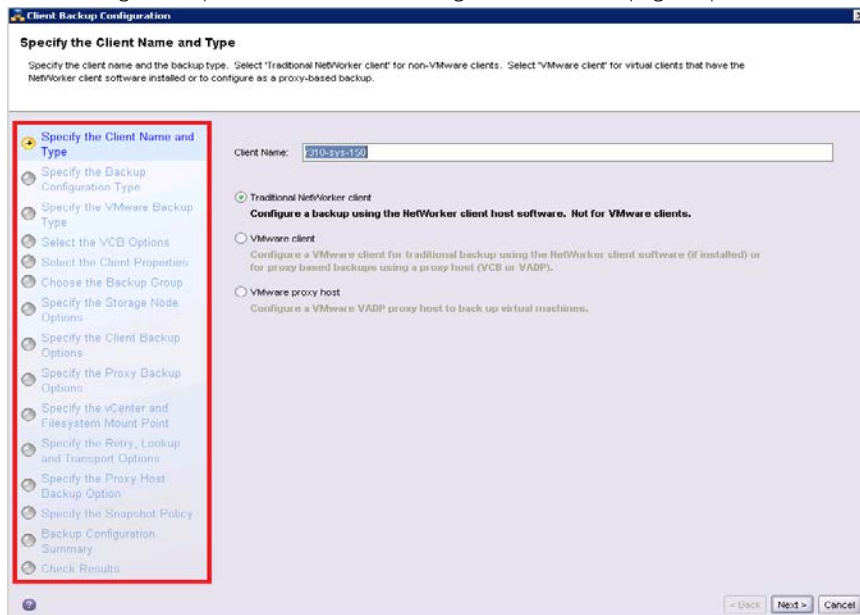
13. Click **Finish**.



14. On the **Configuration** tab, select **Clients**, right-click on the client that will be backed up, select **Client Backup Configuration**, and then click **New**.



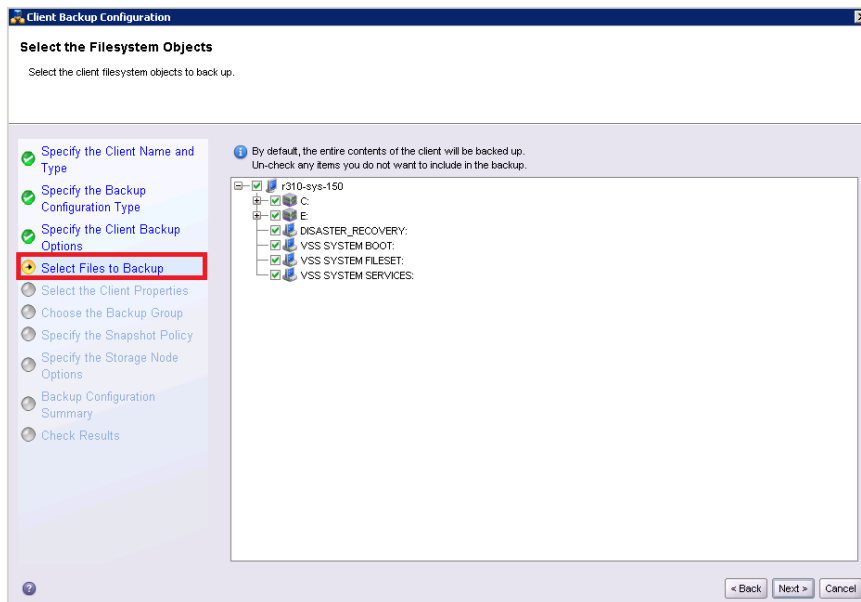
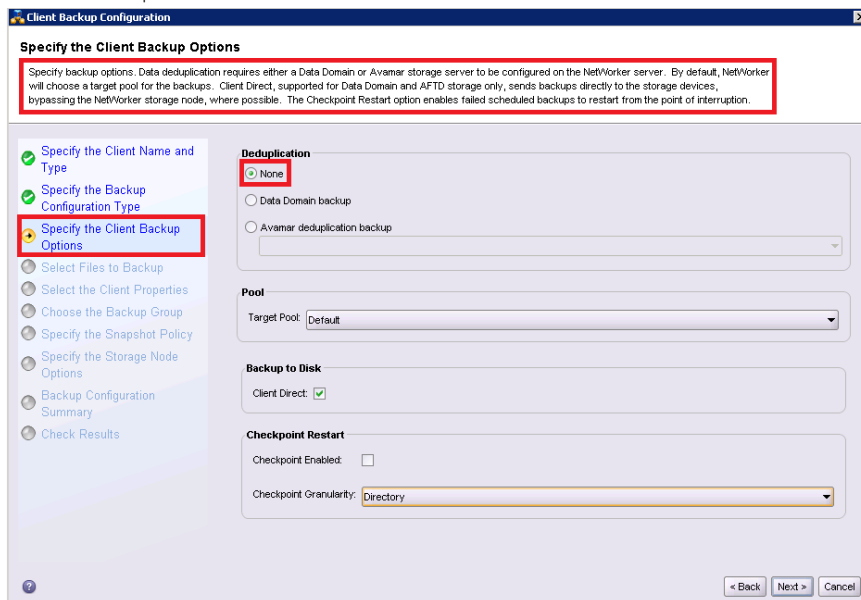
15. Go through the procedure of creating a new backup group.

