



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

Dell Engineering
June 2015

Revisions

Date	Description
January 2014	Initial release
April 2015	Added VTL Content for v3.2 Release
June 2015	Added content for configuring an iSCSI target for Linux

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.

© 2015 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, and PowerVault™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. 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. EMC® and Networker® are registered trademarks of EMC Corporation in the United States and other countries.

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

Executive summary.....	4
1 Installing and configuring the DR Series system	5
2 Creating and configuring CIFS target container(s) for Networker.....	9
2.1 Creating the network share container for Networker use.....	9
2.2 Configuring the Networker storage node – Windows CIFS	11
2.3 Configuring Networker to use the newly created network share	12
2.4 Setting up DR Series system replication and restore from the replication target	25
2.4.1 Creating a replication relationship between two DR Series systems.....	25
2.4.2 Restoring from the replication target container.....	29
3 Creating and configuring iSCSI target container(s) for Networker.....	33
3.1 Creating an iSCSI VTL container for Networker use	33
3.1.1 Configuring the iSCSI Networker storage node – Windows	35
3.1.2 Configuring the iSCSI target – Linux.....	39
3.2 Setting up Networker to use the newly created iSCSI VTL.....	40
4 Creating and configuring NDMP target container(s) for Networker.....	44
4.1 Creating the NDMP VTL container for Networker use.....	44
4.2 Configuring Networker to use the newly created NDMP VTL	46
5 Setting up the DR Series system cleaner	51
6 Monitoring deduplication, compression, and performance	52
A Managing VTL protocol accounts and credentials	53
A.1 iSCSI account details and management.....	53
A.2 NDMP account details and management.....	54
A.3 VTL default account summary table.....	55
B Adding VTL media.....	56
B.1 Adding the VTL media to the container.....	56
B.1.1 VTL media count guidelines	56
B.2 Updating Networker to identify newly added VTL media.....	57



Executive summary

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

For additional information, see the DR Series system documentation and other data management application best practices whitepapers for your specific DR Series system at:

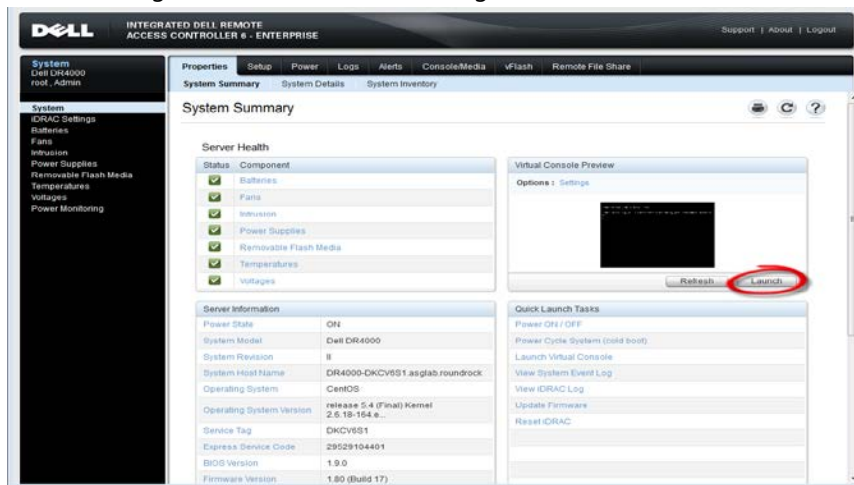
<http://www.dell.com/powervaultmanuals>

Note: The DR Series system and EMC Networker screenshots used for this whitepaper may vary slightly, depending on the firmware version of the DR Series system or the software you are using.

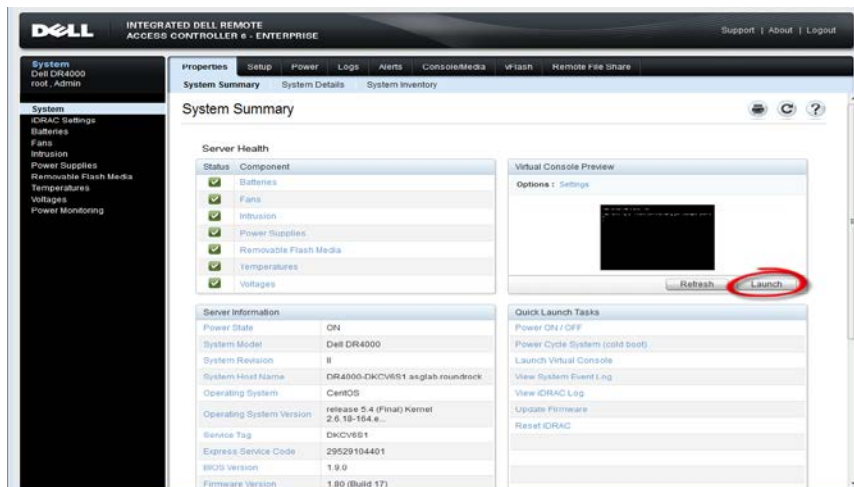


1 Installing and configuring the DR Series system

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



4. Click the **Launch** button to launch the virtual console.



- When the virtual console opens, log on to the system as:
user: **administrator**, password: **St0r@ge!**

NOTE: The "0" in the password is the numeral zero.

