



Setting up Dell™ DR Series Deduplication Appliance as NFS 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.....	5
2 Configure the Networker Storage Node	11
3 Set up Networker	12
4 Set up DR Native Replication & Restore from Replication Target	24
4.1 Create Replication Session between Two DR Appliances.....	24
4.2 Restore from Replication Target Container	28
5 Set up the DR Series Deduplication Appliance Cleaner.....	32
6 Monitoring Dedupe, Compression & Performance.....	33



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 paper is a quick reference guide and does not include all DR Series Deduplication Appliance deployment best practices.

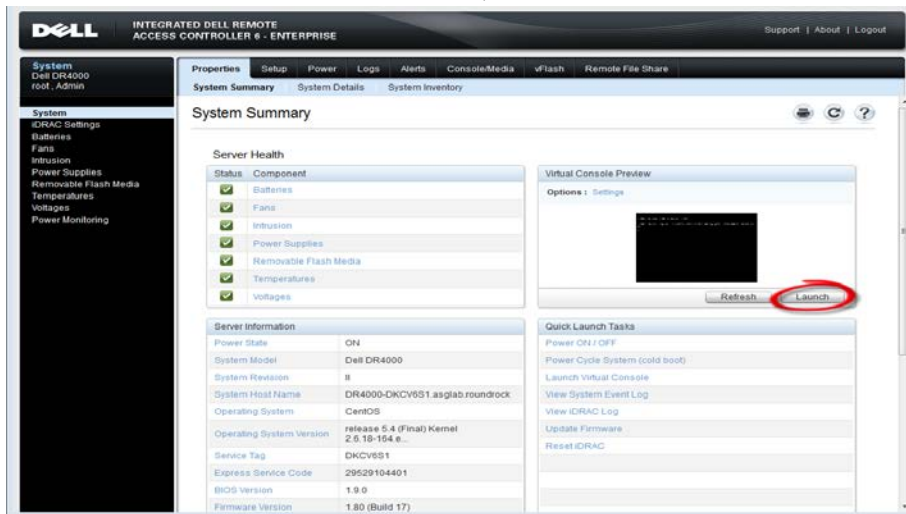
See the DR Series Deduplication Appliance documentation for other data management application best practices whitepapers at <http://www.dell.com/support/troubleshooting/us/en/04/Product/powervault-dr4100>, under "Manuals & Documentation".

NOTE: The DR Series Deduplication Appliance/NetWorker build versions and screen shots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/NetWorker software version used.

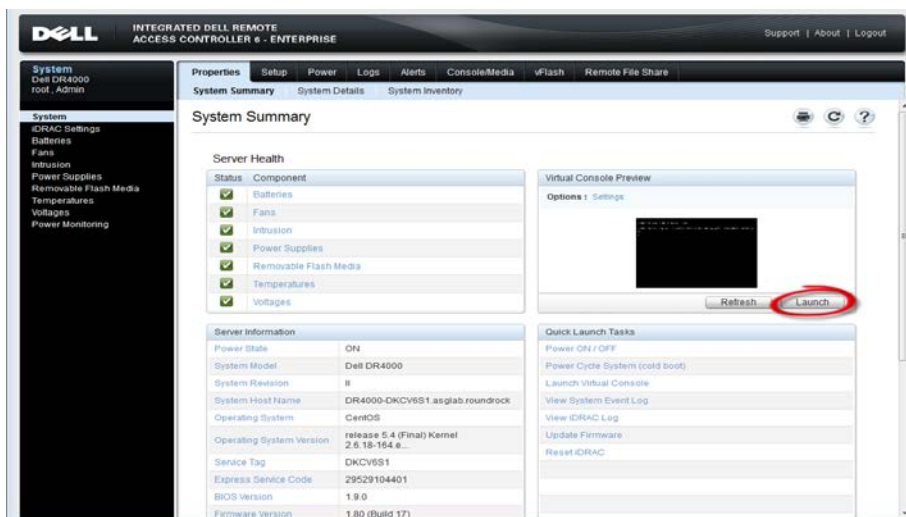


1 Install and Configure the DR Series Deduplication Appliance

1. Rack and cable the DR Series Deduplication Appliance 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 into iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use user name **root**, and the password **calvin**.



4. Launch the virtual console.



5. Once 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).

```
Dcarina release 1 (EAR-1.00.00) Build: 32050
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:
```

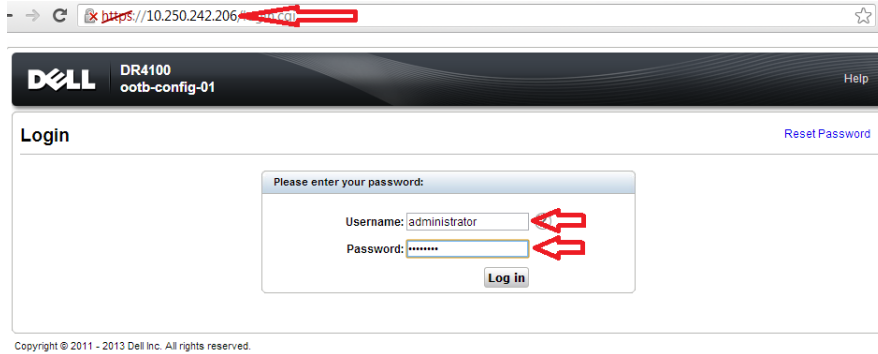
7. View the summary of preferences and confirm that it is correct.

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



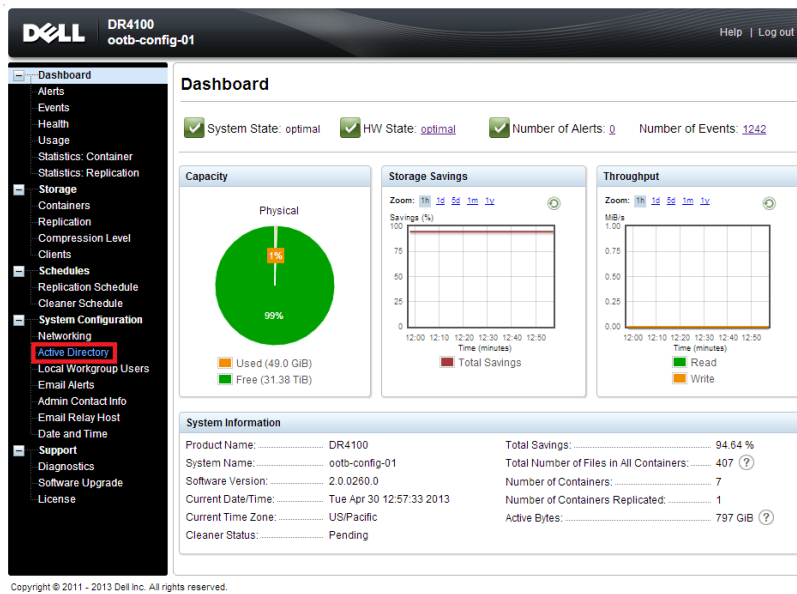
8. Log into the DR Series Deduplication Appliance administrator console, using the IP address you just provided for the DR Series Deduplication Appliance, user **administrator** and the password **St0r@ge!** (The "0" in the password is the numeral zero).



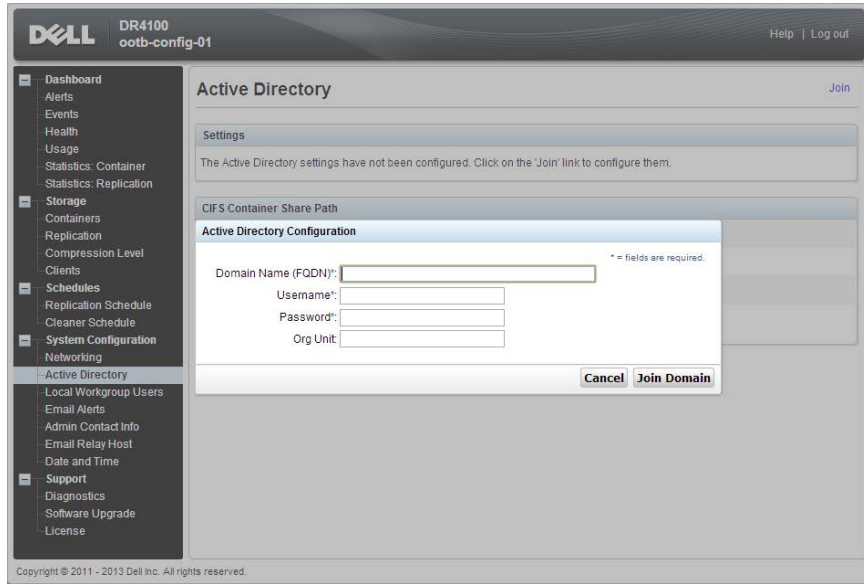
9. (Optional) Join the DR Series Deduplication Appliance to Active Directory --- only when the DR is also providing CIFS access to backup servers.

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

- a. Select **Active Directory** in the tree on the left hand side of the dashboard.