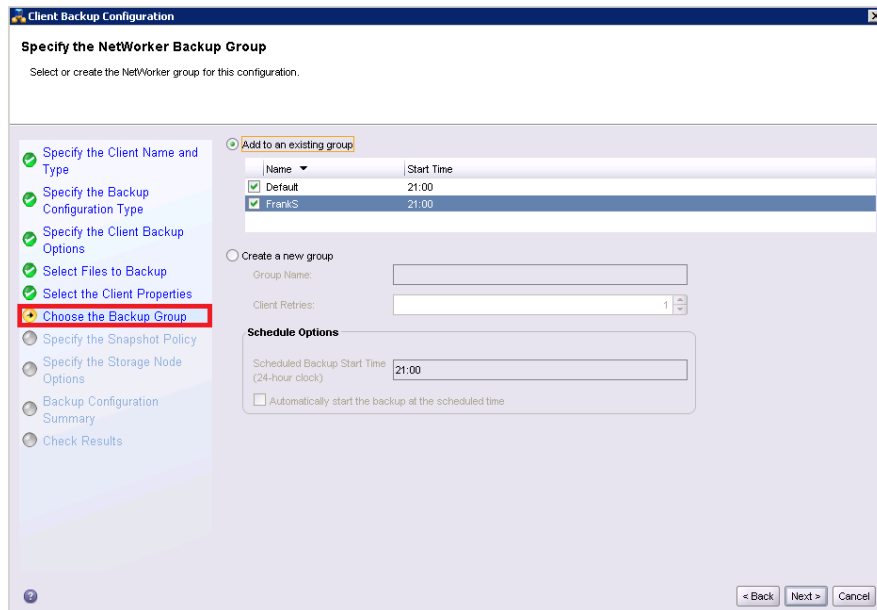
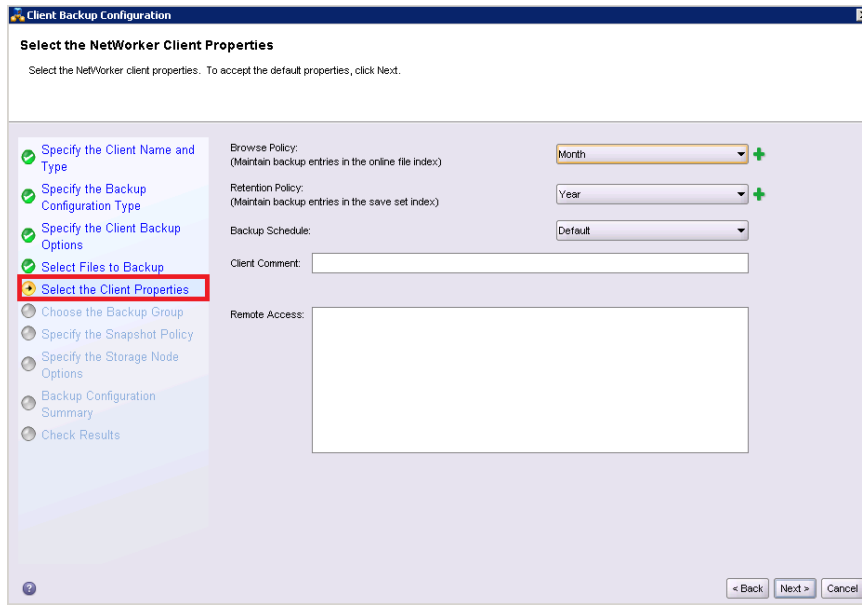