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

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

- 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:
```

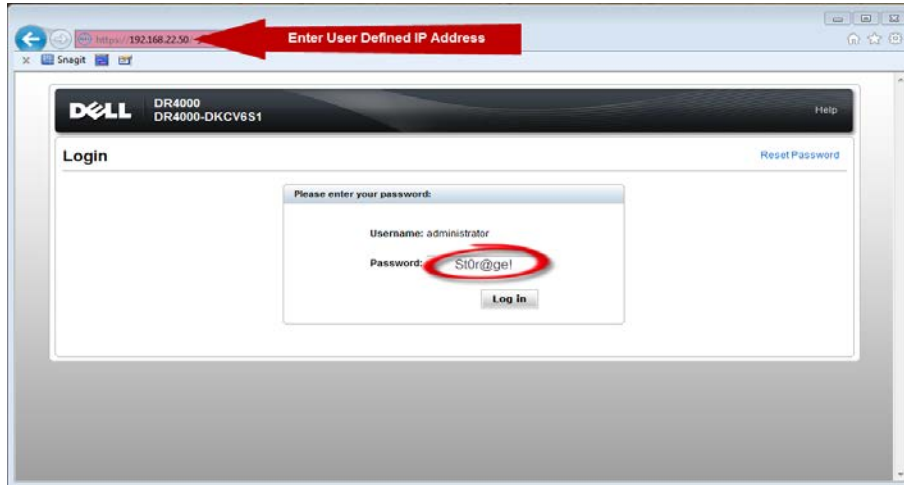
- View the network preferences summary and confirm if the settings are correct.

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



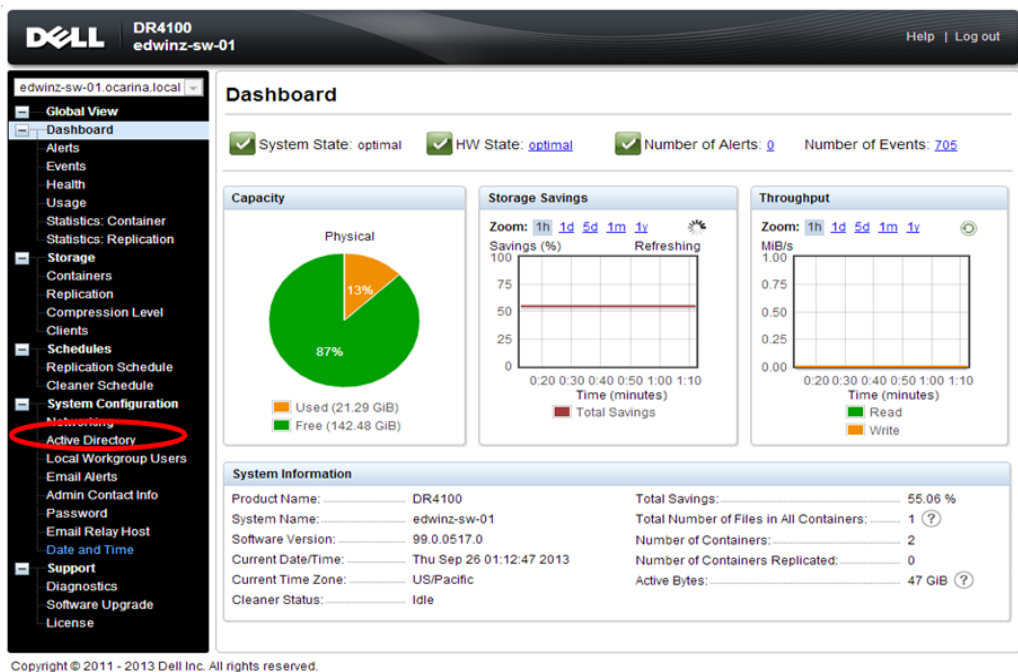
8. Log on to the DR Series system administrator console, using the IP address you just provided for the DR Series system as:
user: **administrator**, password **St0r@ge!**



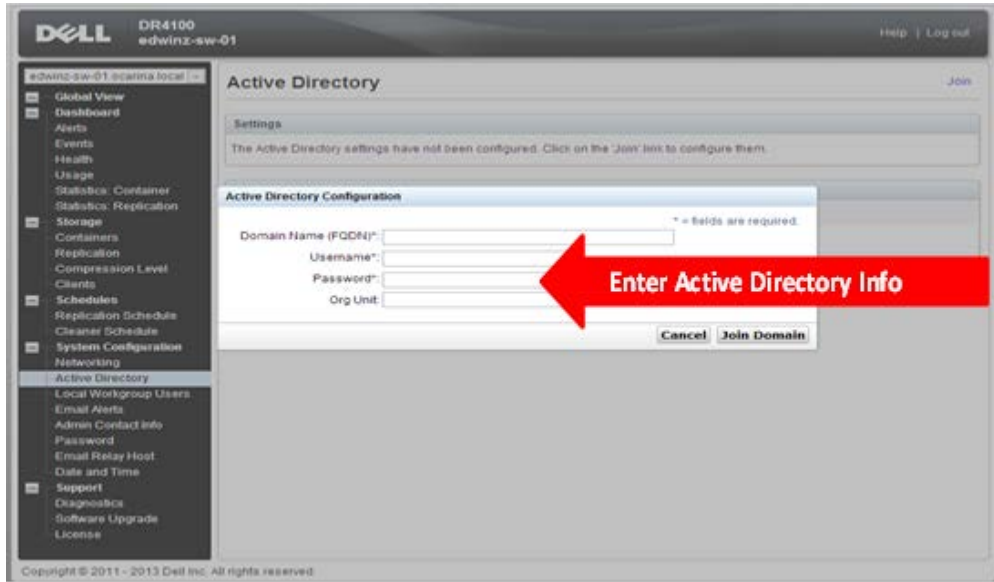
9. Join the DR Series system to Active Directory.

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 area of the GUI.



b. Enter your Active Directory credentials to join the DR Series system to a domain.



2 Creating and configuring CIFS target container(s) for Networker

2.1 Creating the network share container for Networker use

1. Create and mount the container by selecting **Containers** in the navigation area of the GUI, and then clicking **Create** at the top of the page.

The screenshot shows the Dell DR4100 ootb-config-01 GUI. The navigation menu on the left includes: Dashboard, Alerts, Events, Health, Usage, Statistics: Container, Statistics: Replication, Storage, Containers, Replication, Compression Level, Clients, Schedules, Replication Schedule, Cleaner Schedule, System Configuration, Networking, Active Directory, Local Workgroup Users, Email Alerts, Admin Contact Info, Email Relay Host, Date and Time, Support, Diagnostics, Software Upgrade, License. The main content area is titled 'Containers' and features a 'Create' button (highlighted with a red box), 'Edit', 'Delete', and 'Display Statistics' links. Below the header, it states 'Number of Containers: 7' and 'Container Path: /containers'. A table lists the containers:

Containers	Files	NFS	CIFS	OST	Replication	Select
backup	58	✓	✓		Not Configured	⊙
d2d2t	2			✓	N/A	⊙
DDTest	0	✓	✓		Online	⊙
demo2Zhuhai	22	✓	✓		Not Configured	⊙
My_Container_Backup	27	✓	✓		Not Configured	⊙
nfs	44	✓			Not Configured	⊙
ootb-ost-test	254			✓	N/A	⊙

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

2. Enter a Container Name, select the Marker Type as **Networker**, and select the Connection Type as **NFS/CIFS**.

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

3. Under the **CIFS** section, note down the **CIFS share path** (this will be used in configuring the device on the Networker server), and select **Enable CIFS**. For the Client Access section, select either **Open Access** or manually add clients to the Clients 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:

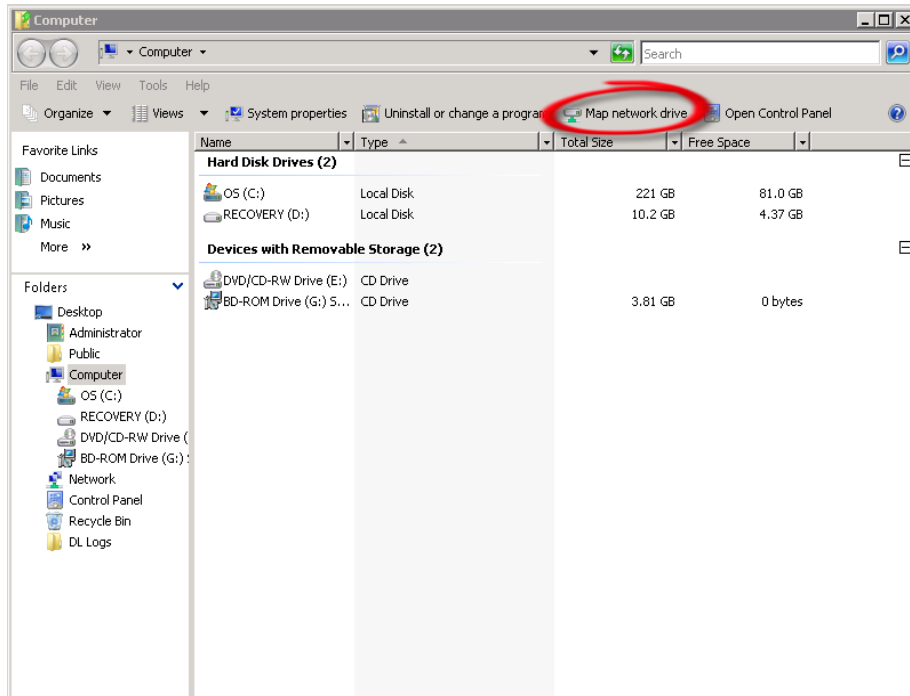


Note: For improved security, Dell recommends adding IP addresses for the backup console (Networker Server), Networker storage nodes, and Networker clients. Not all environments will have all components.

4. Click Create a New Container and confirm that the container is added.

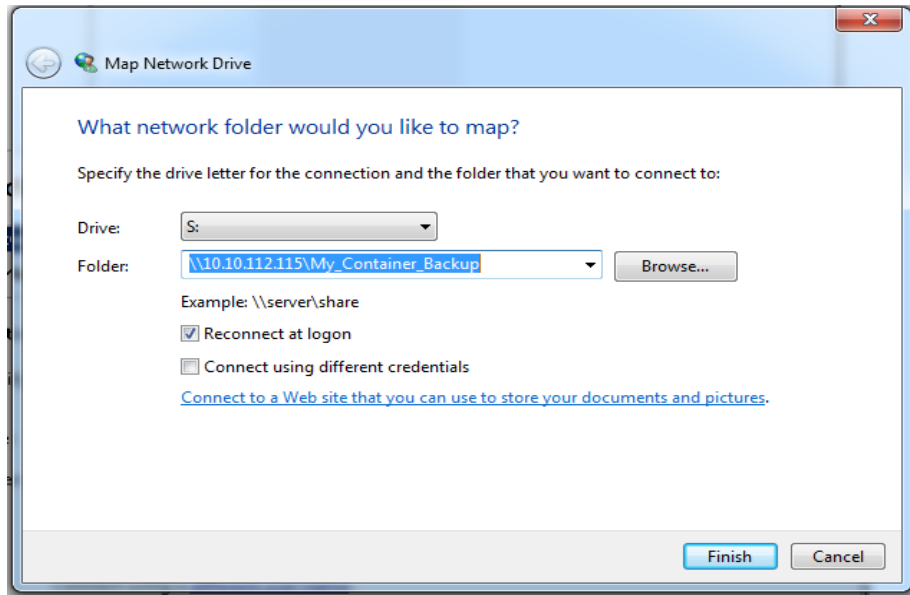
2.2 Configuring the Networker storage node – Windows CIFS

1. Log on to the storage node and click **Start > My Computer**.
2. Click **Map network drive**.



3. In the **Map Network Drive** window, in the **Folder** field, enter the path to the container on the DR Series system.

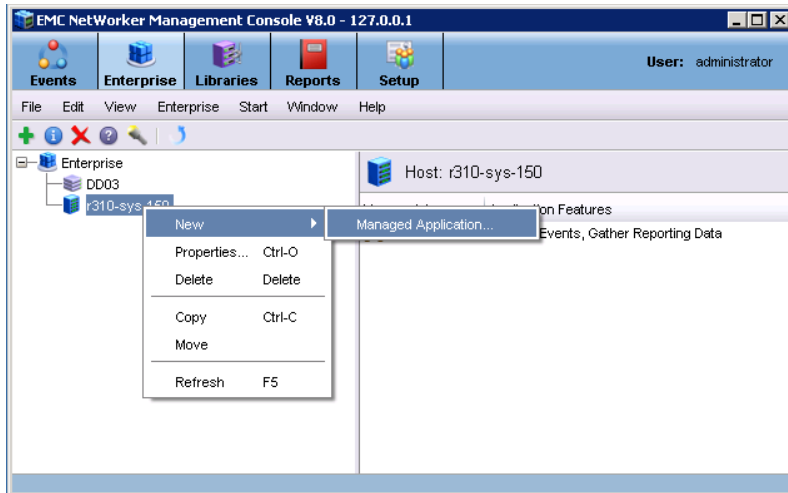




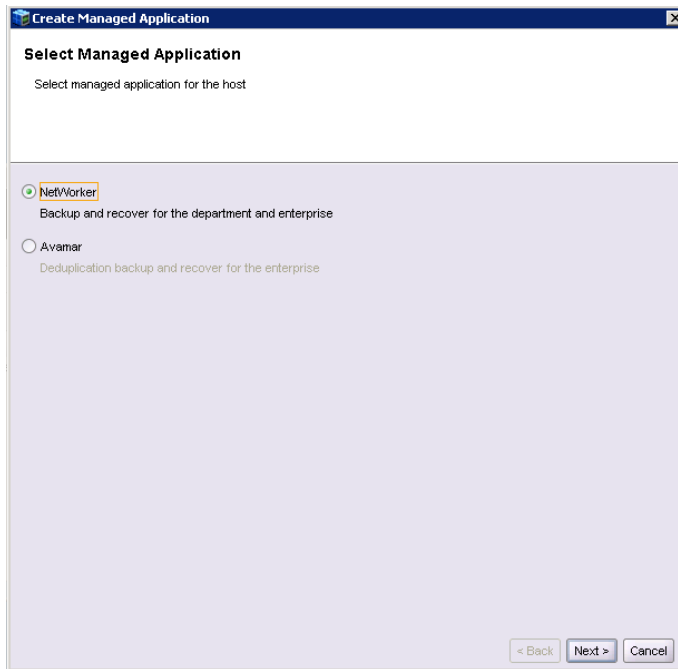
4. Select **Reconnect at logon**.
5. When prompted, enter the CIFS credential to authenticate on the Active Directory domain. The DR Series system container is now mounted to your backup server.
6. If Client Direct is used, make sure all the clients can access the same DR container share using this path. Otherwise, separate **Client Direct Paths** must be entered 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**).

2.3 Configuring Networker to use the newly created network share

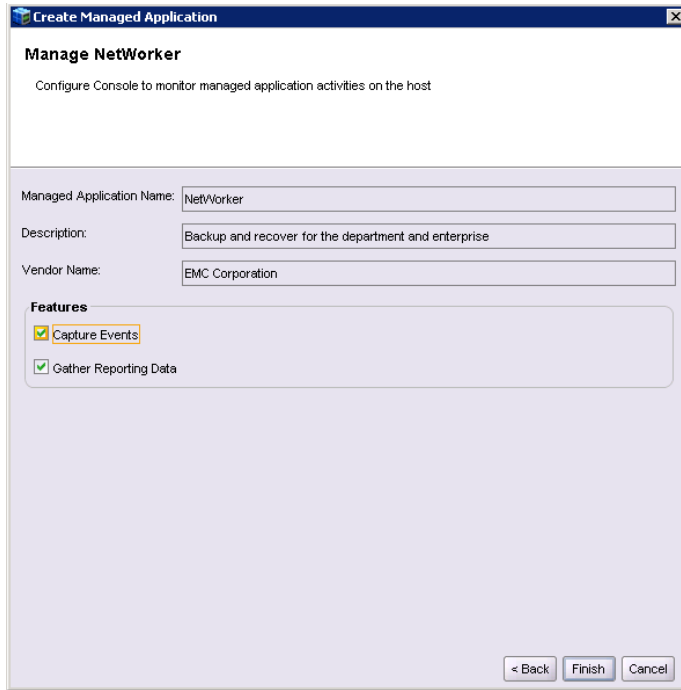
1. Open the **Networker Management Console (NMC)**.
2. Click the **Enterprise** menu button, select the storage node that the DR Series system share will be configured as a backup device, right-click the host, and then click **New > Managed Application**.



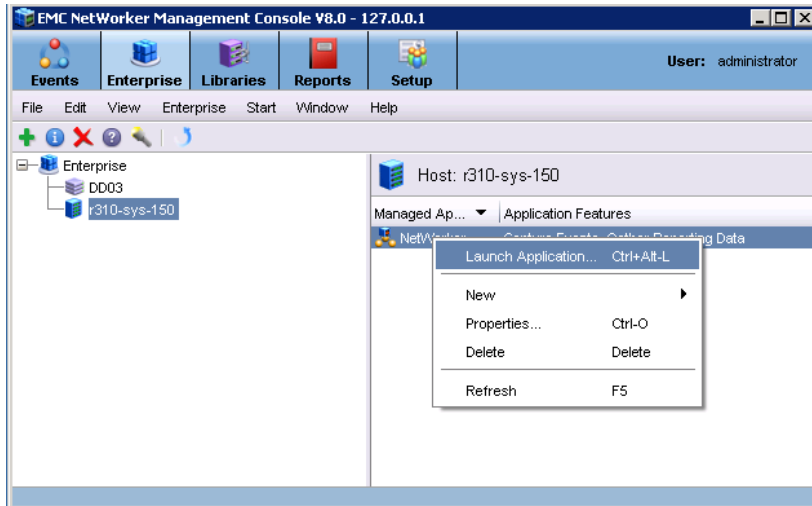
3. Select **NetWorker** and click **Next**.



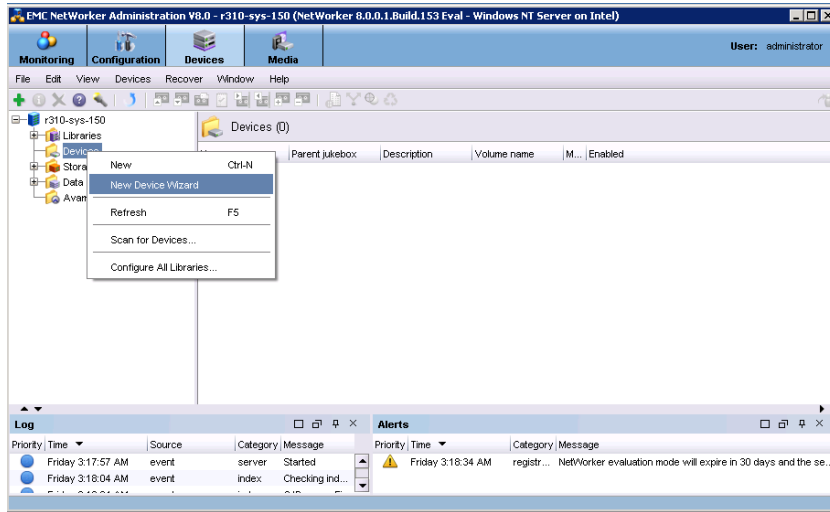
4. Click **Finish**.



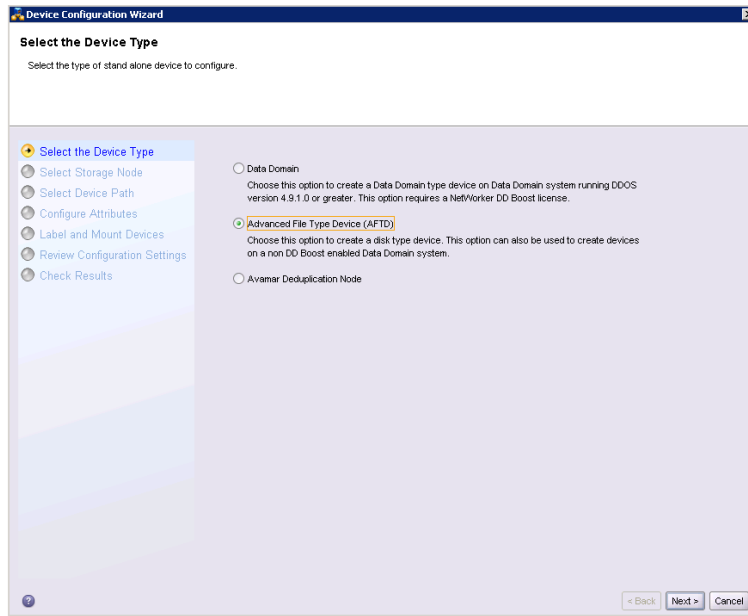
5. Right-click and select the newly created NetWorker application and click **Launch Application**.



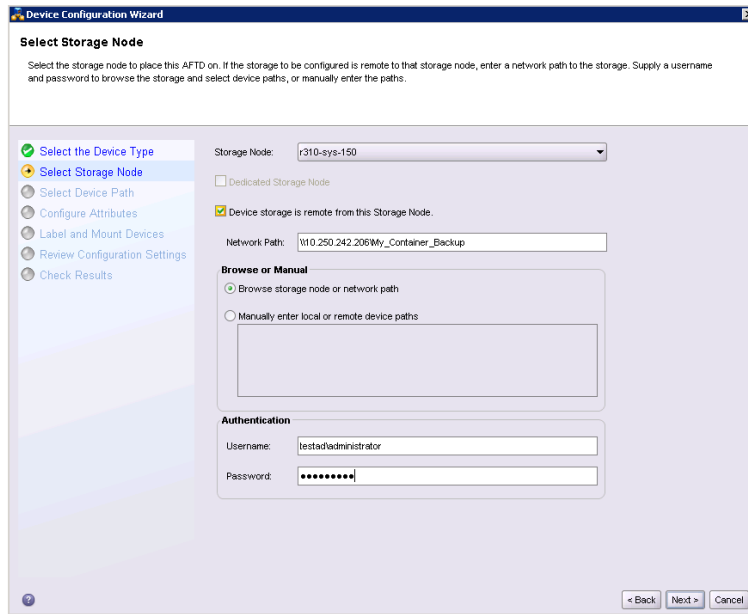
6. In the Devices window, right-click **Device** in the left panel and click **New Device Wizard**.



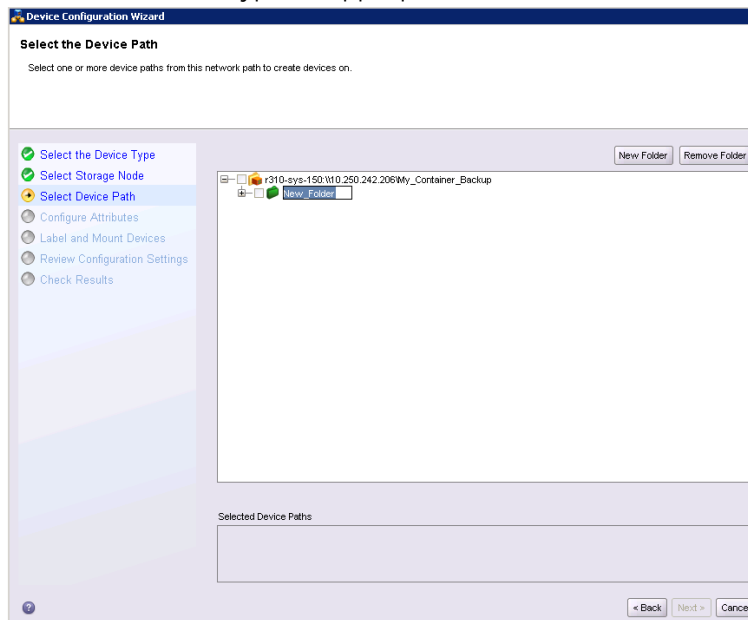
7. Select **Advanced File Type Device (AFTD)**.

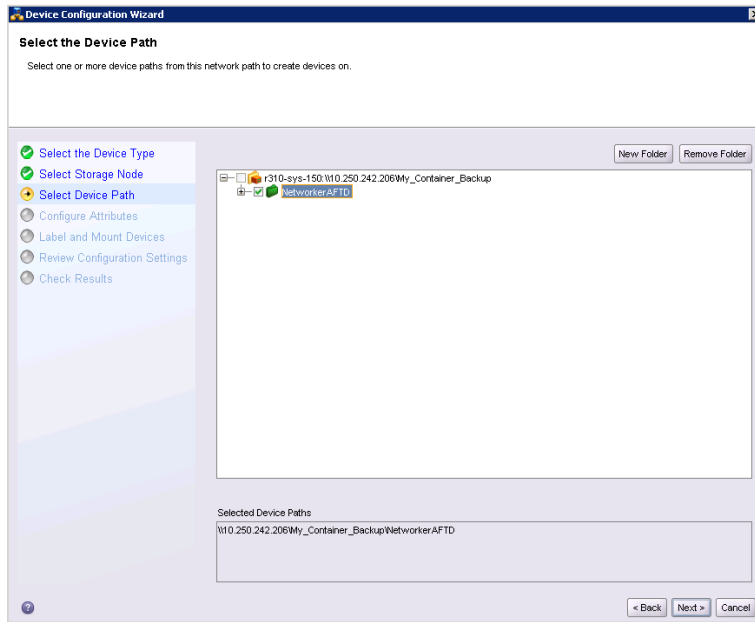


8. In the next dialog box, select **Device storage is remote from this Storage Node**, type in the network path of the DR Series system container share location (if name resolution works, the hostname or FQDN can be used in the server portion of the network path). In the Authentication section, type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



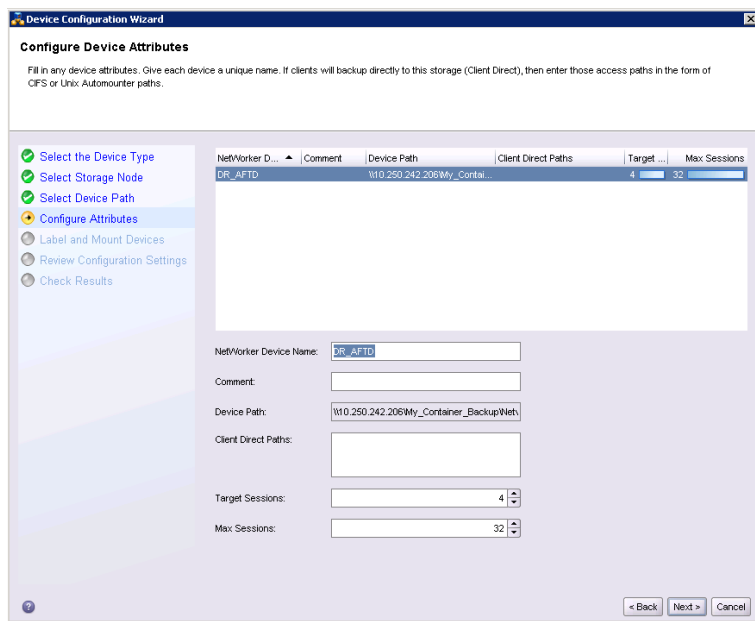