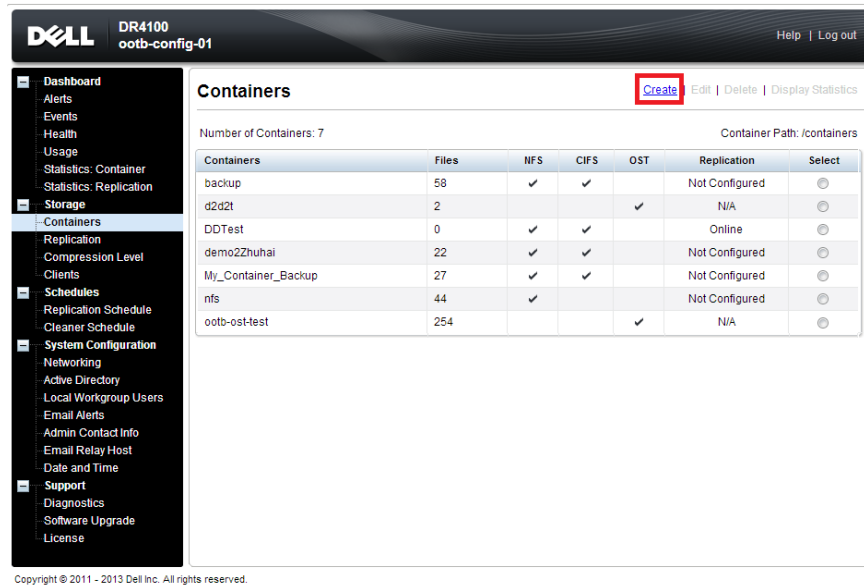


- b. Enter your Active Directory credentials.



10. Create and mount the container.

- a. Select **Containers** in the tree on the left side of the dashboard, and then click the **Create** link 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 **NFS** section, note down the **NFS access path** (this will be used in configuring device on Networker server), and select **Enable NFS**. For **Client Access** section, choose either **Open Access**, or manually add clients into the allow list with having NFS Options as "rw"

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

Client Access:
 Open Access (all clients have access)

Add client (IP or FQDN Hostname):

Clients:

NFS Options:
 rw insecure
 ro

Map root to:
-select-

CIFS

CIFS share path: \\10.250.242.206\My_Container_Backup

Use CIFS to backup MS Windows clients.
 Enable CIFS



Note: For improved security, Dell recommends adding IP addresses for the following (Not all environments will have all components):

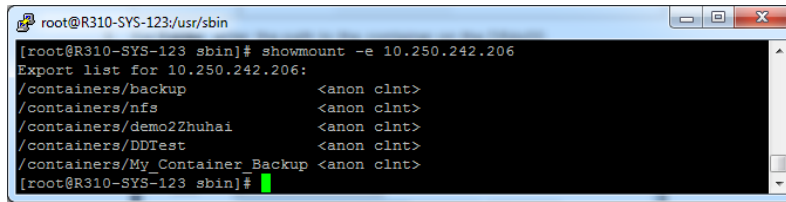
- Backup console (Networker Server)
- Network Storage Nodes
- Networker Clients

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



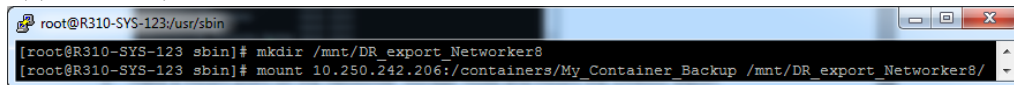
2 Configure the Networker Storage Node

1. Log into the networker storage node and run the command as shown, to display the NFS exports on DR Series Deduplication Appliance



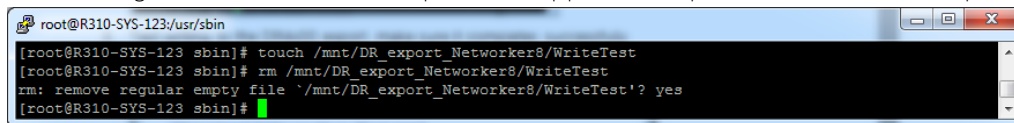
```
root@R310-SYS-123:/usr/sbin
[root@R310-SYS-123 sbin]# showmount -e 10.250.242.206
Export list for 10.250.242.206:
/containers/backup          <anon clnt>
/containers/nfs             <anon clnt>
/containers/demo2Zhuhai    <anon clnt>
/containers/DDTest         <anon clnt>
/containers/My_Container_Backup <anon clnt>
[root@R310-SYS-123 sbin]#
```

2. Make a mount point on the Networker Storage Node and mount the DR Series Deduplication Appliance export



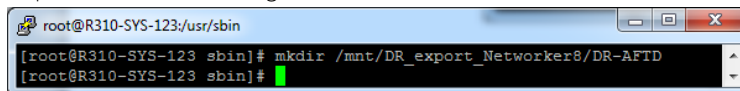
```
root@R310-SYS-123:/usr/sbin
[root@R310-SYS-123 sbin]# mkdir /mnt/DR_export_Networker8
[root@R310-SYS-123 sbin]# mount 10.250.242.206:/containers/My_Container_Backup /mnt/DR_export_Networker8/
```

3. Test writing to the DR Series Deduplication Appliance export, make sure it completes successfully



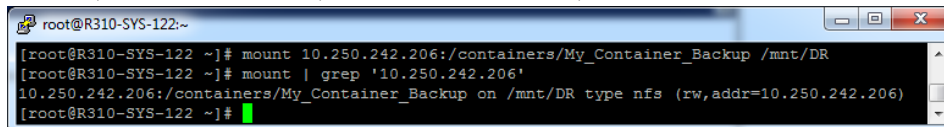
```
root@R310-SYS-123:/usr/sbin
[root@R310-SYS-123 sbin]# touch /mnt/DR_export_Networker8/WriteTest
[root@R310-SYS-123 sbin]# rm /mnt/DR_export_Networker8/WriteTest
rm: remove regular empty file `/mnt/DR_export_Networker8/WriteTest'? yes
[root@R310-SYS-123 sbin]#
```

4. Create a subdirectory to be used as device path in configuring DR Series Deduplication Appliance export onto the storage node



```
root@R310-SYS-123:/usr/sbin
[root@R310-SYS-123 sbin]# mkdir /mnt/DR_export_Networker8/DR-AFTD
[root@R310-SYS-123 sbin]#
```

5. If Client Direct feature will be used, on each of the client, mount the DR export and note down the mount point. This mount point is needed in step 9 of the next section of **Set up Networker**



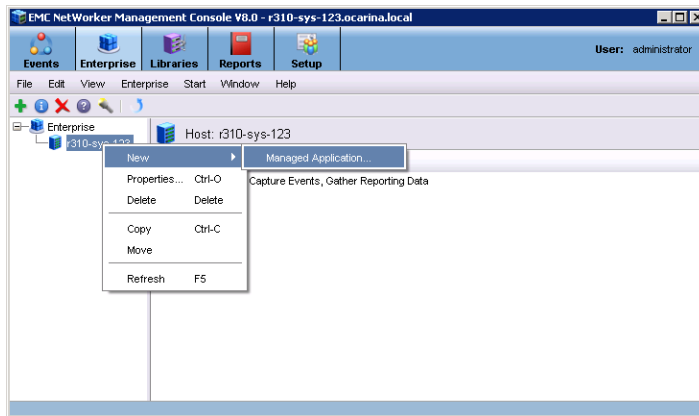
```
root@R310-SYS-122:~
[root@R310-SYS-122 ~]# mount 10.250.242.206:/containers/My_Container_Backup /mnt/DR
[root@R310-SYS-122 ~]# mount | grep '10.250.242.206'
10.250.242.206:/containers/My_Container_Backup on /mnt/DR type nfs (rw,addr=10.250.242.206)
[root@R310-SYS-122 ~]#
```

NOTE: On DR4x00 models, the maximum supported CIFS connections per Appliance is 32, and on DR6000 model the max is 64, so there should be no more than 32 and 64 corresponding clients connected/mapped to a single DR Series Deduplication Appliance for backup at the same time.

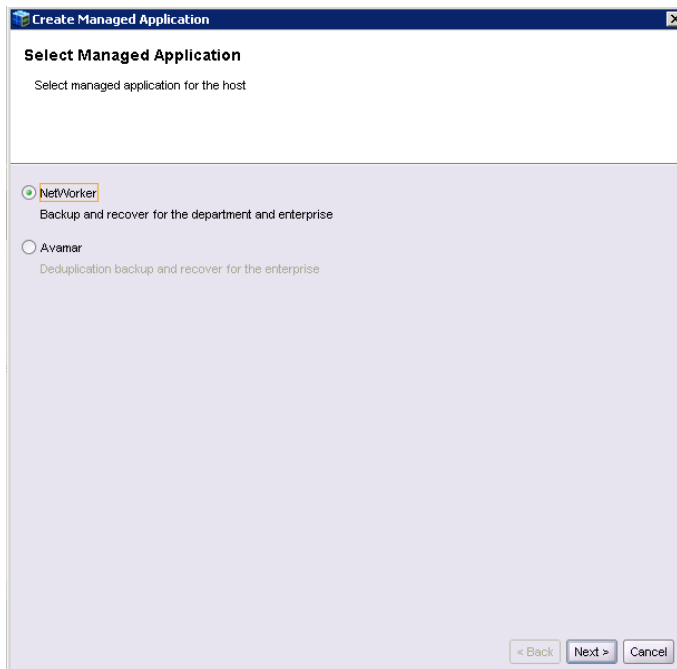


3 Set up Networker

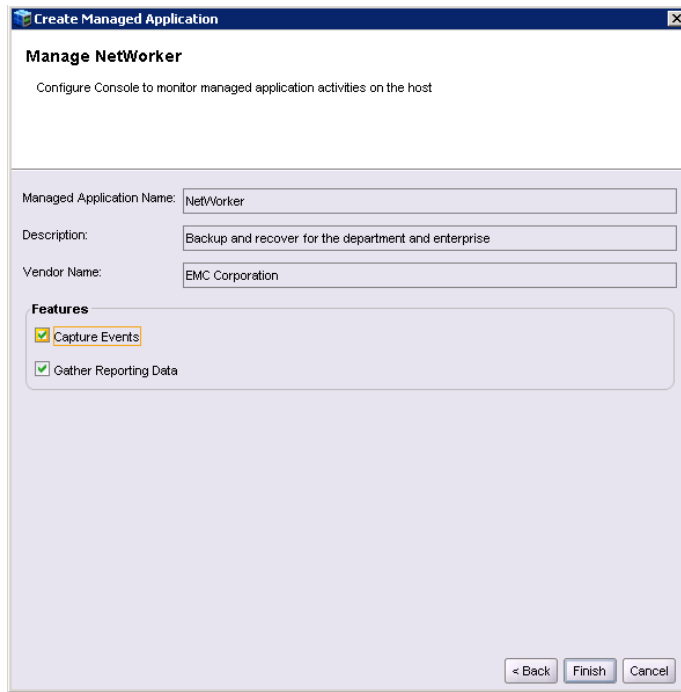
1. Open the **Networker Management Console (NMC)**
2. Click the **Enterprise** menu button, high-light the storage node that the DR Series Deduplication Appliance export will be configured as backup device, right-click on the host and select **New**, then select **Managed Application**