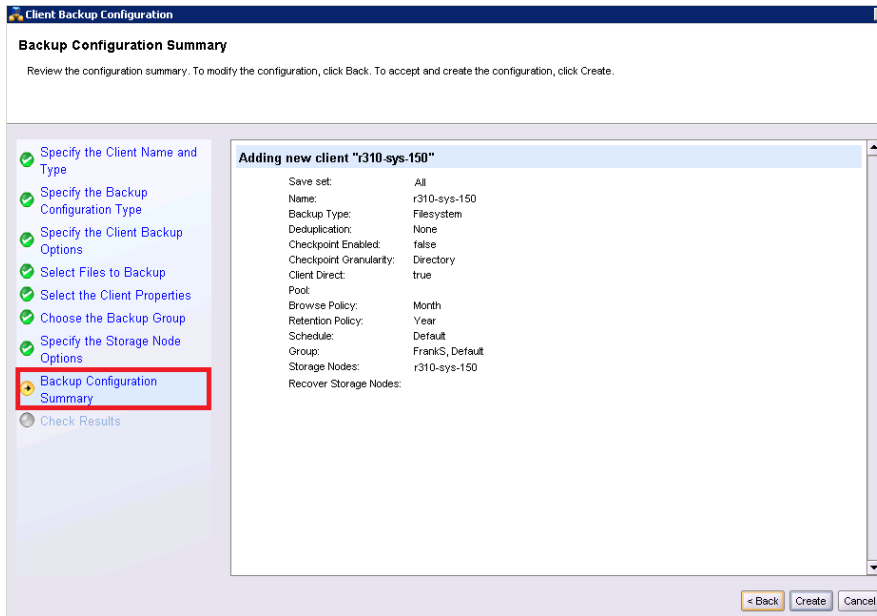
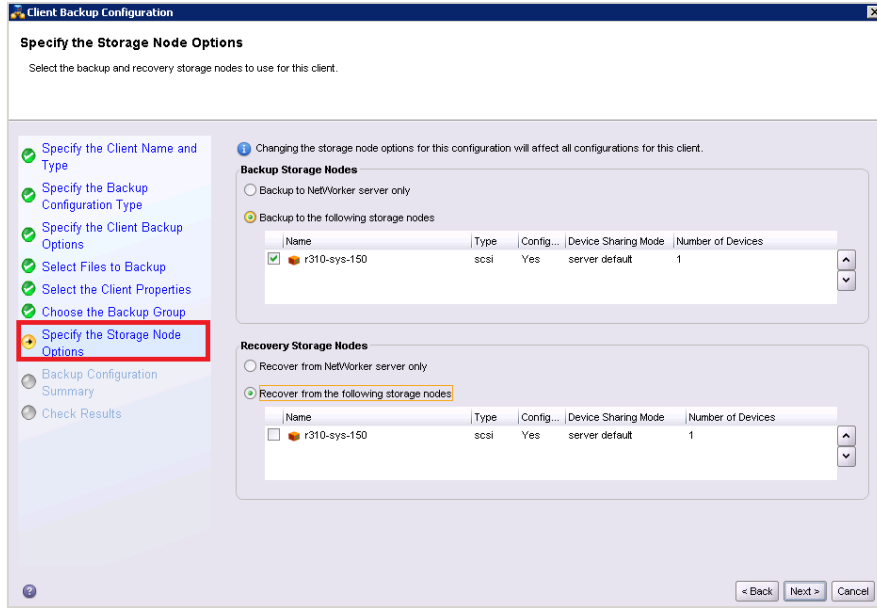
16. In Specify the Client Backup Options, pay special attention to the following settings:
- Deduplication** should be set as **None**;
 - Target Pool** should be set as the pool that has DR Series Deduplication Appliance device included;
 - Client Direct** can be enabled if client directly backing up data to DR is preferred, thus bypassing the storage node managing the DR share. For **Client Direct** to work, the DR device must have at least one device path that the client can use to directly access the DR container



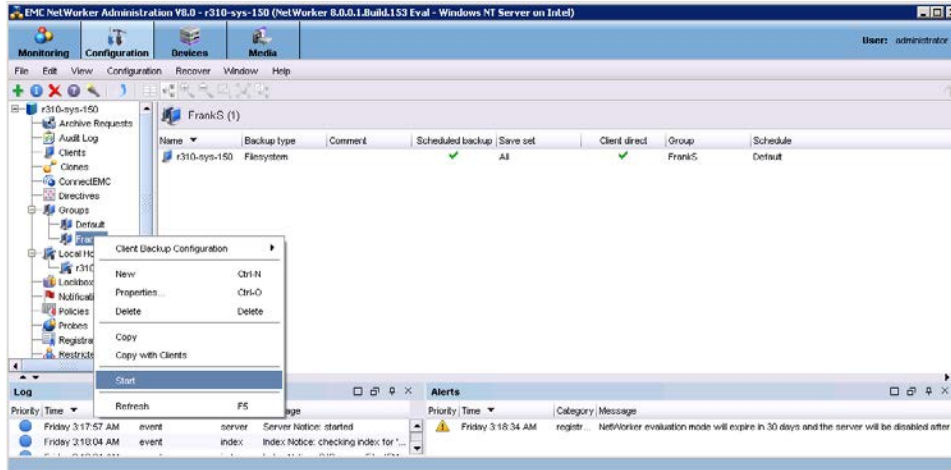
share with (please refer to step 6 in the last section **Configure the Networker Storage Node**, and step 10 in this section).