9. Click **New Folder**, type an appropriate folder name, select the folder, and click **Next**.



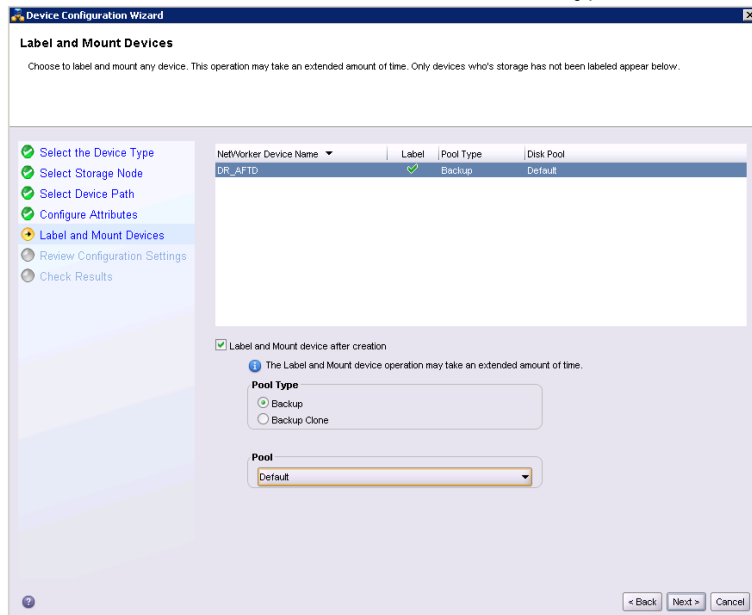


10. Set the session attributes according to the Networker administration documentation and click **Next**.

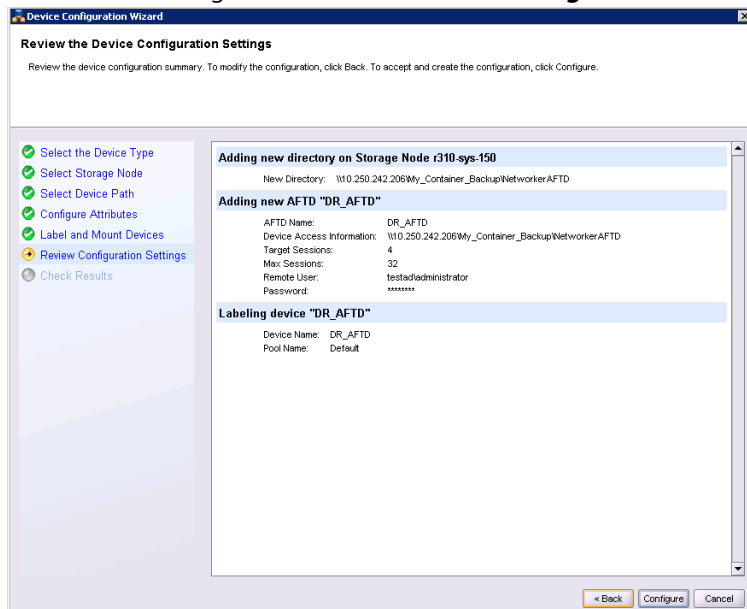
If the Client Direct feature will be used, different device path(s) that clients use to access the DR Series system container share can be entered into the **Client Direct Paths** (please refer to step 6 in the last section **Configure Networker Storage Node**). If all of the clients are able to access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



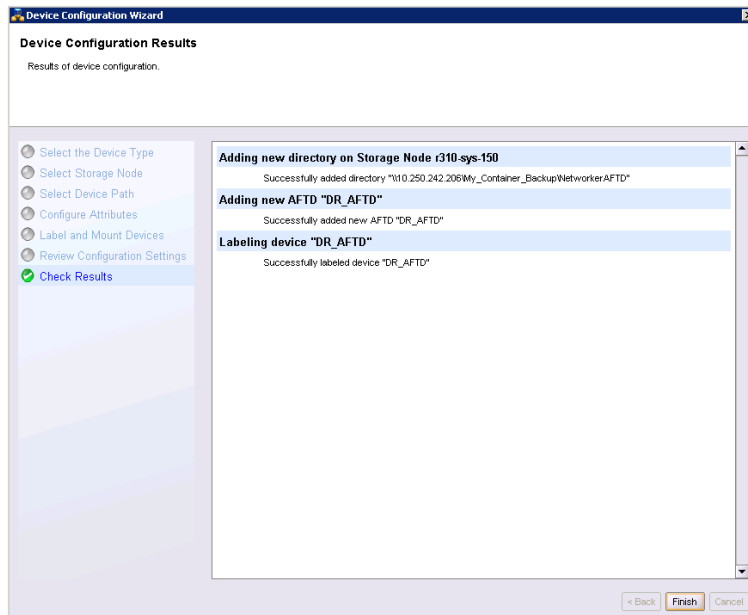
11. The new Networker device should have Pool Type set to **Backup**. Click **Next**.



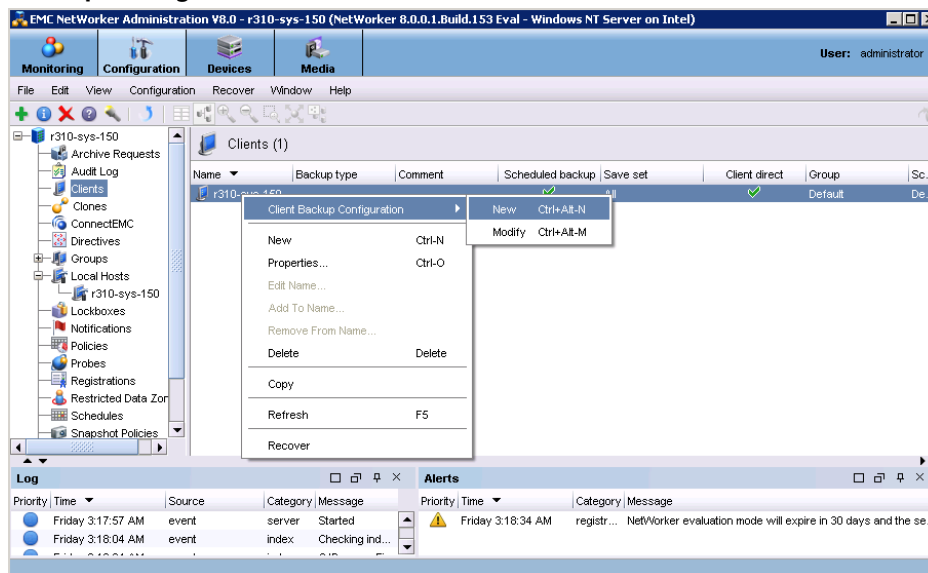
12. Review the configuration and then click **Configure**.



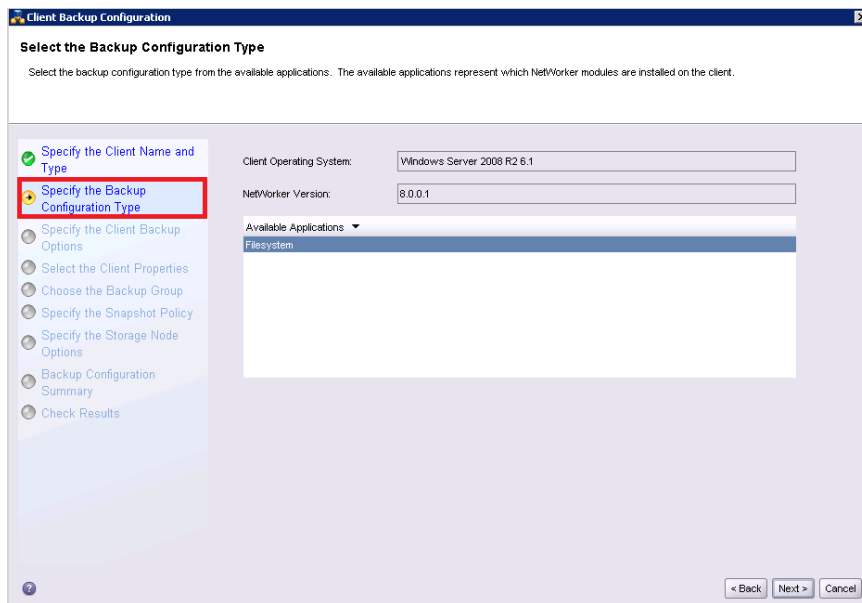
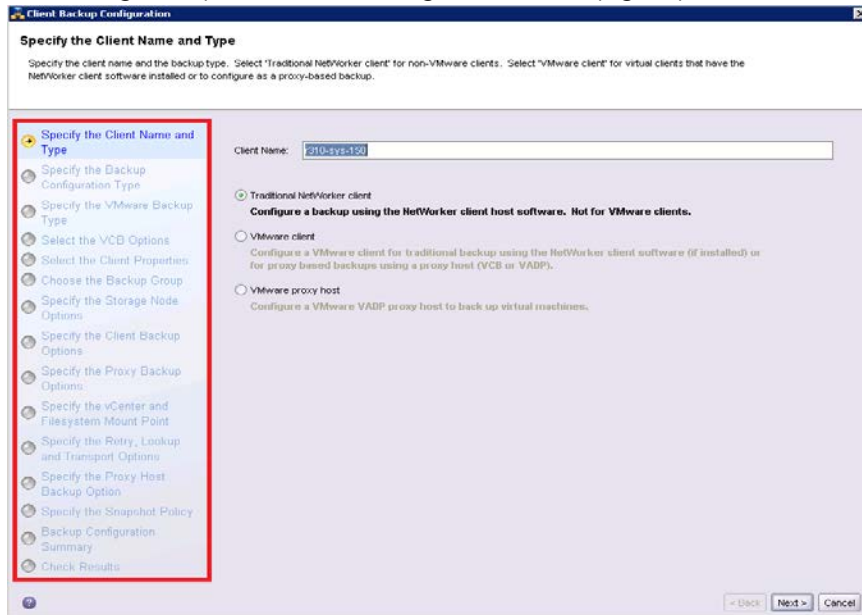
13. Click **Finish**.



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

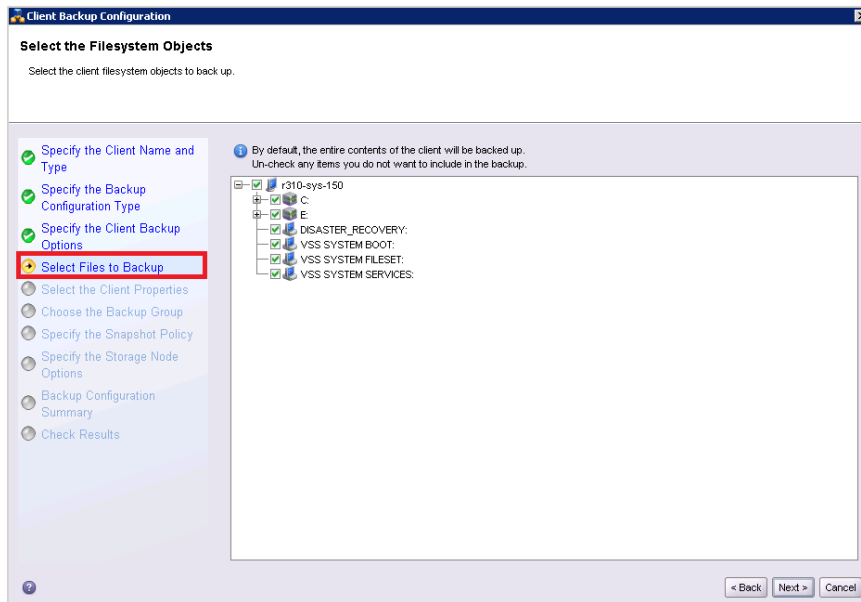
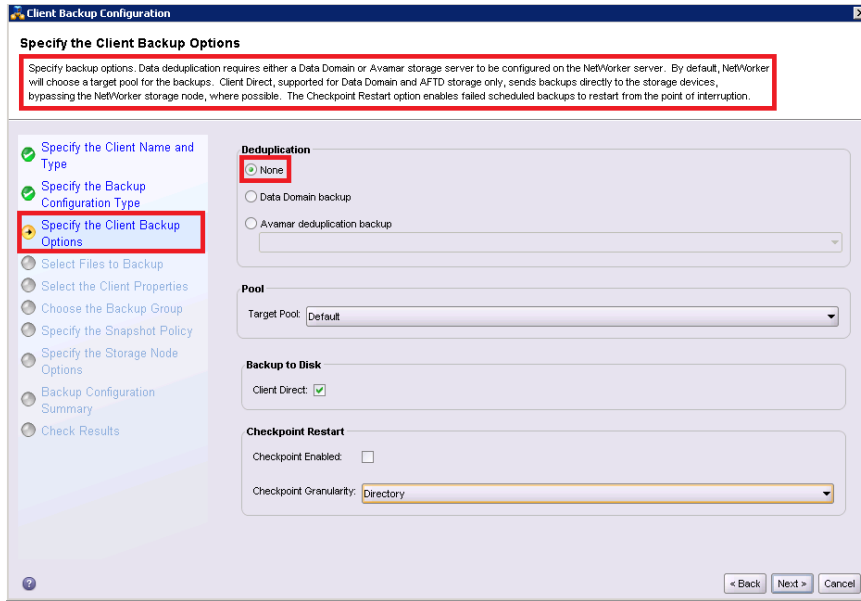


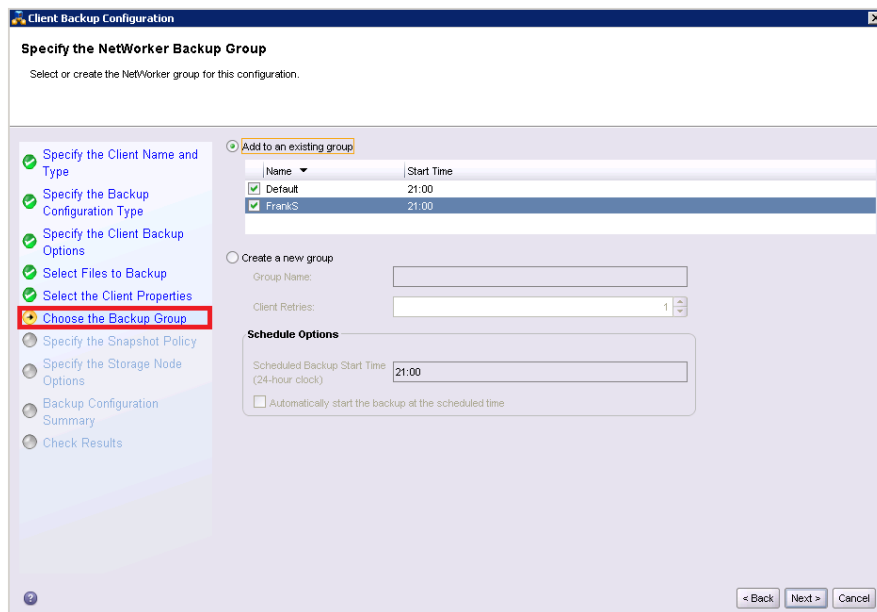
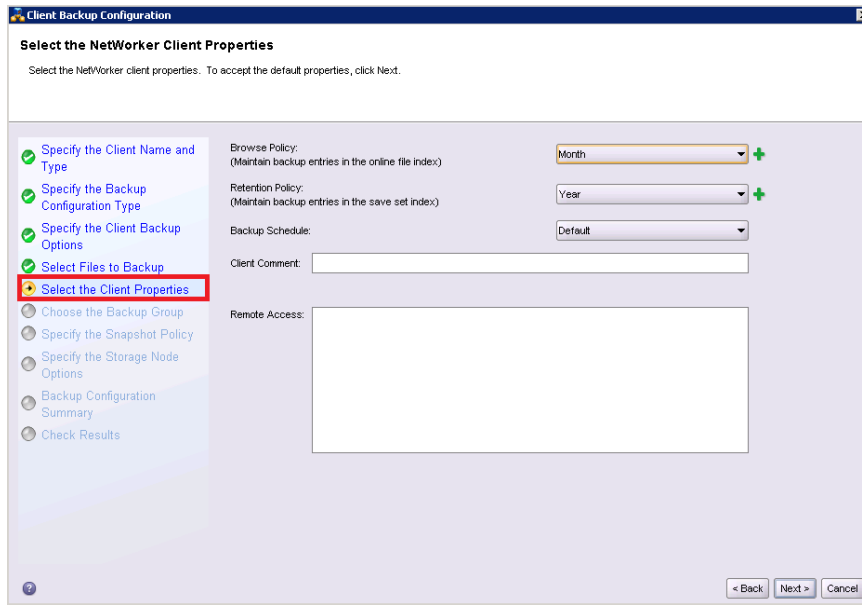
15. Go through the process of creating a new backup group.

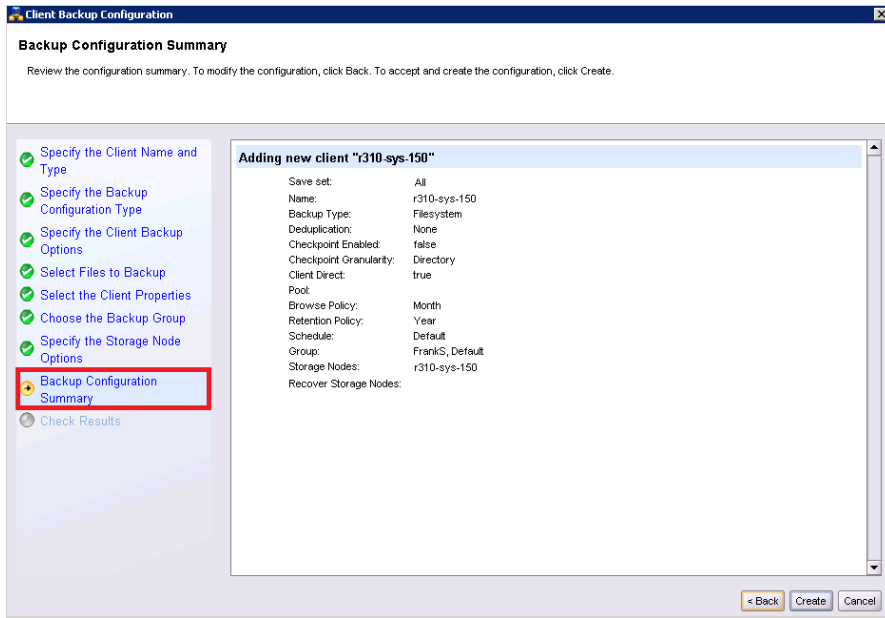
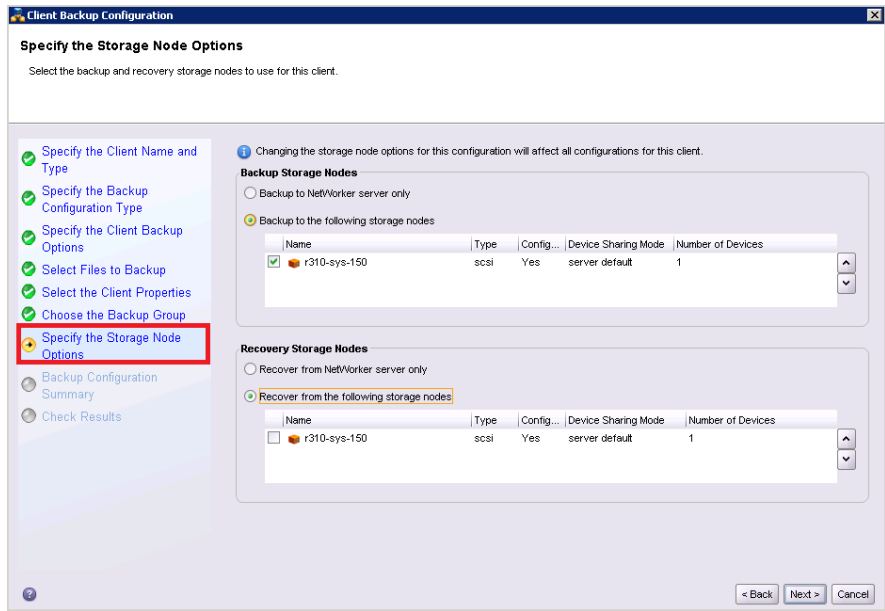


16. In Specify the Client Backup Options, define the following settings as follows.
- Deduplication** should be set as **None**
 - Target Pool** should be set as the pool that has the DR Series system device included.
 - Client Direct** can be enabled if the client is directly backing up data to a preferred DR, thus bypassing the storage node that is 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. Refer to step 6 in the last section **Configure the NetWorker Storage Node**, and step 10 in this section.

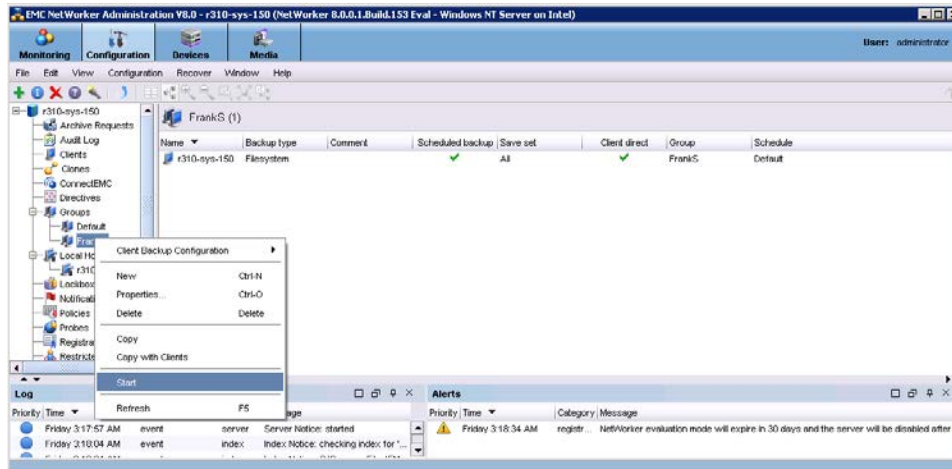




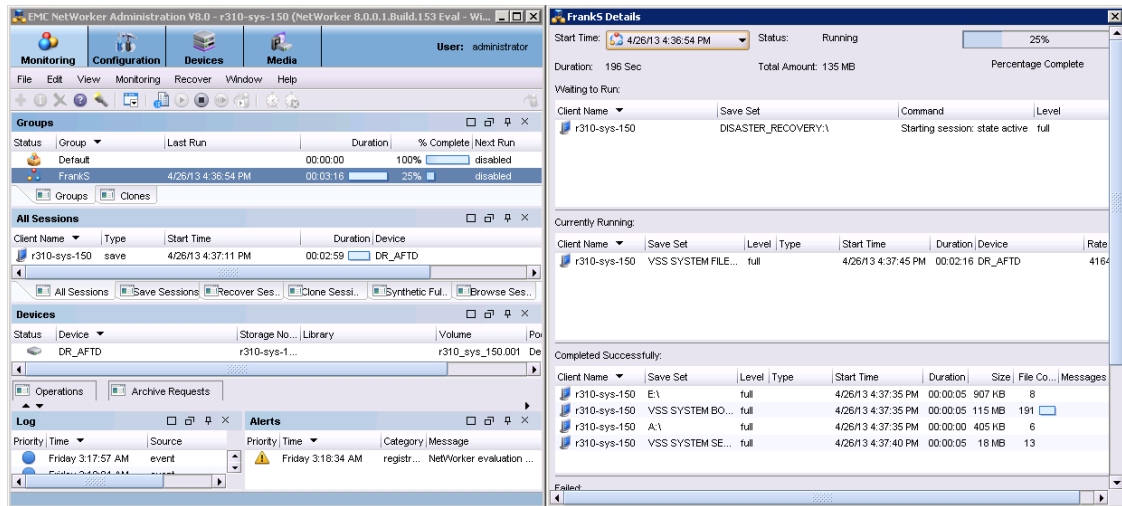




17. After the backup group is successfully created, click **Start** to start the backup.



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



2.4 Setting up DR Series system replication and restore from the replication target

2.4.1 Creating a replication relationship between two DR Series systems

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

The screenshot shows the Dell DR4100-VM web interface for the source system. 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.

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 Series system.

The screenshot shows the Dell DR4100-VM web interface for the target system. 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.