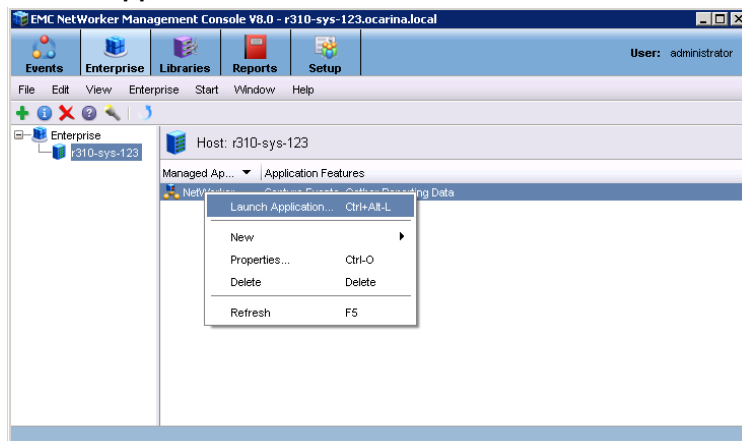
3. Select **Networker** and click on **Next**



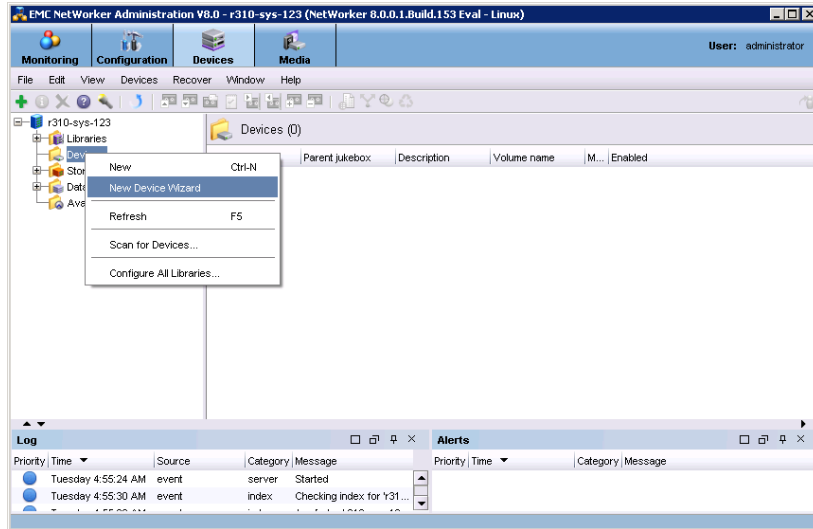
4. Click on **Finish**



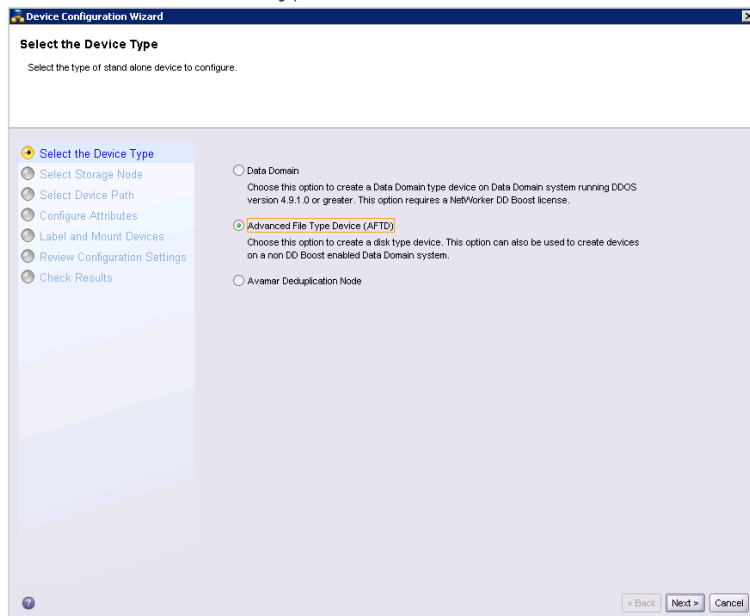
5. High-light the newly created Networker application, right-click on the application and select **Launch Application**



- A new Devices window will open. On left side panel right-click on **Device**, select **New Device Wizard**



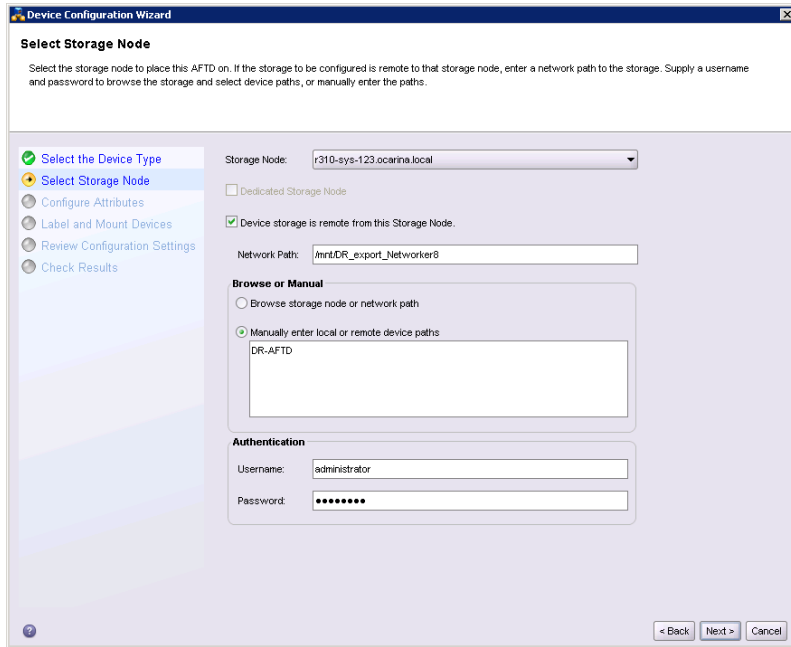
- Select Advanced File Type Device (AFTD)



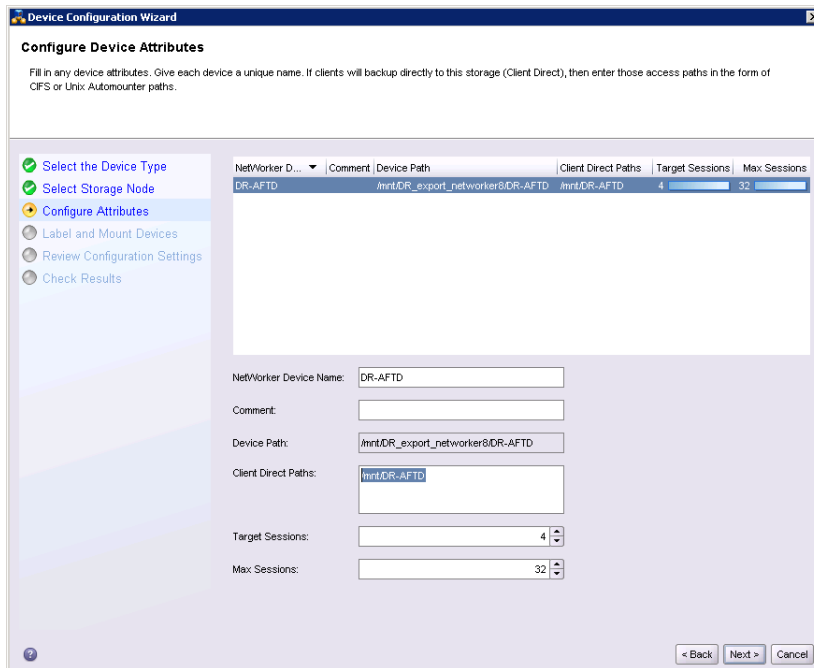
- On next window, Select **Device storage is remote from this Storage Node**, in **Network Path** enter DR Series Deduplication Appliance export mount point on the storage node (if name resolution works, hostname or FQDN can be used in the server portion of the network path). Choose **Manually enter local or remote device paths** and type in the subdirectory name previously created as device path (please refer to step 4 of previous section **Configure the NetWorker Storage Node**). In **Authentication** section, type in DR Series Deduplication Appliance administrator



with password to access the DR Series Deduplication Appliance export. Click on **Next**