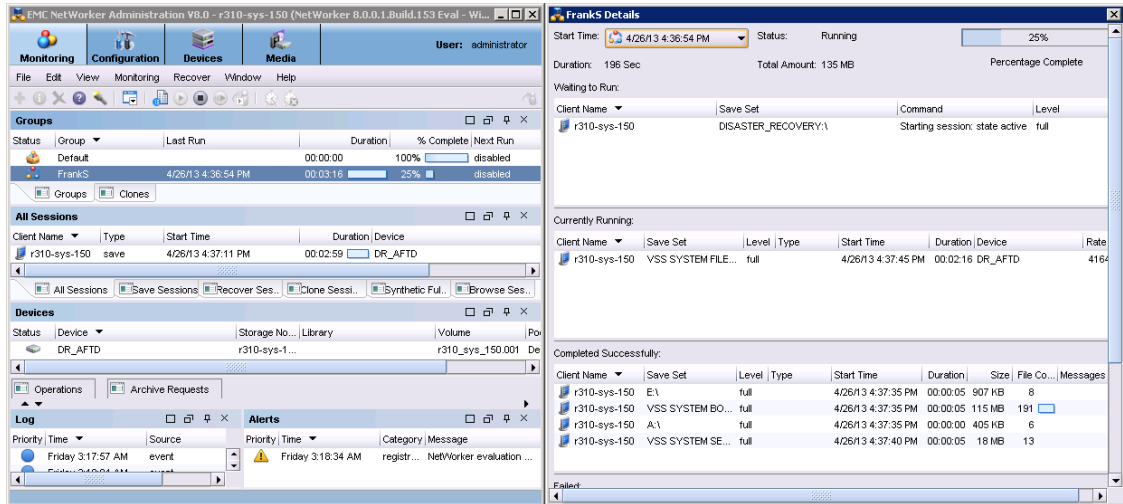




17. After the backup group is successfully created, start the backup.



18. Monitor the job status through the **Monitoring** tab.



4 Set up the DR replication and restore from the replication target

4.1 Create a replication relationship between two DR systems

1. Create a source container on the source DR system.

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 content area displays a table of containers with columns: Containers, Files, NFS, CIFS, RDA, Replication, and Select. The 'rep-source' container is highlighted in red. Below the table, the text 'Copyright © 2011 - 2013 Dell Inc. All rights reserved.' is visible.

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 the target DR system.

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 content area displays a table of containers with columns: Containers, Files, NFS, CIFS, RDA, Replication, and Select. The 'rep-target' container is highlighted in red. Below the table, the text 'Copyright © 2011 - 2013 Dell Inc. All rights reserved.' is visible.

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 the source DR system, go to the **Replication** menu and then click **Create**.

The screenshot shows the Dell DR4100-VM web interface. The left sidebar contains a navigation menu with the following items: Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, **Replication** (highlighted with a red box), Clients, Schedules, Replication Schedule, Cleaner Schedule, System Configuration, Networking, Active Directory, Local Workgroup Users, Email Alerts, Admin Contact Info, Password, Email Relay Host, Date and Time, and Support. The main content area is titled "Replication" and includes a "Create" button (highlighted with a red box) and a table of source replications.

Number of Source Replications: 2

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 newly created container as source container, and then enter the target DR information.

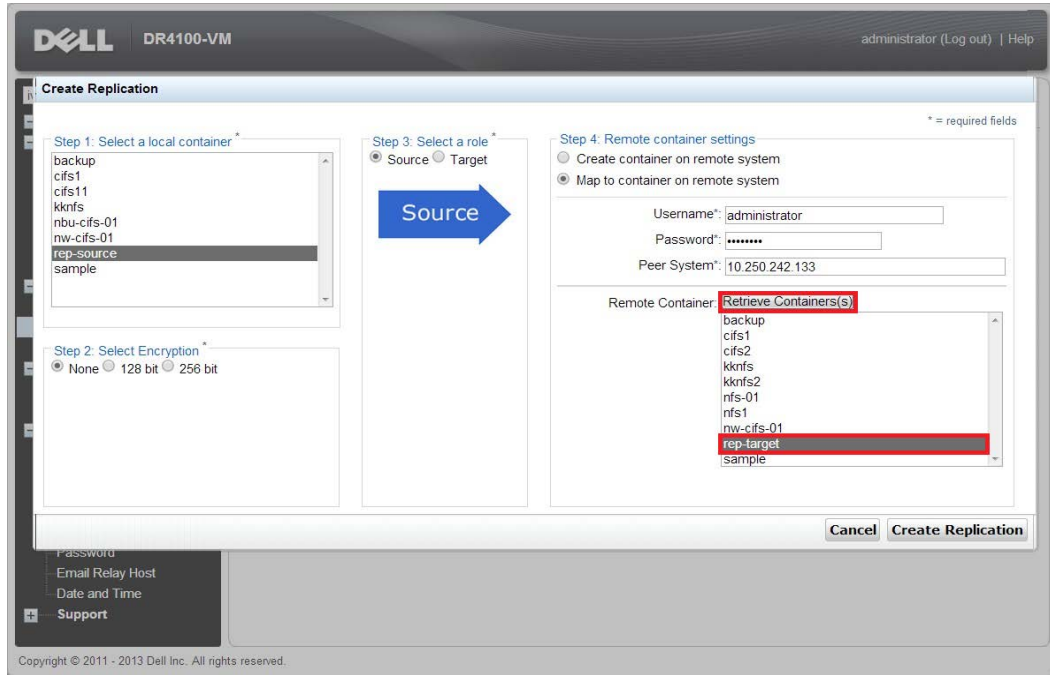
The screenshot shows the "Create Replication" wizard in the Dell DR4100-VM web interface. The wizard consists of four steps:

- 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.
- Step 3: Select a role ***: Radio buttons for "Source" (selected) and "Target" are shown, with a blue arrow pointing from "Source" to "Target".
- Step 4: Remote container settings**: Radio buttons for "Create container on remote system" and "Map to container on remote system" (selected) are shown. The "Map to container on remote system" section is highlighted with a red box and contains:
 - Username*: administrator
 - Password*: [masked]
 - Peer System*: 10.250.242.133
 - Remote Container: Retrieve Containers(s)

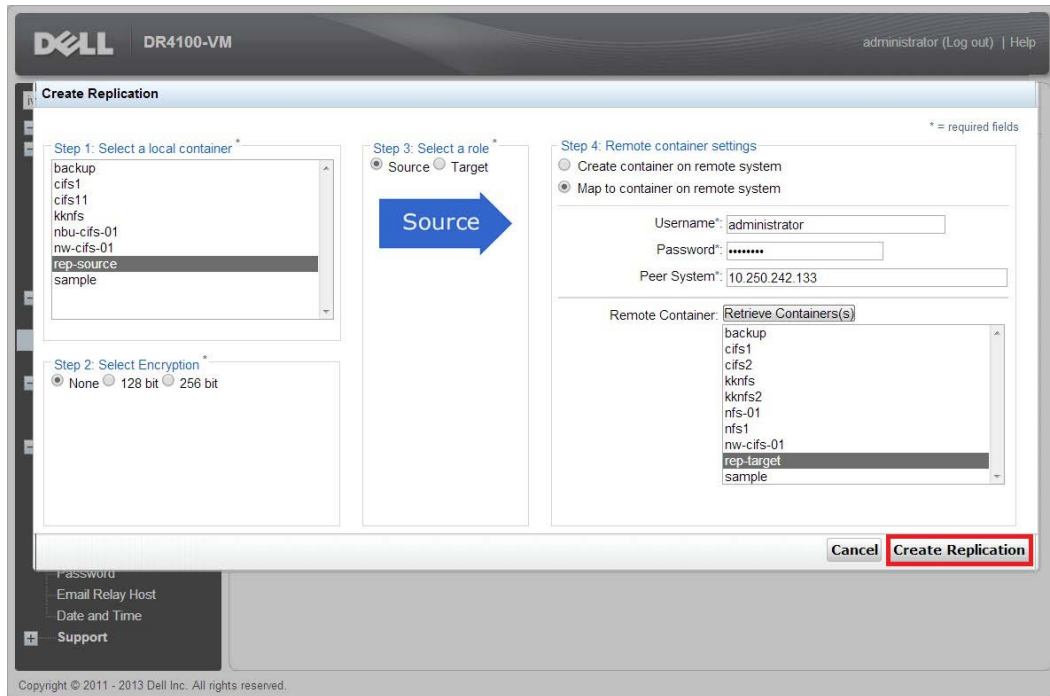
Buttons for "Cancel" and "Create Replication" are at the bottom right. The footer reads "Copyright © 2011 - 2013 Dell Inc. All rights reserved."



5. Click **Retrieve Container(s)** and then select the newly created target container from the list.



6. Click **Create Replication**.



7. Verify that the replication relationship between the DRs has been created and that the **Peer Status** is **Online**.

The screenshot shows the Dell DR4100-VM web interface. The top header includes the Dell logo, the system name 'DR4100-VM', and the user 'administrator (Log out) | Help'. A left-hand navigation menu is visible, with 'Replication' selected. The main content area is titled 'Replication' and includes a sub-header 'Number of Source Replications: 3'. Below this is a table with the following data:

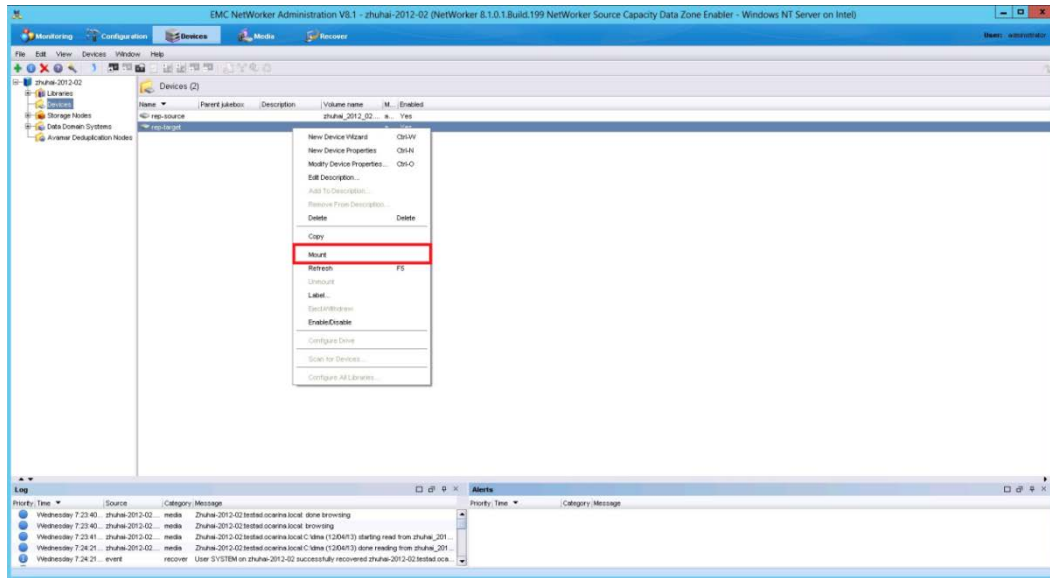
Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nvbu	source	10.250.243.18 nvbu	Stopped	Default	<input type="radio"/>
nvbu1	source	10.250.243.18 nvbu1	Online	Default	<input type="radio"/>
rep-source	source	10.250.242.133 rep-target	Online	Default	<input checked="" type="radio"/>

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



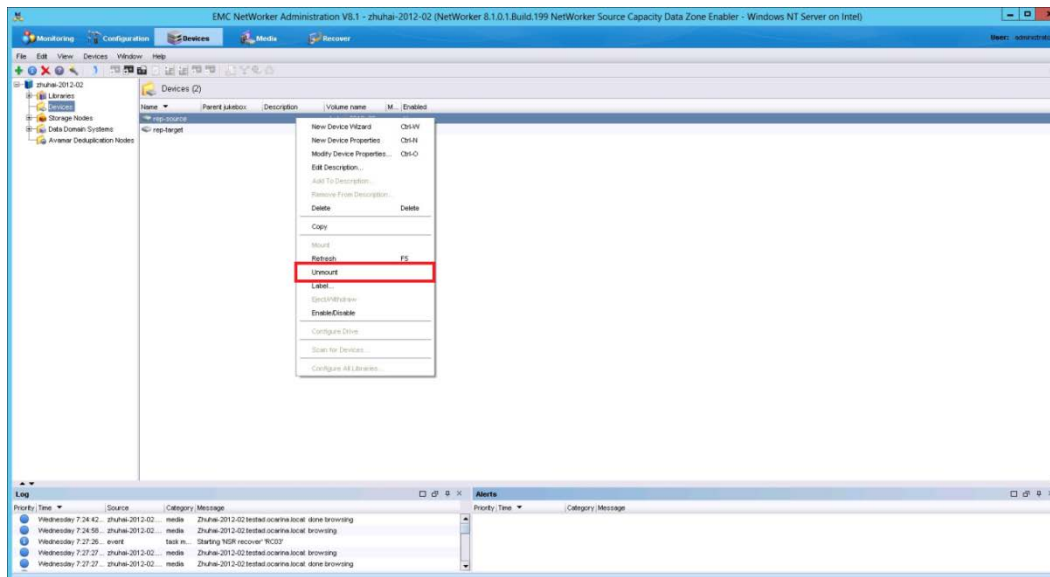
4.2 Restore from the replication target container

1. Add the target container onto the Networker storage node (right-Click **Device** -> **New Device Properties**, and then fill in necessary information for the target device). When complete, mount the device.

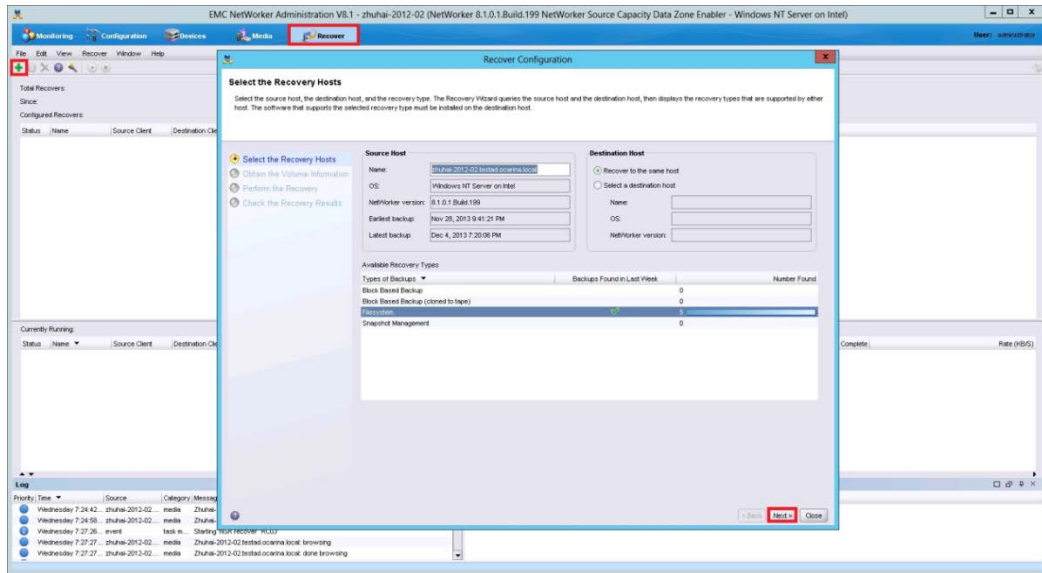


Note: Don't label the target device.