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

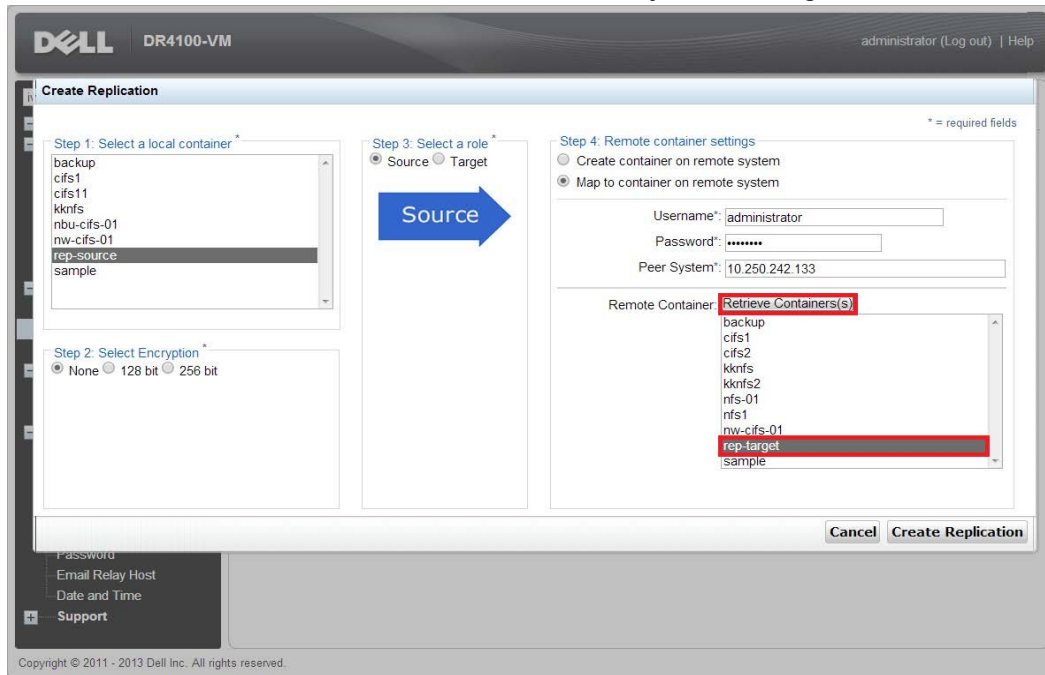
Copyright © 2011 - 2013 Dell Inc. All rights reserved.

- Select the newly created container as the source container, and then enter the target DR Series system information.

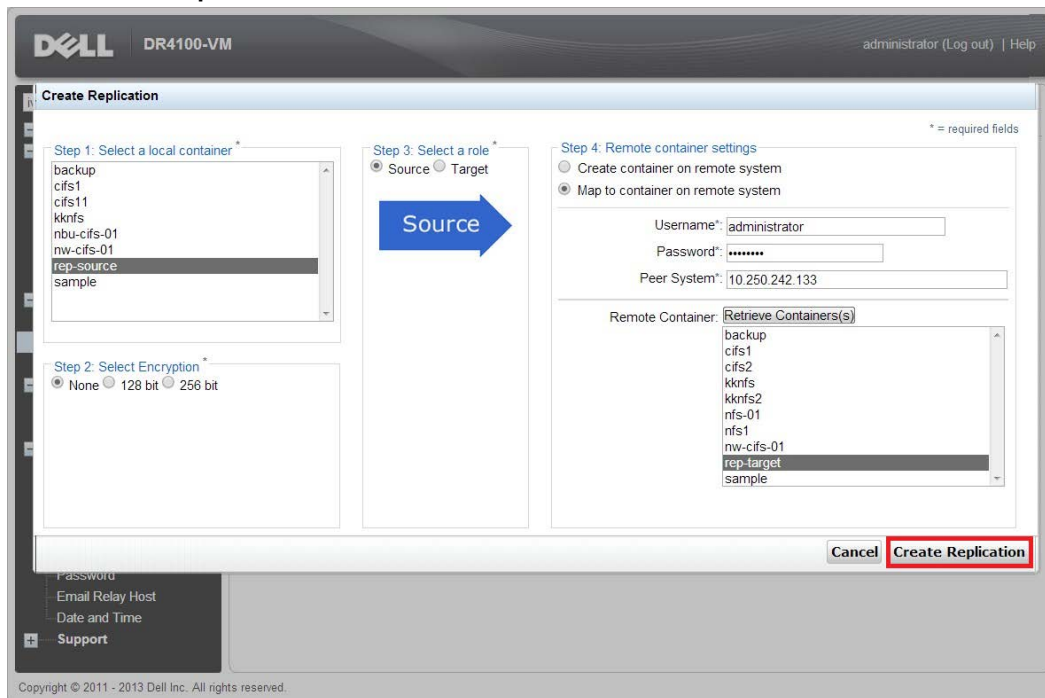
Copyright © 2011 - 2013 Dell Inc. All rights reserved.



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



6. Click **Create Replication**.



- Verify that the replication relationship between the DR Series systems has been created and that the **Peer Status** is **Online**.

The screenshot shows the Dell DR4100-VM management interface. The top header includes the Dell logo, the system 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, System Configuration, and Support. The main content area is titled 'Replication' and includes a sub-header with links: 'Create | Edit | Delete | Stop | Start | Bandwidth | Display Statistics'. Below this, it states 'Number of Source Replications: 3'. A table lists the replication relationships:

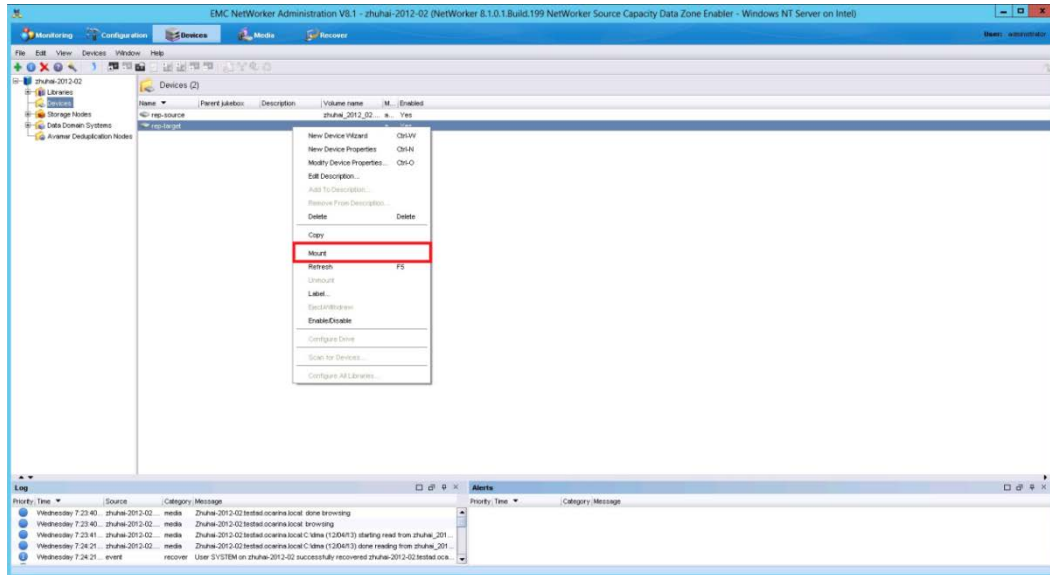
Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nvbu	source	10.250.243.18 nvbu	Stopped	Default	<input type="radio"/>
nvbu1	source	10.250.243.18 nvbu1	Online	Default	<input type="radio"/>
rep-source	source	10.250.242.133 rep-target	Online	Default	<input checked="" type="radio"/>

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



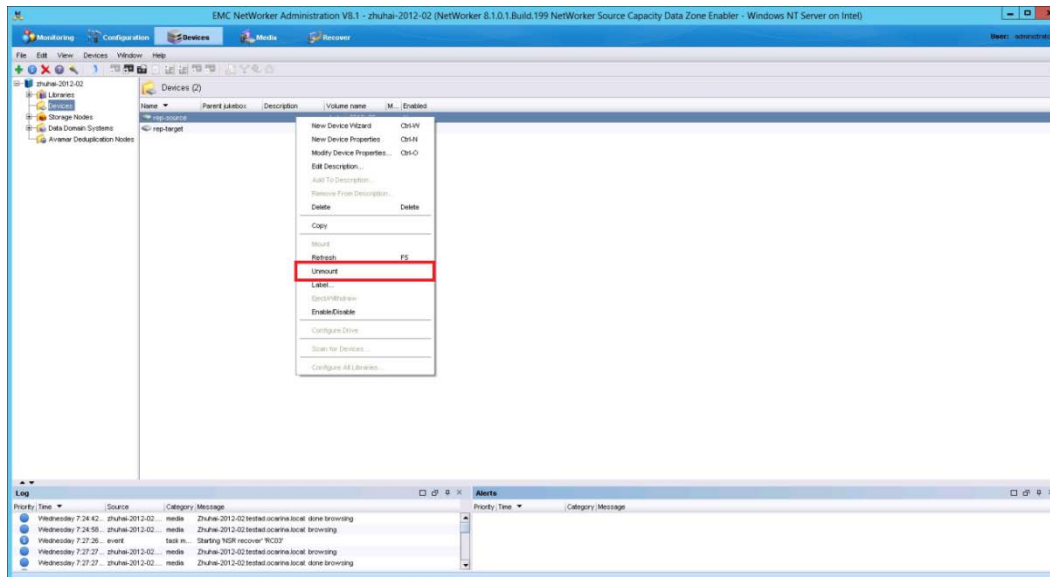
2.4.2 Restoring from the replication target container

1. Add the target container onto the Networker storage node. Right-Click **Device** > **New Device Properties**, and then enter necessary information for the target device. When complete, mount the device.

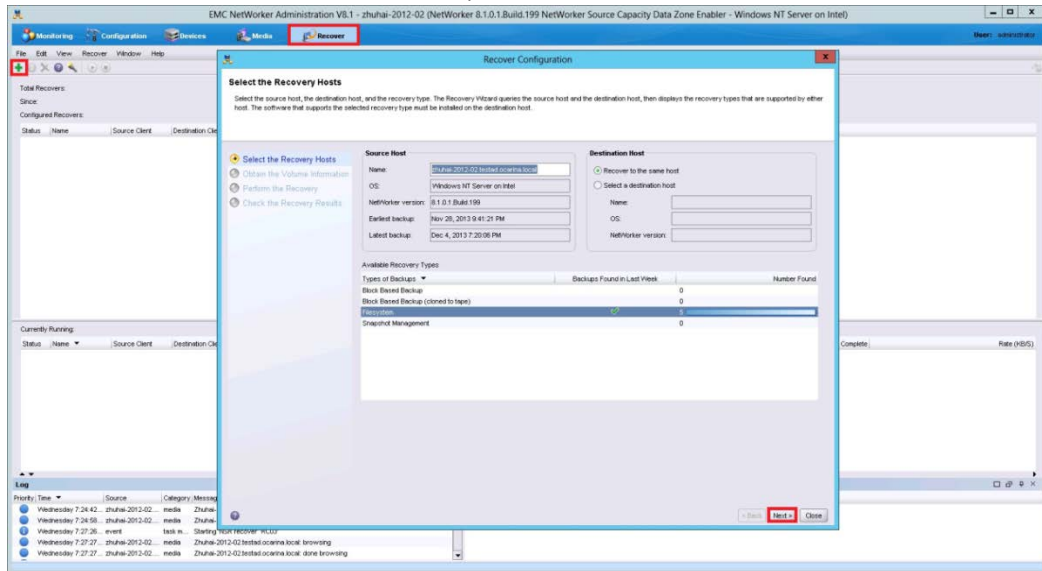


NOTE: Do not label the target device.

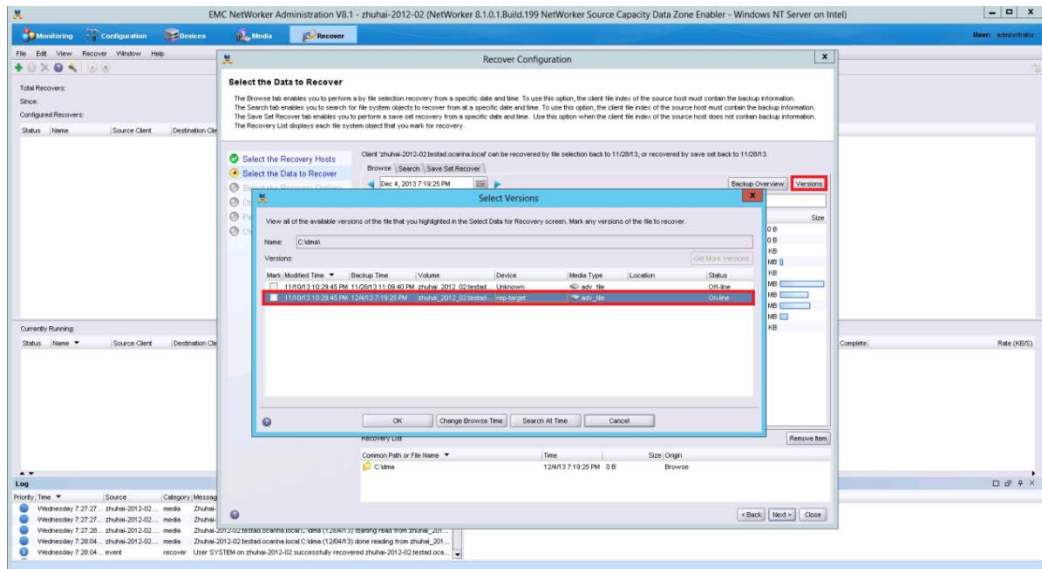
2. Unmount the source container.



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



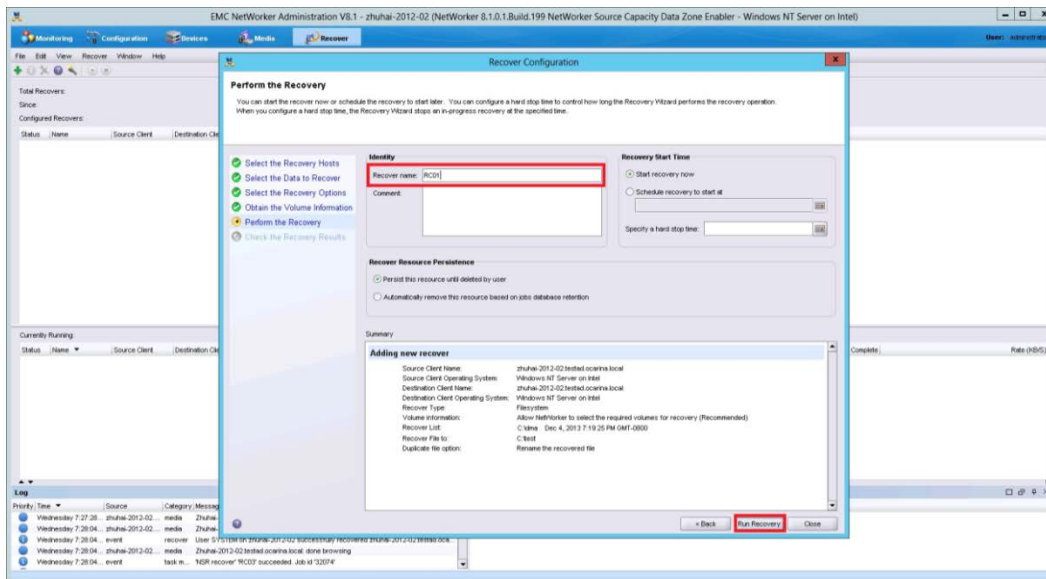
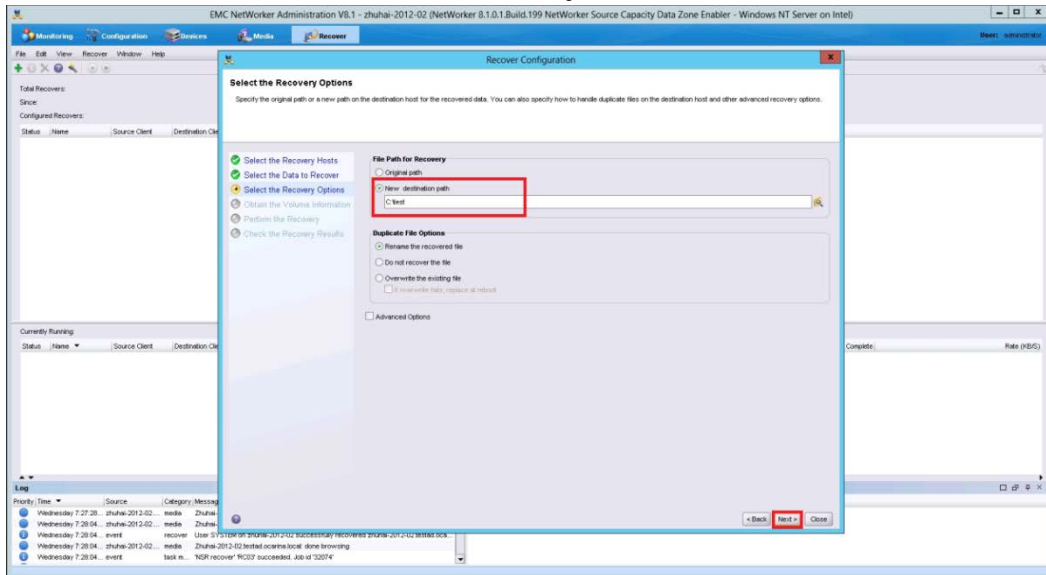
- Select the data set to recover, click **Versions** to view the **Select Versions** window, select the data, and click **OK**.



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



6. Enter a **Recover name**, and click **Run Recovery**.



7. Check the Recovery Results.

The screenshot shows the EMC NetWorker Administration V8.1.1 interface. The main window is titled "Recover Configuration" and displays the "Check the Recovery Results" dialog box. The dialog box contains the following information:

- Recover Name:** RC01
- Size:** 1873 MB
- Status:** Succeeded
- Source Client:** zhuhai-2012-02\tested.ocarma.local
- Completed:** 1873 MB
- Start time:** Dec 6, 2013 1:20:01 AM
- Duration:** 00:04:26
- Drives:** rep-target
- Volumes used:** zhuhai_2012_02\tested.ocarma.local\003

The dialog box also includes a "Recovery Log" section with a list of files and folders, and a "Log" section with system messages. The "Log" section shows the following messages:

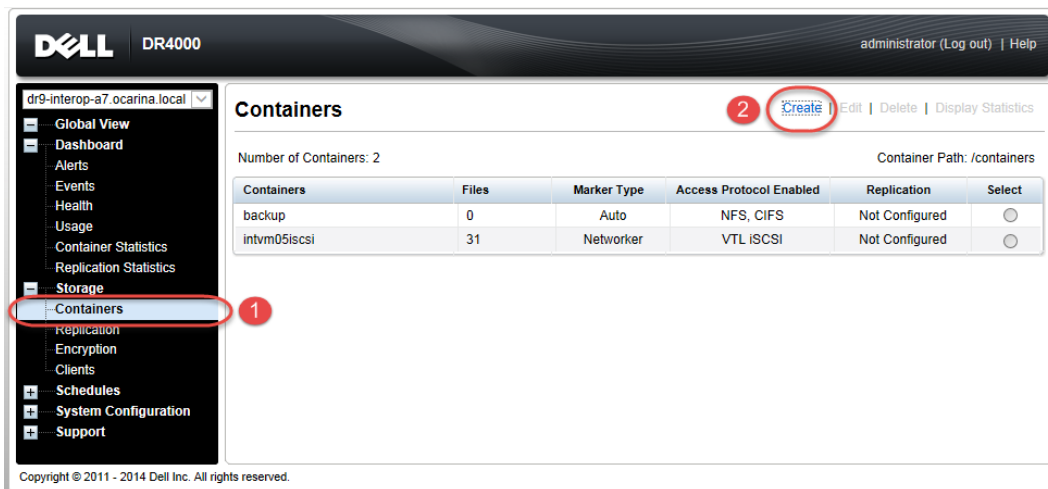
- Wednesday 7:30:19 zhuhai-2012-02 media Zhuhai
- Wednesday 7:30:20 zhuhai-2012-02 media Zhuhai
- Wednesday 7:30:54 zhuhai-2012-02 media Zhuhai-2012-02\tested.ocarma.local (1/2047) 3098166091 from zhuhai_001
- Wednesday 7:30:55 event recover User SYSTEM on zhuhai-2012-02 successfully recovered zhuhai-2012-02\tested.oc...
- Wednesday 7:30:55 zhuhai-2012-02 media Zhuhai-2012-02\tested.ocarma.local done browsing



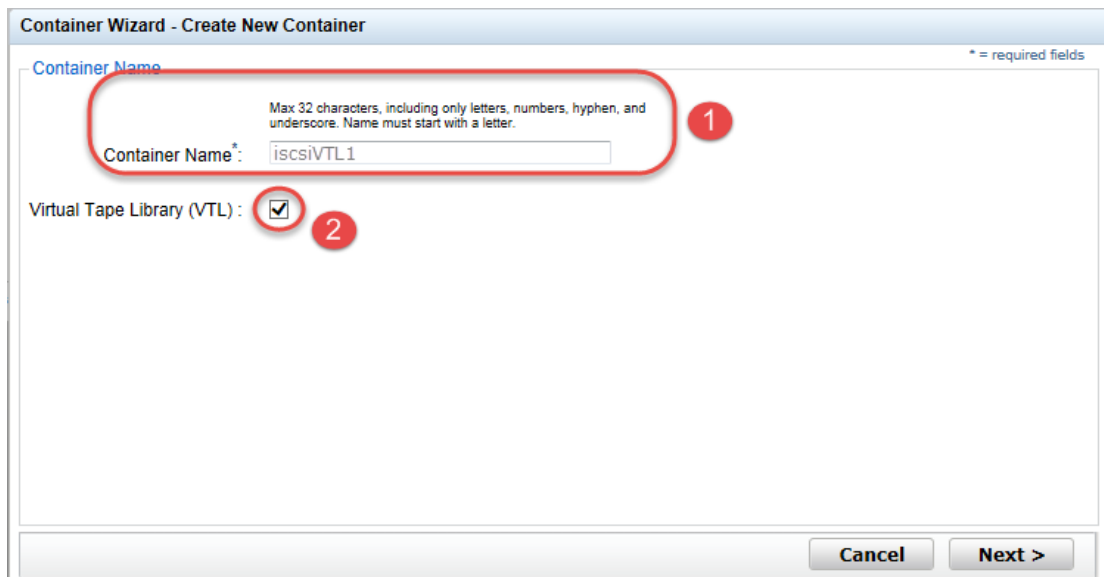
3 Creating and configuring iSCSI target container(s) for Networker

3.1 Creating an iSCSI VTL container for Networker use

1. Create and export the iSCSI container by selecting **Containers** in the left navigation pane of the DR Series system GUI, and click **Create** at the top of the page.



2. Enter a container name and select the **Virtual Tape Library (VTL)** container option. Click **Next**.



3. Select the iSCSI **Access Protocol**. Specify the DMA **Access Control** by providing the storage node / media node IP Address, IQN or FQDN. For Marker Type, select **Networker**. Click **Next**.

The screenshot shows the 'Configure Virtual Tape Library' step of the 'Container Wizard - Create New Container' dialog. The 'Container Name and Type' section on the right shows 'iscsiVTL1' and 'VTL'. The 'Access Protocol' is set to 'iSCSI' (marked with a red circle 1). The 'Access Control (initiator)' field contains 'iqn.1991-05.com.microsoft:2k8r2intvm05' (circled in red with a red circle 2). The 'Marker Type' is set to 'Networker' (marked with a red circle 3). Other options include 'Tape Size' (800GB, 400GB, 200GB, 100GB, 50GB, 10GB), 'Access Protocol' (NDMP, No Access), and 'Marker Type' (Unix Dump, BridgeHead, Time Navigator, None, Auto). At the bottom are '< Back', 'Cancel', and 'Next >' buttons.

4. Click **Create a New Container**.