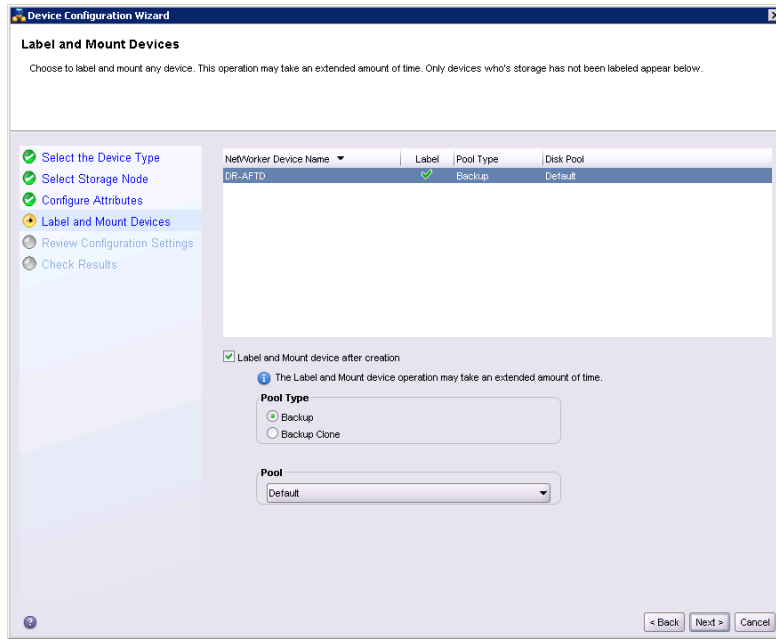


- Set the sessions attributes according to Networker administration document. If **Client Direct** feature will be used, enter each of the client machine DR export mount points as a separate line into the **Client Direct Paths list** (Please refer to step 5 of last section **Configure the Networker Storage Node**). Click on **Next**

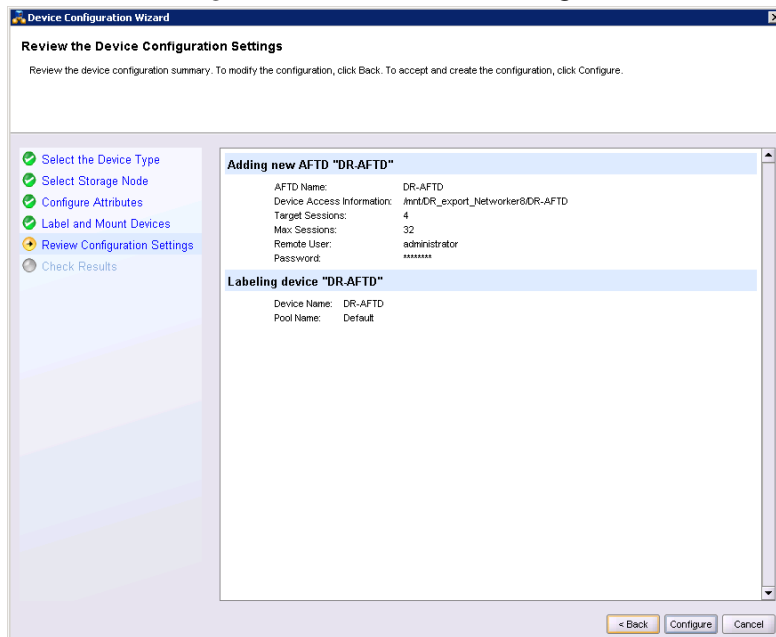


NOTE: On DR4x00 models, the maximum supported CIFS connections per Appliance is 32, and on DR6000 model the max is 64, so there should be no more than 32 and 64 corresponding clients connected/mapped to a single DR Series Deduplication Appliance for backup at the same time.

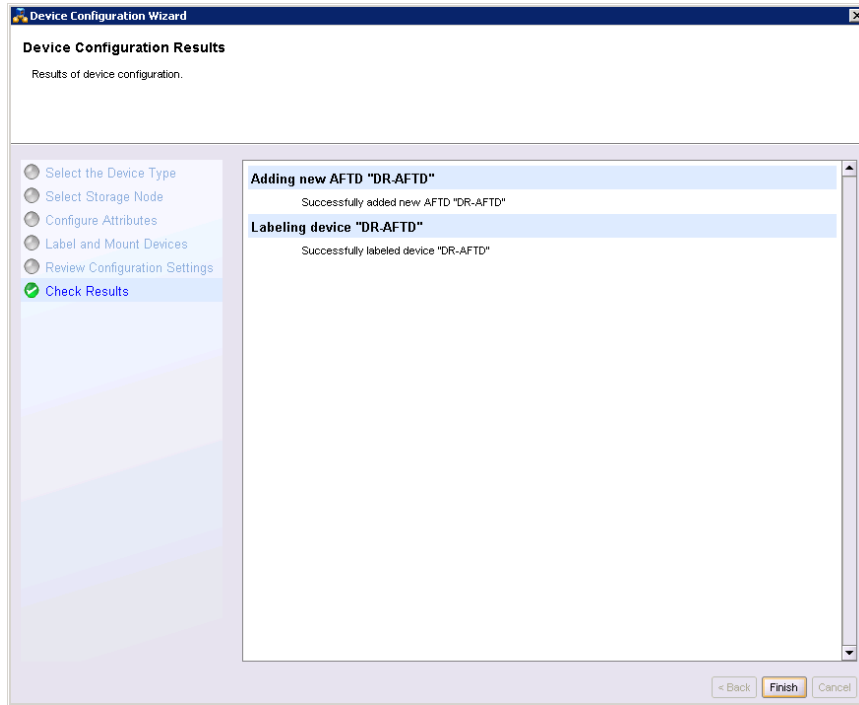
10. The new Networker device should have **Backup** as Pool Type, click **Next**



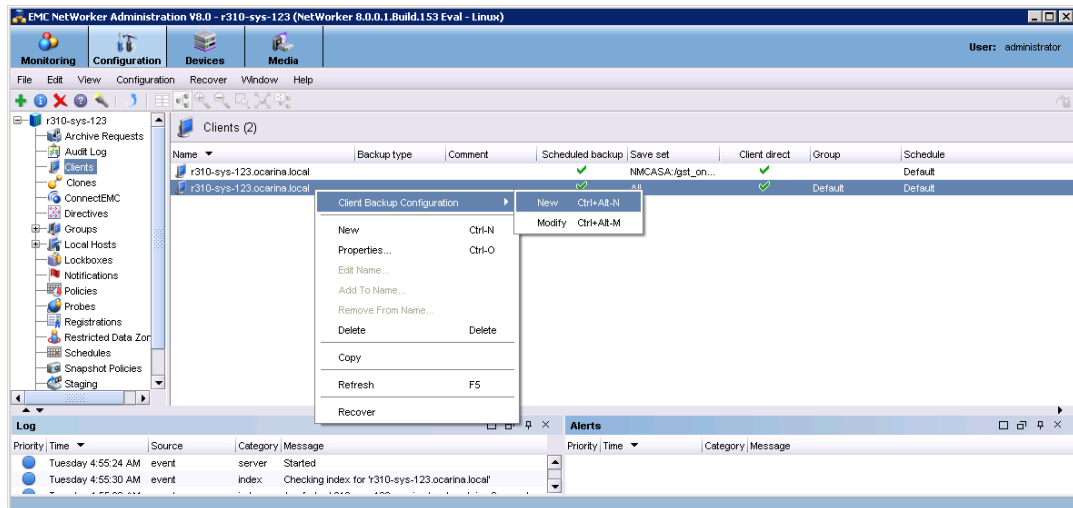
11. Review the configuration, then click on **Configure**



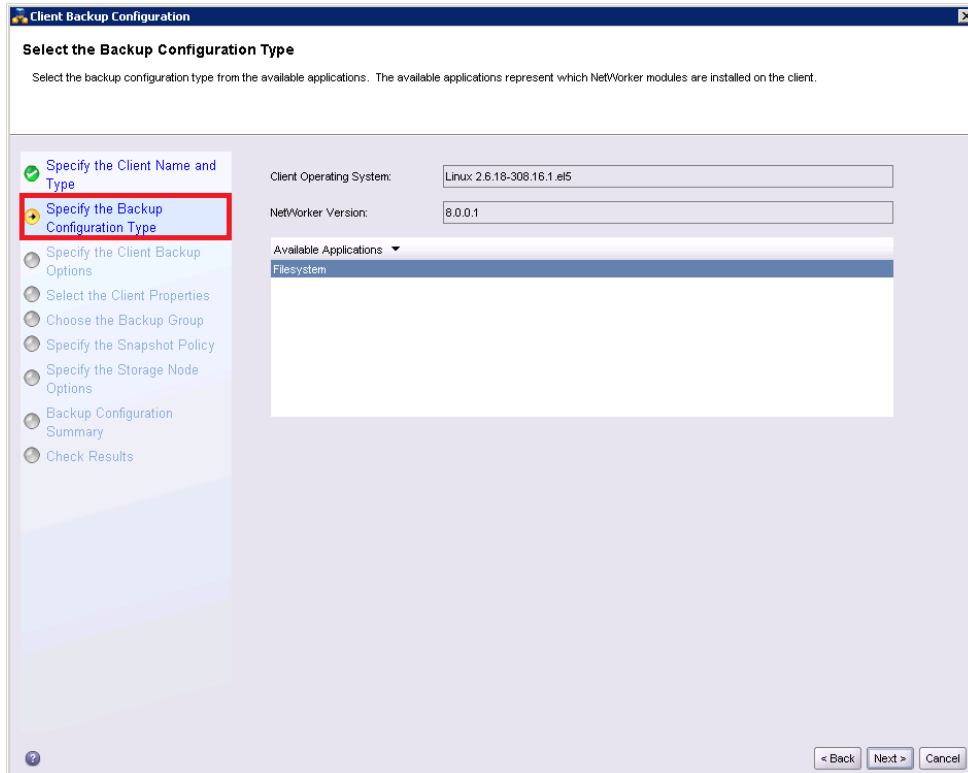
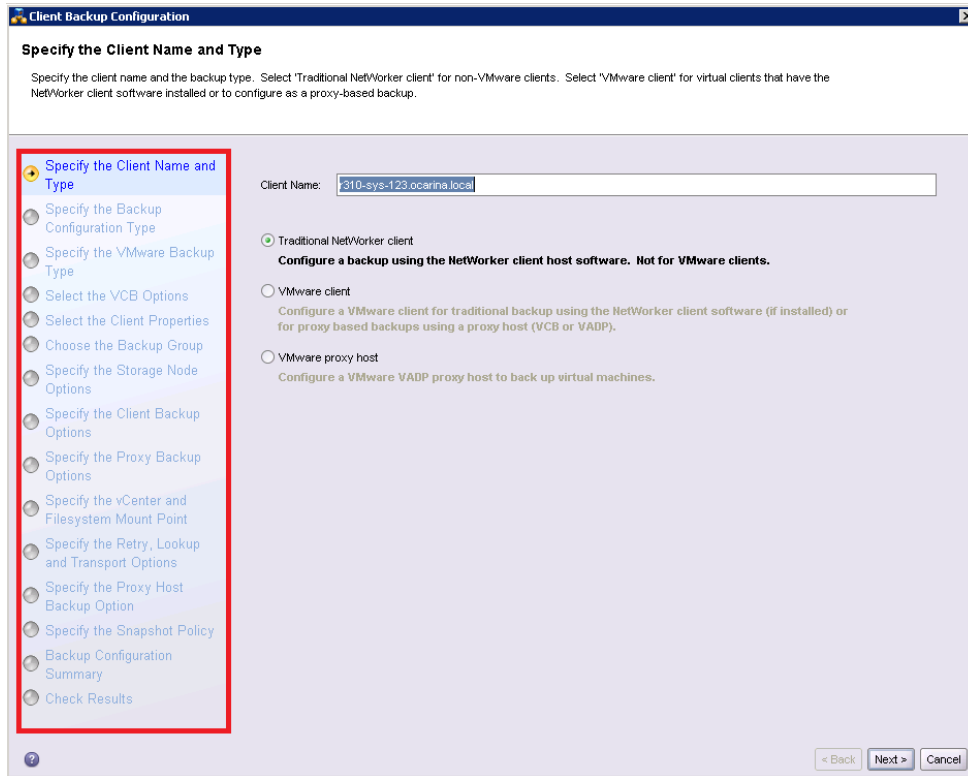
12. Click on **Finish**