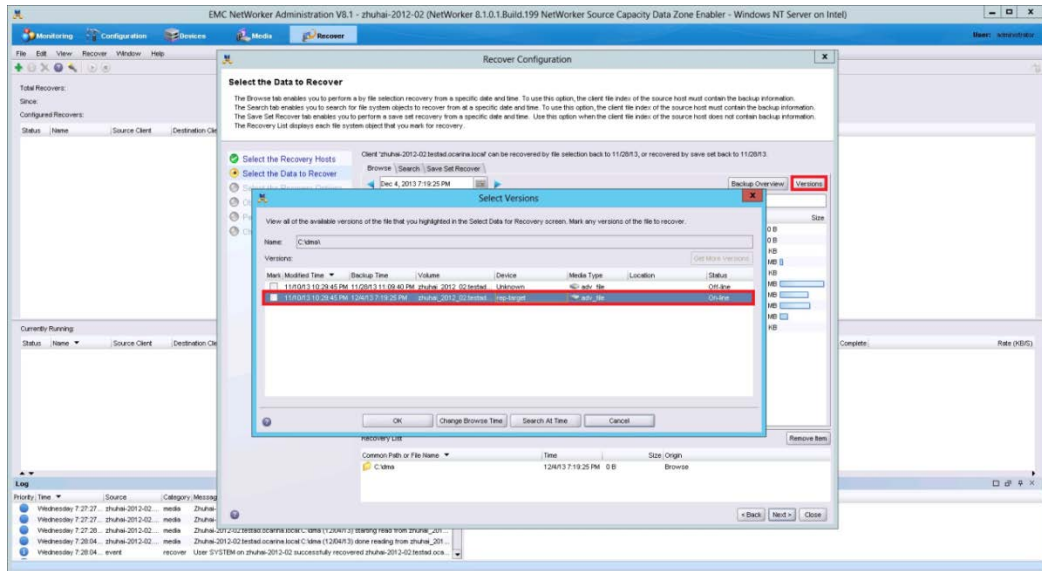
2. Unmount the source container.



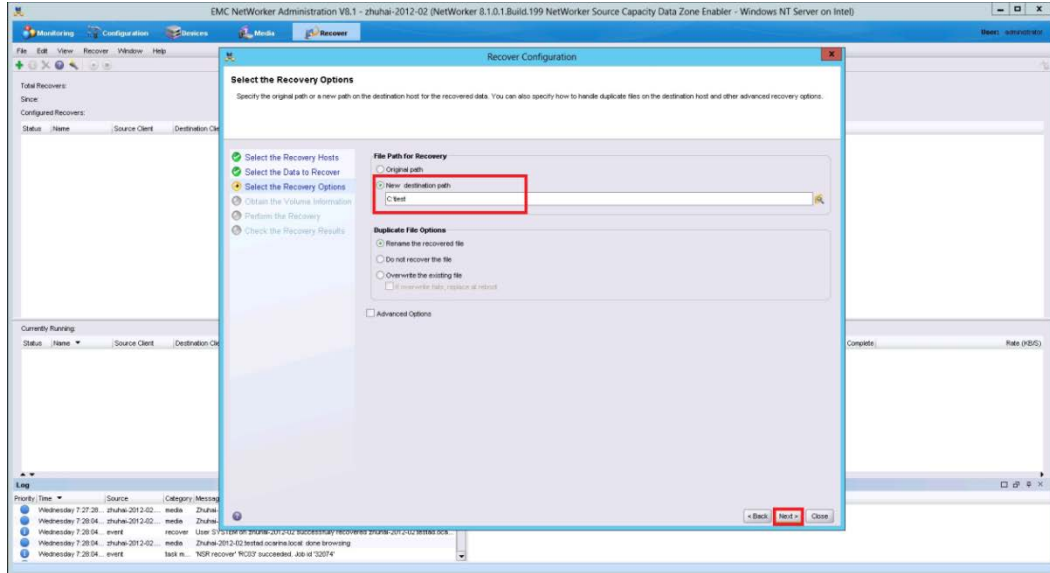
- Go to **Recover**, click **+**, select a backup source host, and then click **Next**.