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



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



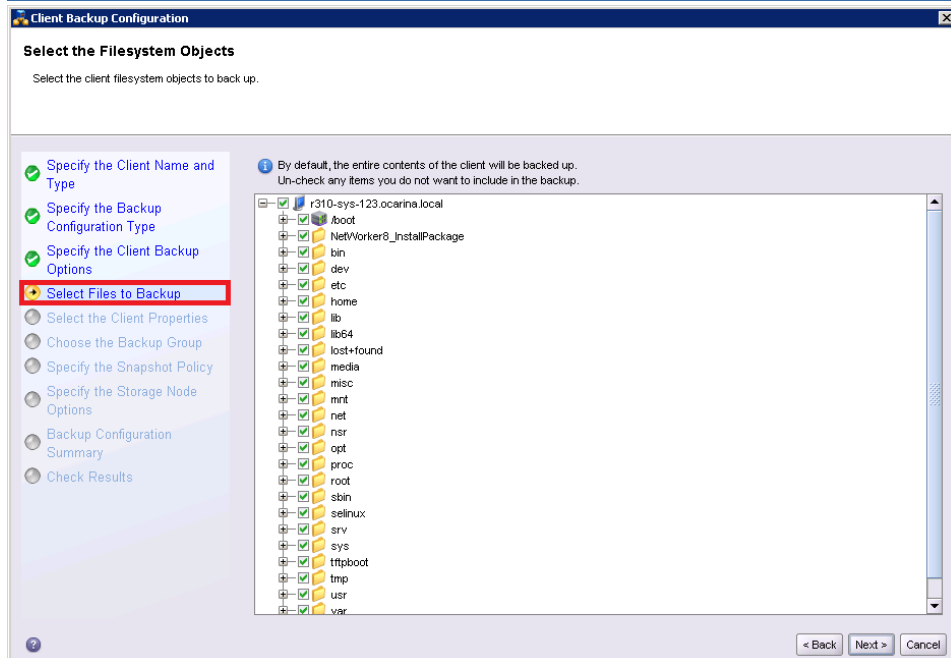
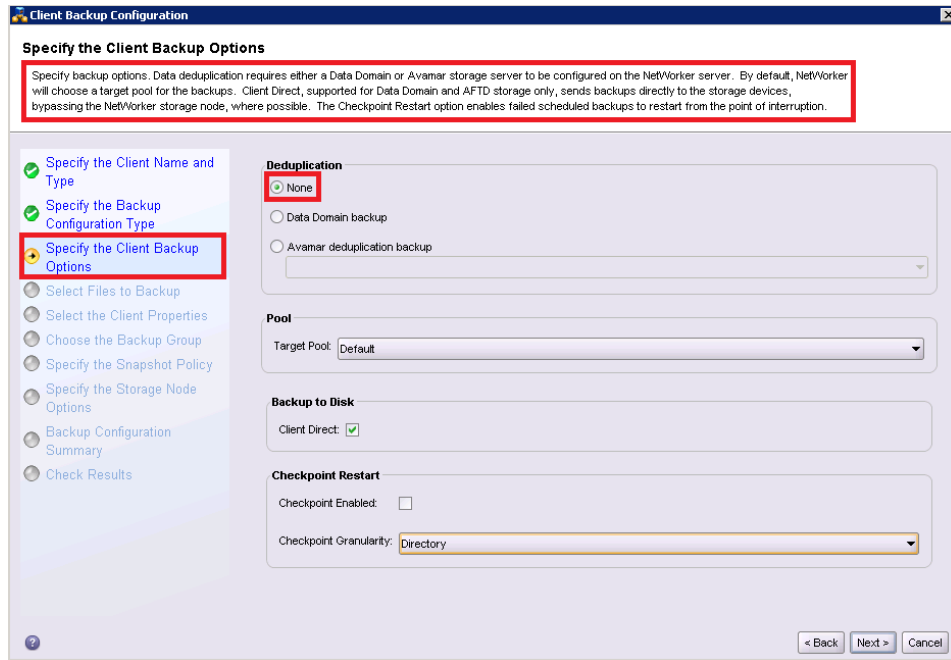
Note: Pay special attention to the following step while setting the other options appropriately according to the backup environment:

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 (please refer to step 9 above in the same section, and step 5 in

Configure the Networker Storage Node section).



Client Backup Configuration

Select the NetWorker Client Properties

Select the NetWorker client properties. To accept the default properties, click Next.

- Specify the Client Name and Type
- Specify the Backup Configuration Type
- Specify the Client Backup Options
- Select Files to Backup
- Select the Client Properties**
- Choose the Backup Group
- Specify the Snapshot Policy
- Specify the Storage Node Options
- Backup Configuration Summary
- Check Results

Browse Policy: (Maintain backup entries in the online file index) +

Retention Policy: (Maintain backup entries in the save set index) +

Backup Schedule:

Client Comment:

Remote Access:

< Back Next > Cancel

Client Backup Configuration

Specify the NetWorker Backup Group

Select or create the NetWorker group for this configuration.

- Specify the Client Name and Type
- Specify the Backup Configuration Type
- Specify the Client Backup Options
- Select Files to Backup
- Select the Client Properties
- Choose the Backup Group**
- Specify the Snapshot Policy
- Specify the Storage Node Options
- Backup Configuration Summary
- Check Results

Add to an existing group

Name	Start Time
<input checked="" type="checkbox"/> Default	21:00

Create a new group

Group Name:

Client Retries:

Schedule Options

Scheduled Backup Start Time (24-hour clock)

Automatically start the backup at the scheduled time

< Back Next > Cancel



Client Backup Configuration

Specify the Storage Node Options

Select the backup and recovery storage nodes to use for this client.

- Specify the Client Name and Type
- Specify the Backup Configuration Type
- Specify the Client Backup Options
- Select Files to Backup
- Select the Client Properties
- Choose the Backup Group
- Specify the Storage Node Options**
- Backup Configuration Summary
- Check Results

Changing the storage node options for this configuration will affect all configurations for this client.

Backup Storage Nodes

Backup to NetWorker server only

Backup to the following storage nodes

Name	Type	Config...	Device Sharin...	Number of Devices
<input checked="" type="checkbox"/> r310-sys-123.ocarina.local	scsi	Yes	server default	1

Recovery Storage Nodes

Recover from NetWorker server only

Recover from the following storage nodes

Name	Type	Config...	Device Sharin...	Number of Devices
<input checked="" type="checkbox"/> r310-sys-123.ocarina.local	scsi	Yes	server default	1

< Back Next > Cancel

Client Backup Configuration

Backup Configuration Summary

Review the configuration summary. To modify the configuration, click Back. To accept and create the configuration, click Create.

- Specify the Client Name and Type
- Specify the Backup Configuration Type
- Specify the Client Backup Options
- Select Files to Backup
- Select the Client Properties
- Choose the Backup Group
- Specify the Storage Node Options
- Backup Configuration Summary**
- Check Results

Adding new group "NW_DR"

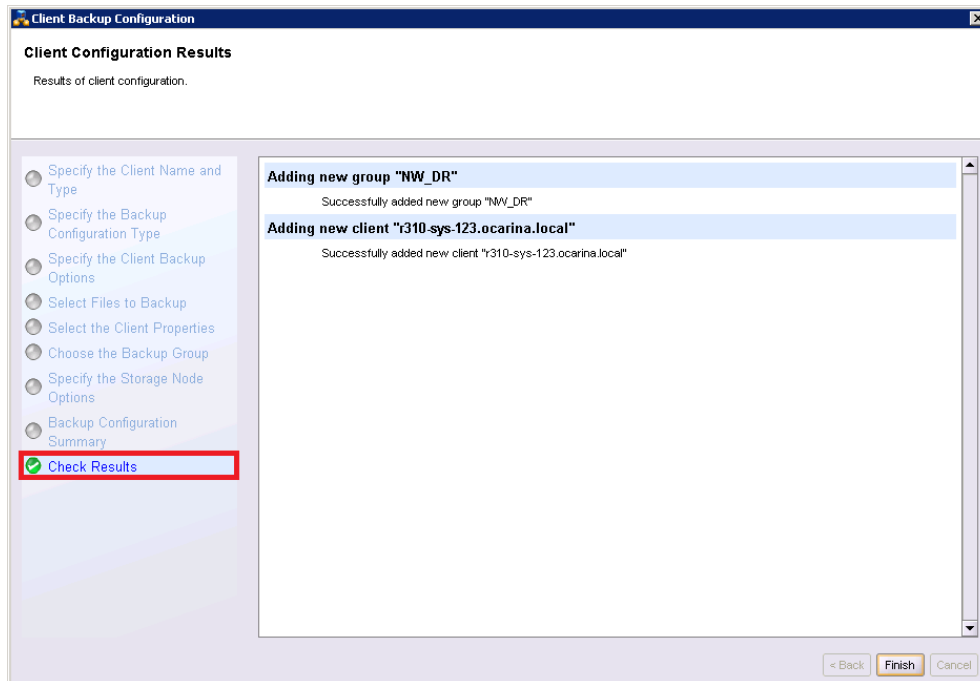
Name: NW_DR
 Client Retries: 1
 Start Time: 21:00
 Autostart: No

Adding new client "r310-sys-123.ocarina.local"

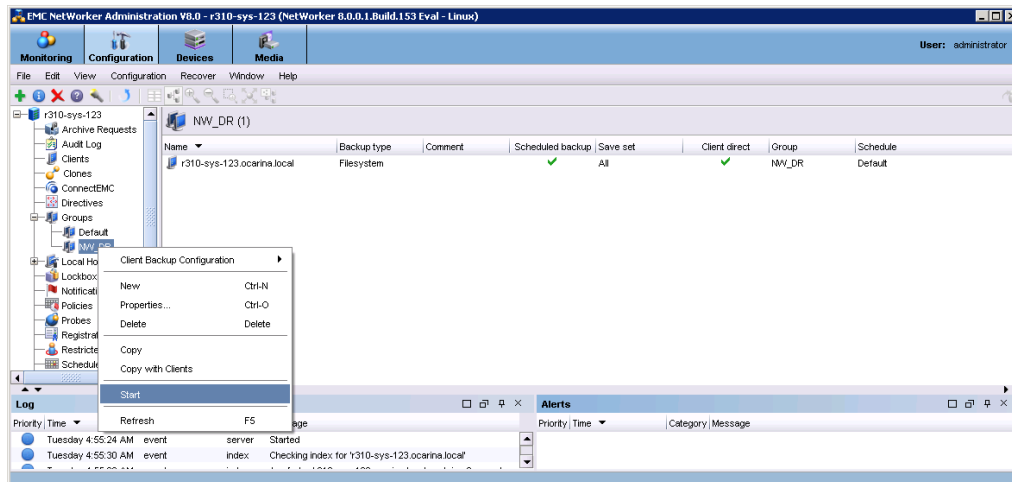
Save set: All
 Name: r310-sys-123.ocarina.local
 Backup Type: Filesystem
 Deduplication: None
 Checkpoint Enabled: false
 Checkpoint Granularity: Directory
 Client Direct: true
 Pool:
 Browse Policy: Month
 Retention Policy: Year
 Schedule: Default
 Group: NW_DR
 Storage Nodes: r310-sys-123.ocarina.local
 Recover Storage Nodes: r310-sys-123.ocarina.local

< Back Create Cancel





15. Once the backup group is successfully created, start the backup



16. Monitor the job status through Monitoring tab

The screenshot shows the EMC NetWorker Administration interface. The 'Monitoring' tab is active, displaying the following sections:

- Groups:** A table showing job groups. The 'NW_DR' group is highlighted, showing a status of '100%' and 'disabled'.
- All Sessions:** A table showing active sessions. Two sessions are listed for 'r310-sys-12...' with a status of 'save' and a duration of '00:00:30'.
- Devices:** A table showing device information. One device 'DR-AFTD' is listed with a message 'space recovered from volume r310...'.
- Log:** A table showing system events. Two events are listed for 'Tuesday 4:55:24 AM' with categories 'server' and 'index'.
- Alerts:** A table showing alerts, currently empty.
- NW_DR Details:** A detailed view of a job. It shows a 'Start Time' of '4/30/13 10:16:26 AM', a 'Status' of 'Succeeded', and a 'Percentage Complete' of '100%'. The 'Duration' is '130 Sec' and the 'Total Amount' is '4003 MB'.

The 'Completed Successfully' section contains the following table:

Client Name	Save Set	Level	Type	Start Time	Duration	Size	File Co...	Messages
r310-sys-12...	f	full		4/30/13 10:16:34 ...	00:01:55	3970 MB	96447	86705.save: Successfully established DFA s...
r310-sys-12...	boot	full		4/30/13 10:16:29 ...	00:00:00	21 MB	40	86705.save: Successfully established DFA s...
r310-sys-12...	r310-sys-123.ocari...	full		4/30/13 10:16:34 ...	00:00:00	12 MB	5	86705.save: Successfully established DFA s...
r310-sys-12...	r310-sys-123.ocari...	full		4/30/13 10:16:34 ...	00:00:05	93 KB	138	86705.save: Successfully established DFA s...

The 'Failed' section is currently empty.



4 Set up DR Native Replication & Restore from Replication Target

4.1 Create Replication Session between Two DR Appliances

Note: below screenshots show as CIFS containers, but the procedure is exact the same for NFS containers

1. Create a source container on the source DR appliance

The screenshot shows the Dell DR4100-VM web interface. The left sidebar contains navigation menus for Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Schedules, System Configuration, Networking, and Support. The main content area is titled 'Containers' and shows a table of containers. The 'rep-source' container is highlighted with a red background.

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 appliance

The screenshot shows the Dell DR4100-VM web interface. The left sidebar contains navigation menus for Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Schedules, System Configuration, Networking, and Support. The main content area is titled 'Containers' and shows a table of containers. The 'rep-target' container is highlighted with a red background.

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 appliance, go to **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, then enter the target DR related info in **Step 4** menu item

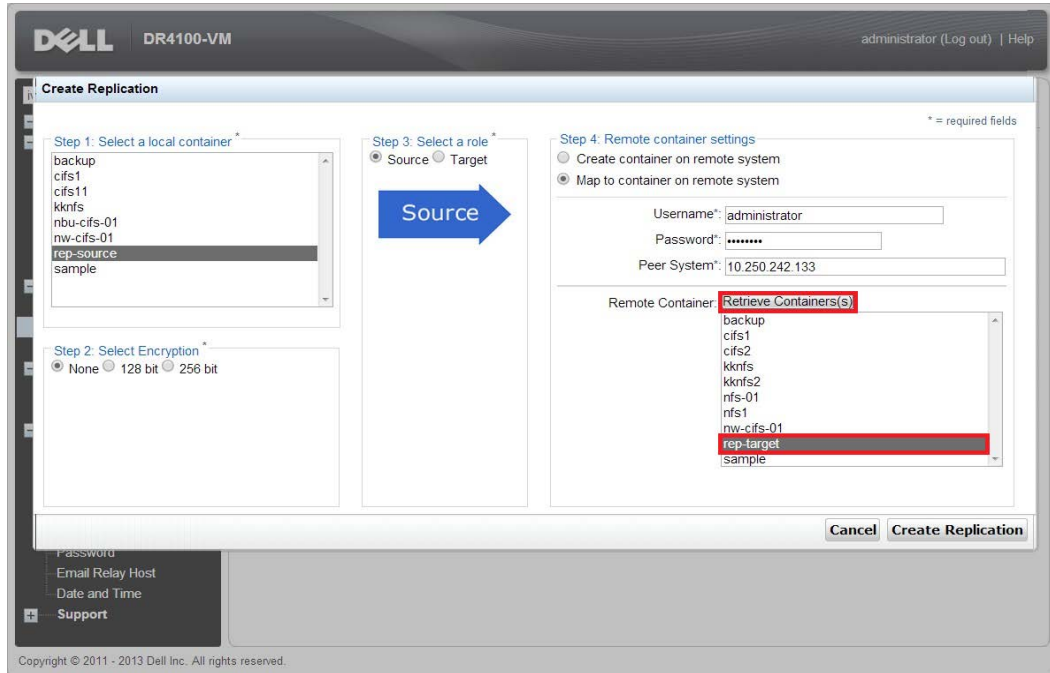
The screenshot shows the "Create Replication" wizard in the Dell DR4100-VM web interface. The wizard consists of four steps:

- 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 visible.
- Step 3: Select a role**: Radio buttons for "Source" (selected) and "Target" are visible. A blue arrow labeled "Source" points from Step 1 to Step 3.
- Step 4: Remote container settings**: This step is highlighted with a red box. It includes:
 - Radio buttons for "Create container on remote system" and "Map to container on remote system" (selected).
 - Fields for "Username*" (administrator), "Password*" (masked), and "Peer System*" (10.250.242.133).
 - A "Remote Container:" field with a "Retrieve Containers(s)" button.