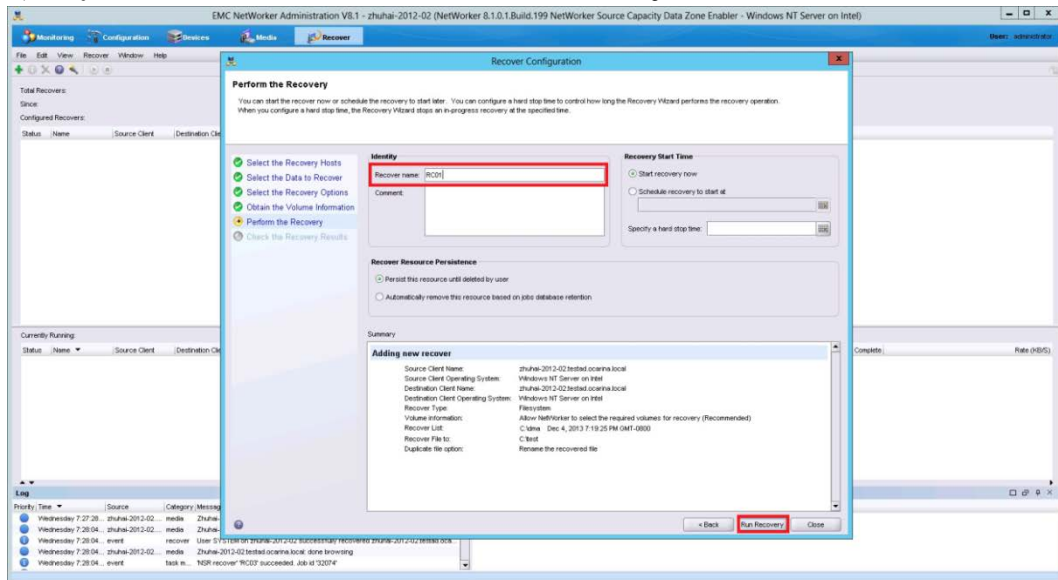
- Select the data set to recover, click **Versions** to view the **Select Versions** window, make selection on the data, and then click **OK**.



5. Select the **Recovery Options**, choose **Original path** or enter a new destination path to recover data to, and then click **Next**.



6. Specify a **Recover name**, and then click **Run Recovery**.

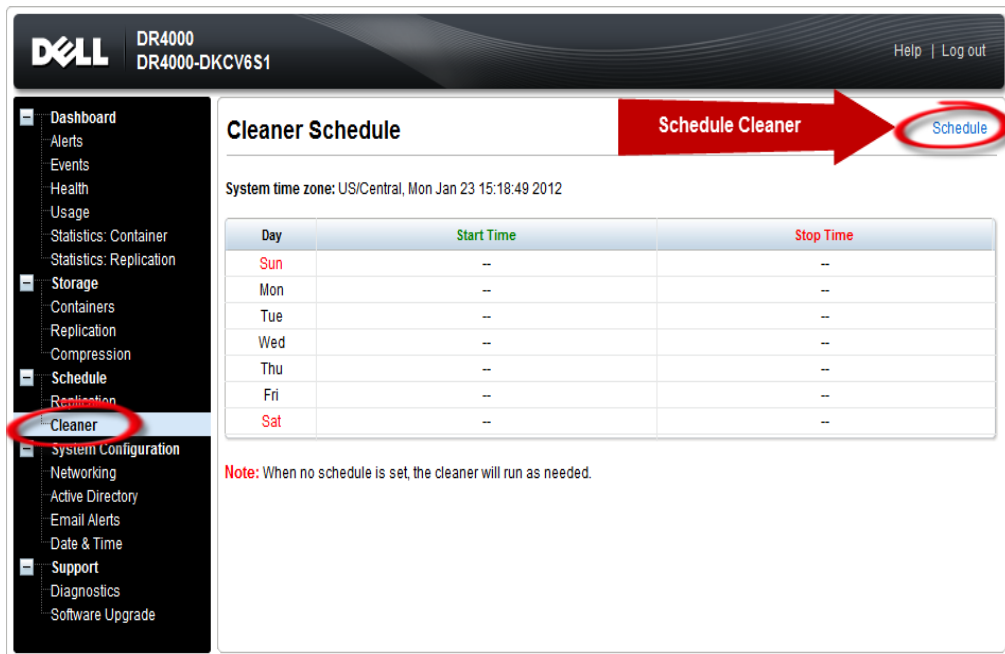


5 Set up the DR Series system cleaner

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

The 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 of the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least six hours per week when backups are not taking place, and generally after a backup job has completed.



The screenshot shows the Dell DR Series system cleaner configuration interface. The sidebar menu on the left includes options like Dashboard, Alerts, Events, Health, Usage, Statistics: Container, Statistics: Replication, Storage, Containers, Replication, Compression, Schedule, Replication, Cleaner (highlighted with a red circle), System Configuration, Networking, Active Directory, Email Alerts, Date & Time, Support, Diagnostics, and Software Upgrade. 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 displays the current schedule for the cleaner, with columns for Day, Start Time, and Stop Time. A red arrow points to a 'Schedule Cleaner' button, and a red circle highlights a 'Schedule' button.

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

Note: When no schedule is set, the cleaner will run as needed.

6 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.