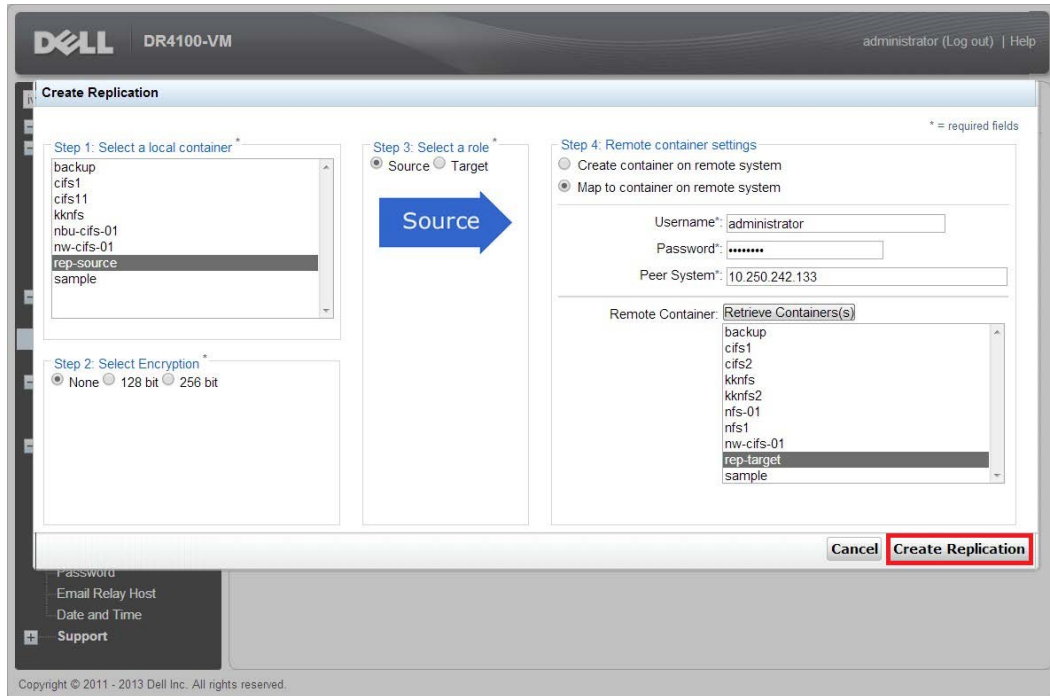
Buttons for "Cancel" and "Create Replication" are at the bottom right. The copyright notice "Copyright © 2011 - 2013 Dell Inc. All rights reserved." is at the bottom.



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



6. Click Create Replication button



7. Verify the replication relation between DRs is created, and **Peer Status** is **Online**

The screenshot shows the Dell DR4100-VM management interface. The top navigation bar includes the Dell logo, the model name 'DR4100-VM', and the user 'administrator (Log out) | Help'. A left sidebar contains a navigation menu with categories like Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Replication, Clients, Schedules, and System Configuration. 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:

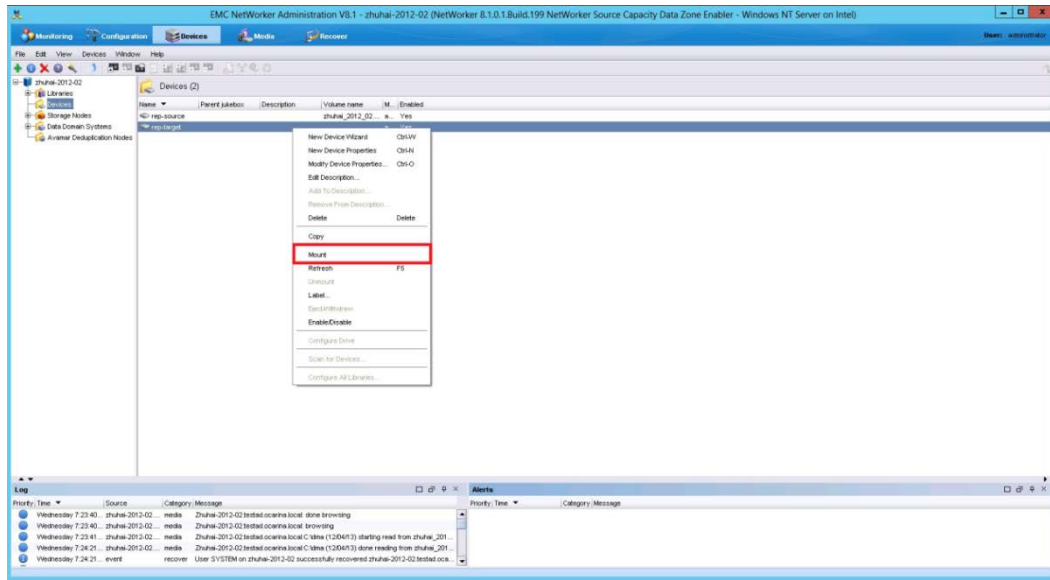
Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nvbu	source	10.250.243.18 nvbu	Stopped	Default	<input type="radio"/>
nvbu1	source	10.250.243.18 nvbu1	Online	Default	<input type="radio"/>
rep-source	source	10.250.242.133 rep-target	Online	Default	<input checked="" type="radio"/>

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



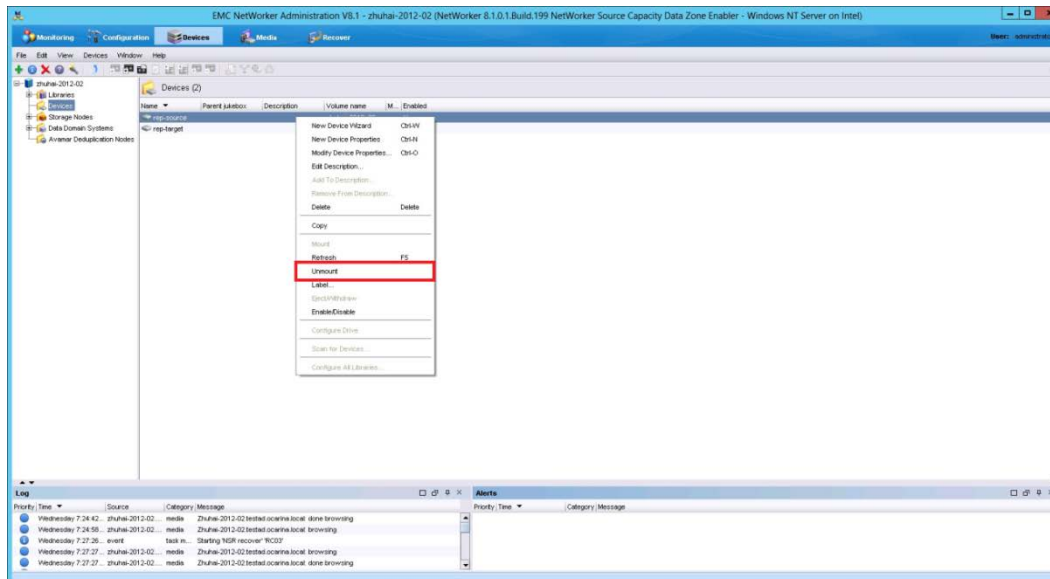
4.2 Restore from Replication Target Container

1. Add the target container onto NetWorker Storage Node (Right-Click **Device** -> **New Device Properties**, then fill in necessary information for the target device). After it's done, **Mount** the device

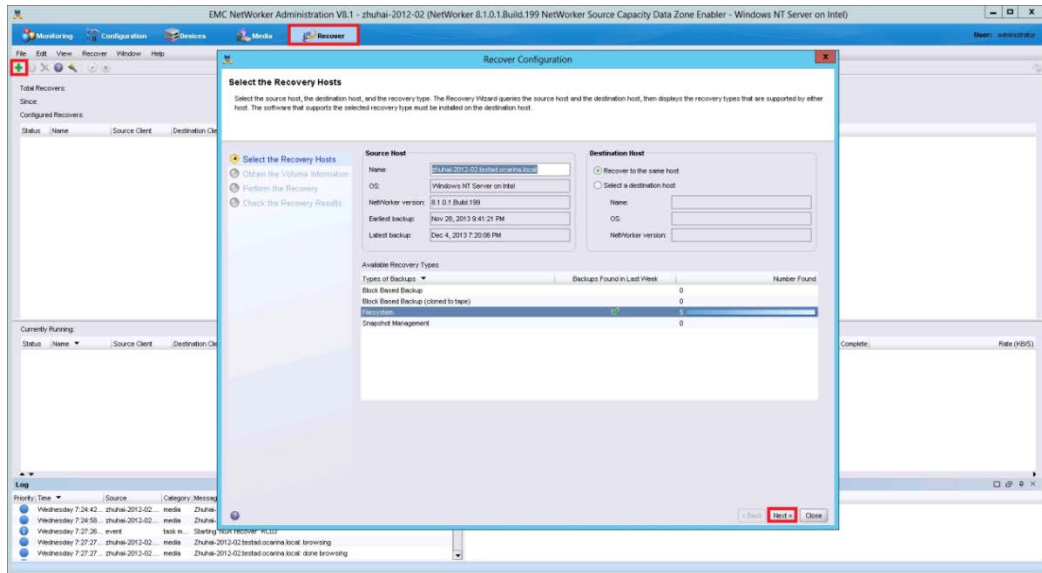


Note: Don't label the target device

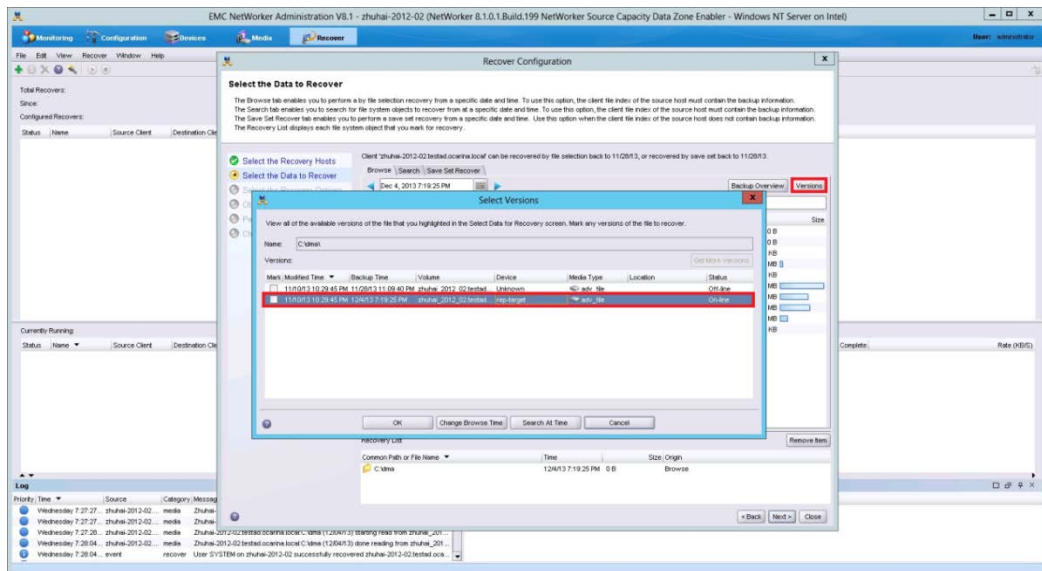
2. **Unmount** the source container



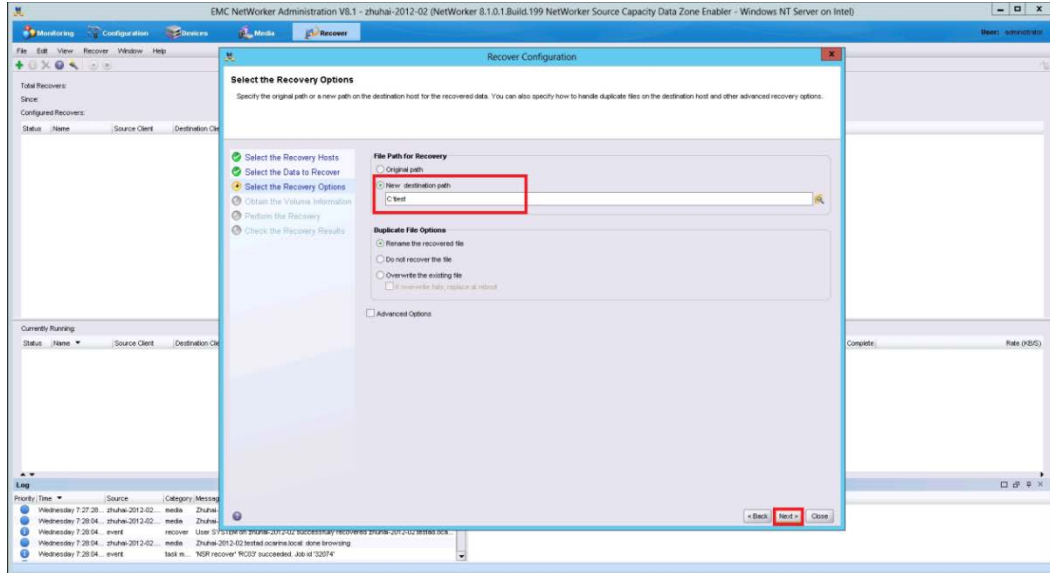
- Go to **Recover**, click **+**, select a backup source host, then click **Next**



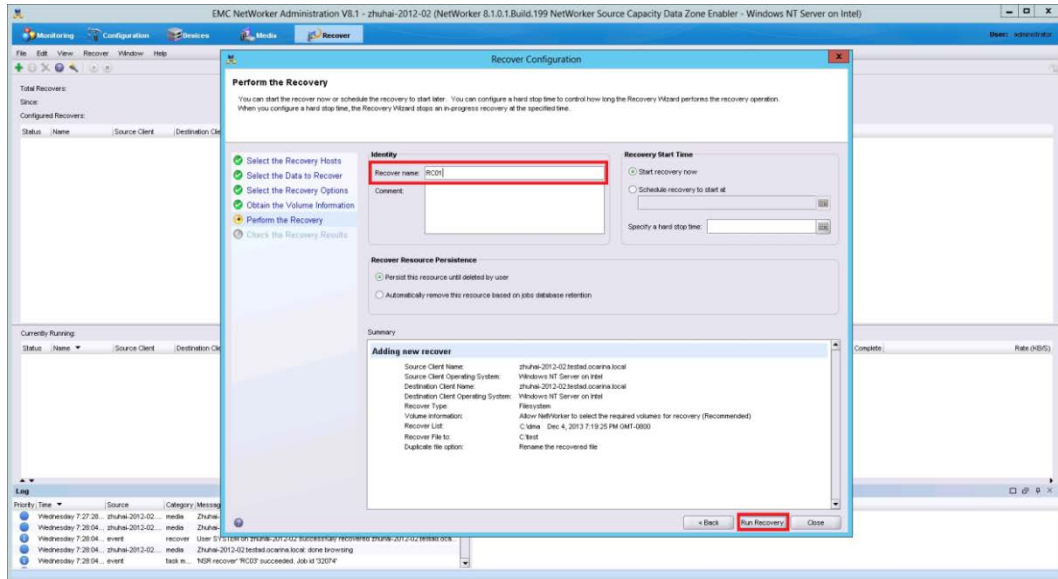
- Select the data set to recover, click **Versions** to view **Select Versions** window, make selection on the data then click on **OK**



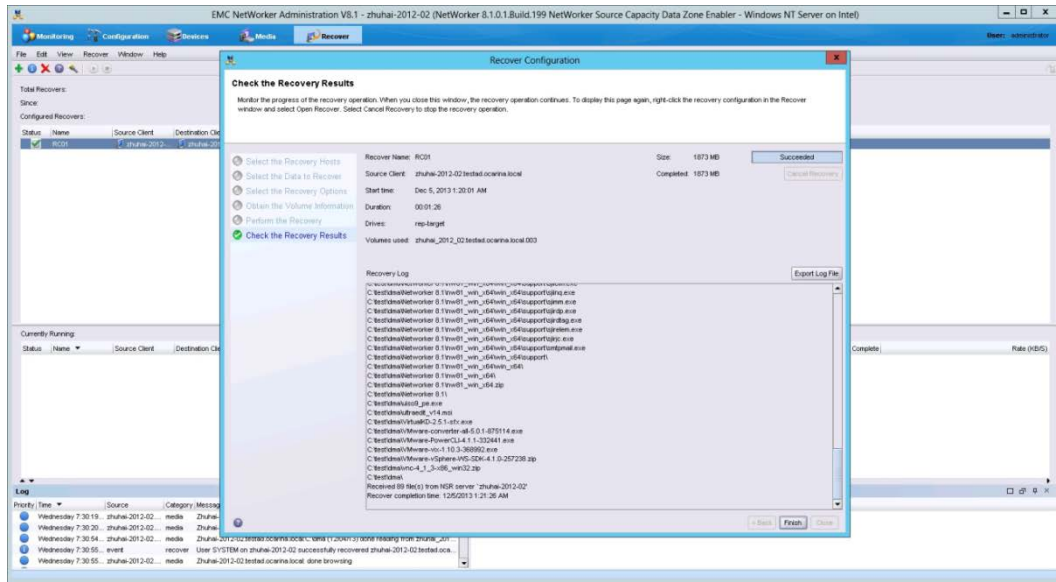
5. Select the **Recovery Options**, choose **Original path** or enter a **New destination path** to recover data to, then click **Next**



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



7. Check the Recovery Results

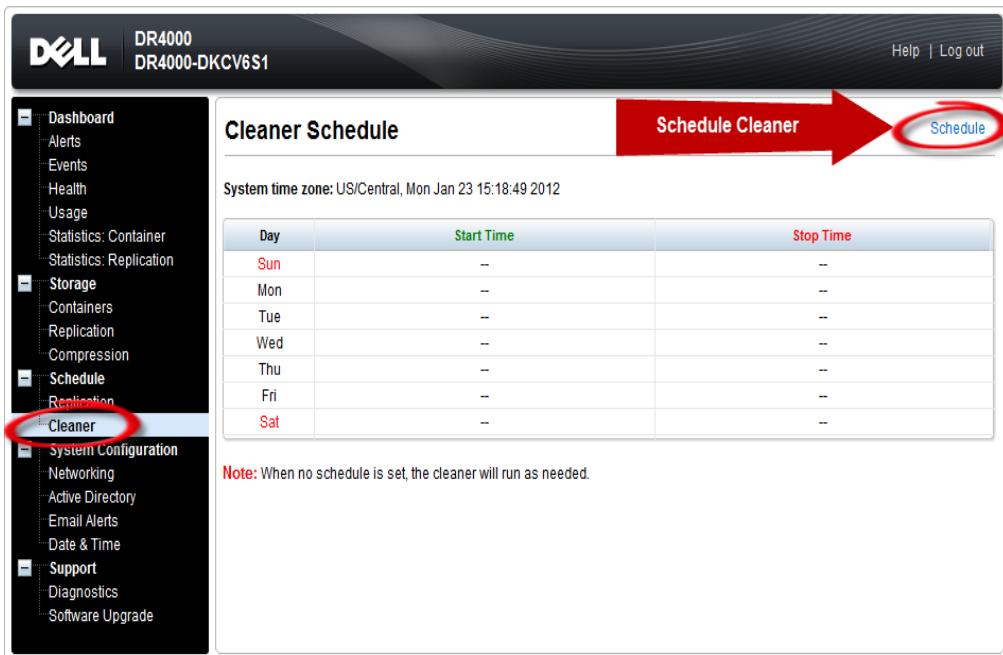


5 Set up the DR Series Deduplication Appliance Cleaner

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 shows the Dell DR4000 web interface. The top header includes the Dell logo, model numbers (DR4000, DR4000-DKCV6S1), and links for Help and Log out. A left-hand navigation menu lists various system components, with 'Cleaner' highlighted and circled in red. The main content area is titled 'Cleaner Schedule' and features a red arrow pointing to a 'Schedule Cleaner' button, which in turn points to a 'Schedule' button also circled in red. Below the title, the system time zone is shown 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. The table shows that the cleaner is currently not scheduled for any days. 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	--	--

6 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.