The screenshot shows the 'Configuration Summary' step of the 'Container Wizard - Create New Container' dialog. It displays the configuration details for the container: 'Container Name and Type' (iscsiVTL1, VTL) and 'Virtual Tape Library' (OEM: no, Tape Size: 10gb, Access Protocol: iSCSI, Access Control: iqn.1991-05.com.microsoft:2k8r2intvm05, Marker Type: Networker). At the bottom are '< Back', 'Cancel', and 'Create a New Container' buttons (the latter is circled in red).

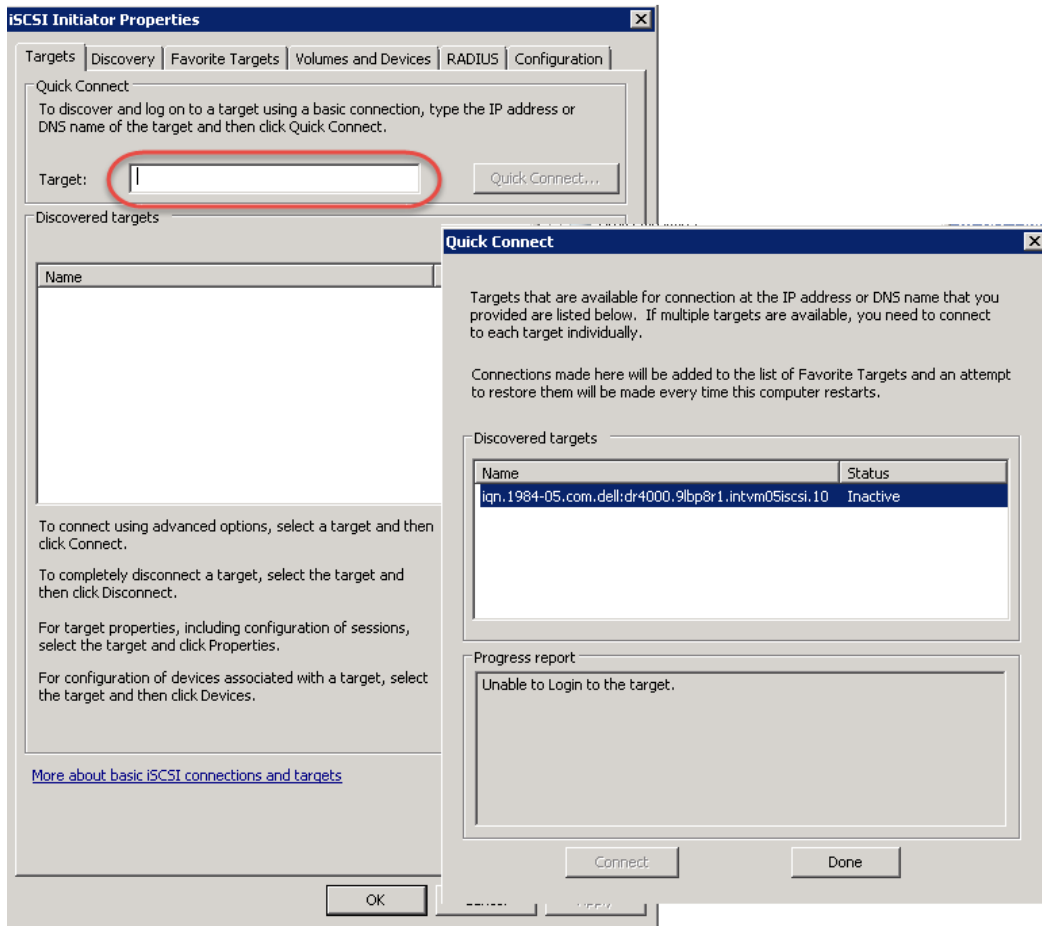


3.1.1 Configuring the iSCSI Networker storage node – Windows

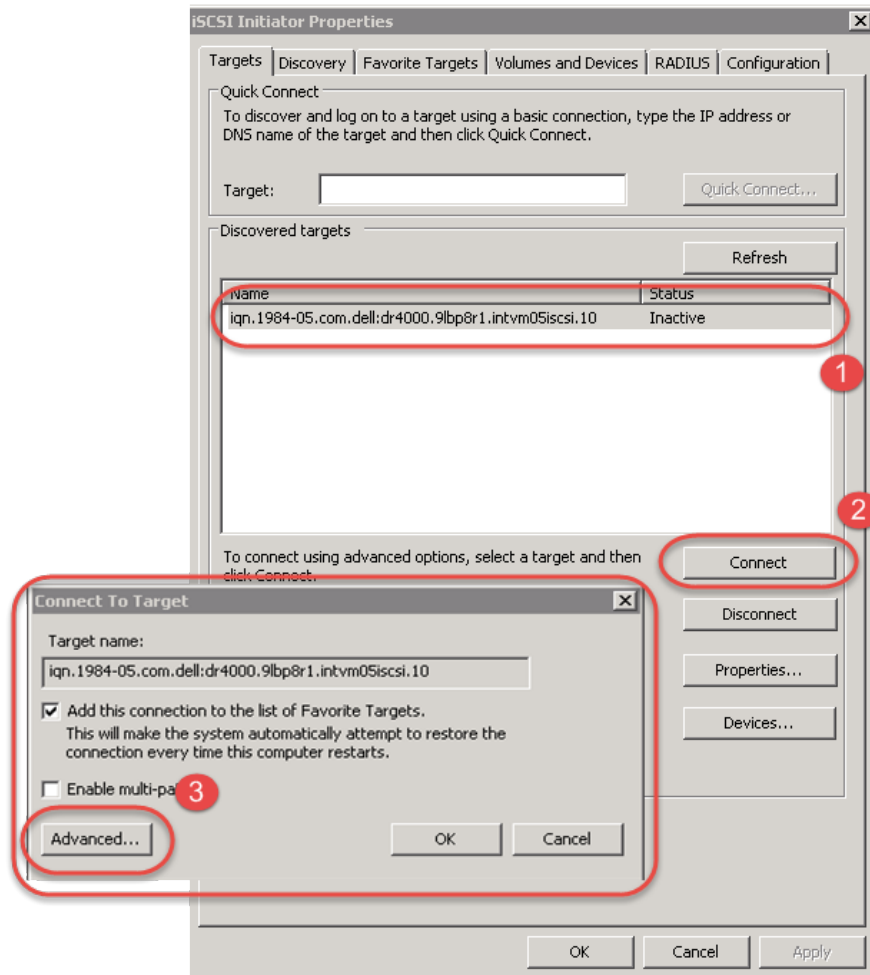
iSCSI initiator configuration is a two-step process, consisting of:

- Target discovery.
- Establishing an iSCSI session with the target using CHAP authentication.

1. Provide the IP or FQN of the DR Series system in the **Target** field. Click **Quick Connect**, which results in target discovery. The Quick Connect dialog box lists all available targets on the DR Series system. At this point, the status will be Inactive. Click **Done** and close the dialog box.



2. Close the dialog box and proceed by selecting the newly discovered target. This target will have an **Inactive Status** as it requires authentication parameters to be provided for iSCSI login. Select the Target from the list, click the **Connect** button, and then in the **Connect to Target** dialog box select the **Advanced** button.



3. In **Advanced Settings**, select to **Enable CHAP log on** and type the **User Name** and **Target Secret / Password**. Select **OK** to save the settings. Refer to *Appendix A* for further details about accounts and credentials.

Advanced Settings

General | IPsec

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

Data digest Header digest

Enable CHAP log on **1**

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified. **2**

Name: dr9-interop-a7

Target secret:

Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

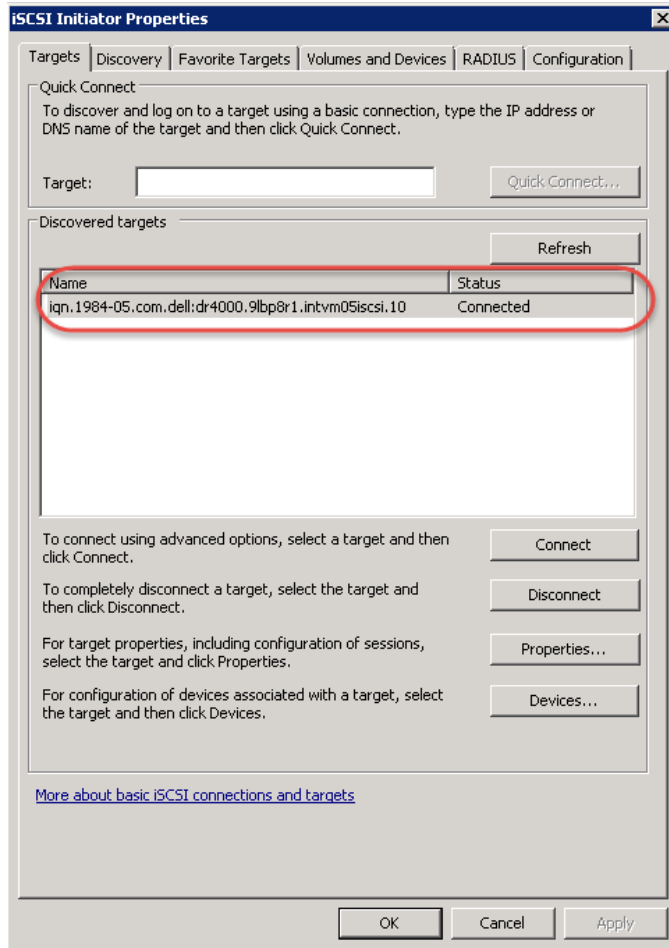
Use RADIUS to generate user authentication credentials

Use RADIUS to authenticate target credentials

OK Cancel Apply

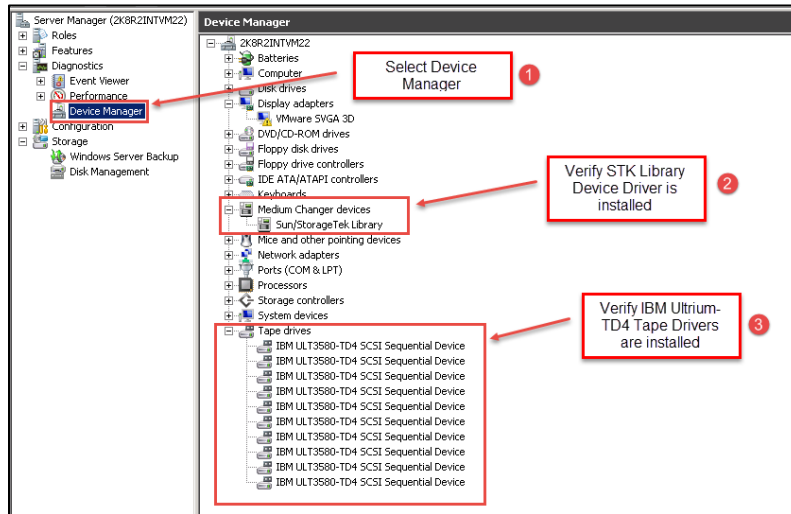


The iSCSI target should now appear as connected and the device discovery can now proceed.



4. Open the **Server Manager Snap-in** and verify that the newly connected devices appear in the **Device Manager**. Verify that the STK Library and IBM Ultrium-TD4 Device Drivers are installed.

Note: (Refer to the link, <http://catalog.update.microsoft.com/v7/site/home.aspx> for information and assistance in acquiring Microsoft Device Drivers , for example, StorageTek Library Drivers).



3.1.2 Configuring the iSCSI target – Linux

Before you begin this procedure, ensure that the iSCSI initiator is installed (iscsi-initiator-utils). For example:

```
yum install iscsi-initiator-utils ; /etc/init.d/iscsi start
```

To configure the iSCSI target for Linux, follow these steps.

1. Add the CHAP Authentication details for the DR Series system on the Linux Initiator as follows:
 - a. Edit /etc/iscsi/iscsid.conf and un-comment the following line:

```
node.session.auth.authmethod = CHAP
```

- b. Modify the following lines:

```
# To set a CHAP username and password for initiator
```

```
# authentication by the target(s), uncomment the following lines:
```

```
node.session.auth.username = iscsi_user
```

```
node.session.auth.password = St0r@ge!iscsi
```

2. Set the Discovery Target Node(s) by using this command:

```
iscsiadm -m discovery -t st -p <IP or IQN of DR>
```



For example:

```
iscsiadm -m discovery -t st -p 10.8.230.108
```

3. Enable login to the DR Series system iSCSI VTL target(s) by using the following command:

```
iscsiadm -m node --portal <IP or IQN of DR:PORT> --login
```

For example:

```
iscsiadm -m node --portal "10.8.230.108:3260" --login
```

4. Display the open session(s) with DR VTL(s) by using the following command:

```
iscsiadm -m session
```

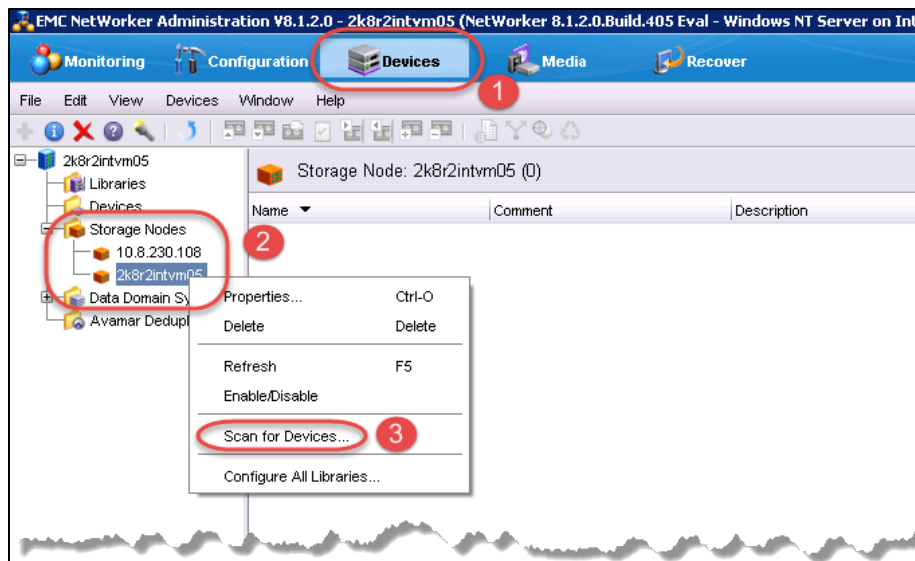
For example:

```
iscsiadm -m session = tcp: [8] 10.8.230.108:3260,1 iqn.1984-05.com.dell:dr4000.3071067.interoprhel52n1.30
```

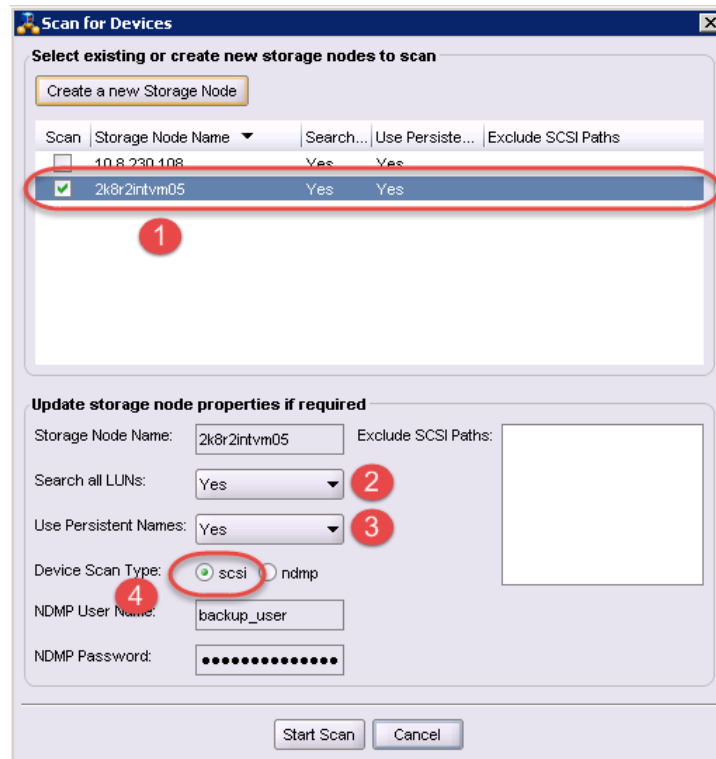
5. Review dmesg or /var/log/messages for details about the tape devices created upon adding the DR Series system iSCSI VTL.

3.2 Setting up Networker to use the newly created iSCSI VTL

1. Access the **Devices** menu within the Networker Administration interface. Select the Storage Node that has had the NDMP VTL configured for access. Select to **Scan for Devices**.

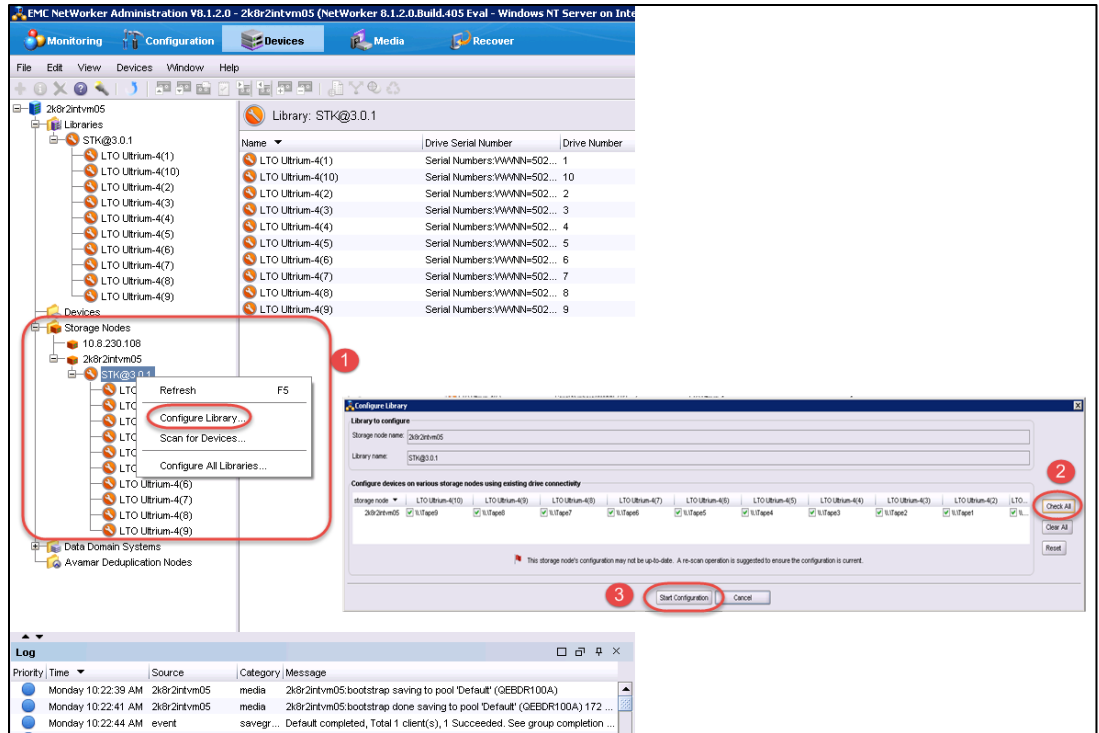


2. In the **Scan for Device** dialog box, select the appropriate storage node with the settings to **Search all LUNs**, **Use Persistent Names** and **Device Scan Type** of **scsi**.

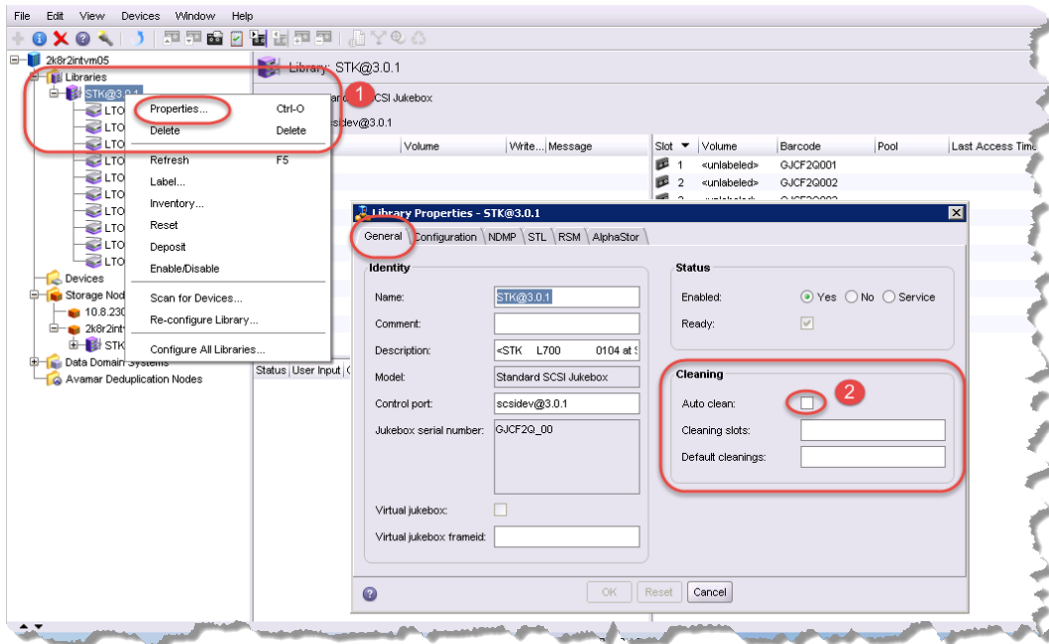


3. After the device scans, the iSCSI VTL should now appear and must be configured for use. Select the library within the **Storage Nodes** navigation tree and proceed with the **Configure Library** option. In the **Configure Library** dialog box, **Check All** drives and click **Start Configuration**.

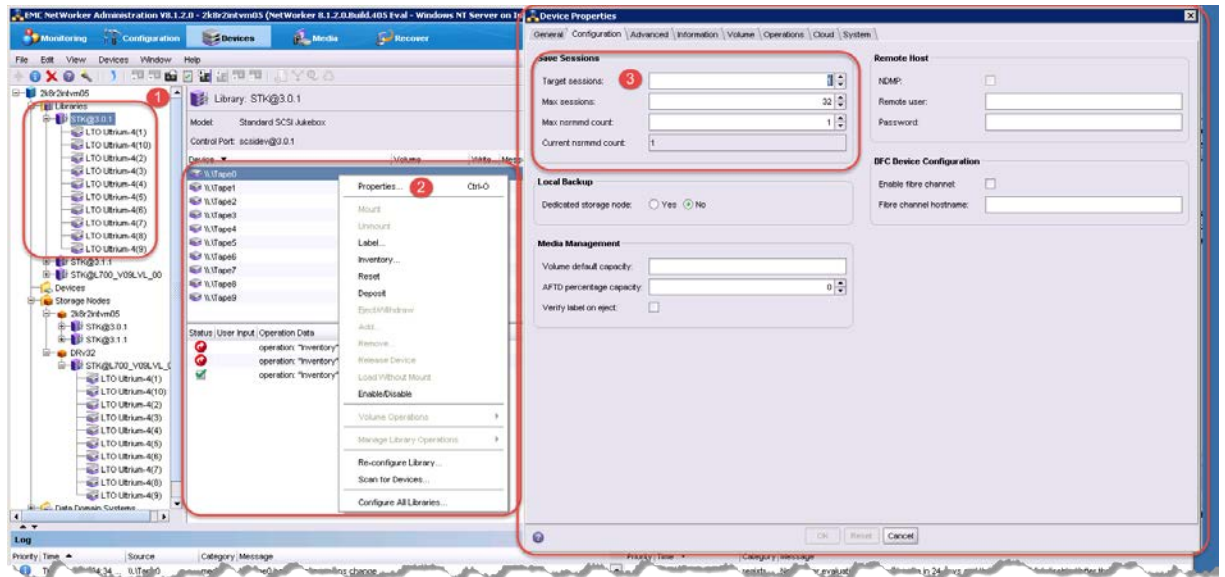




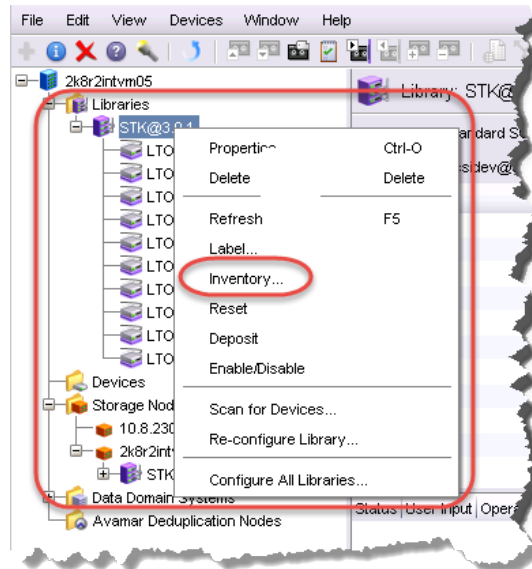
- The VTL should now show up ready for use. By default, the cleaning option is enabled, which must be disabled. Within the navigation tree, select the Library and **Properties** option. In the dialog box, disable the **Auto-clean** option, and omit the default slot and cleanings settings. Click **OK** to save the changes.



- After the library has been configured, the individual tape drives must be configured so that they service only one target session at any given time. Multiplexing to virtual tape drives has an adverse effect on deduplication and thus requires that each drive only handle a single target session.



- Conduct a full inventory of the library.



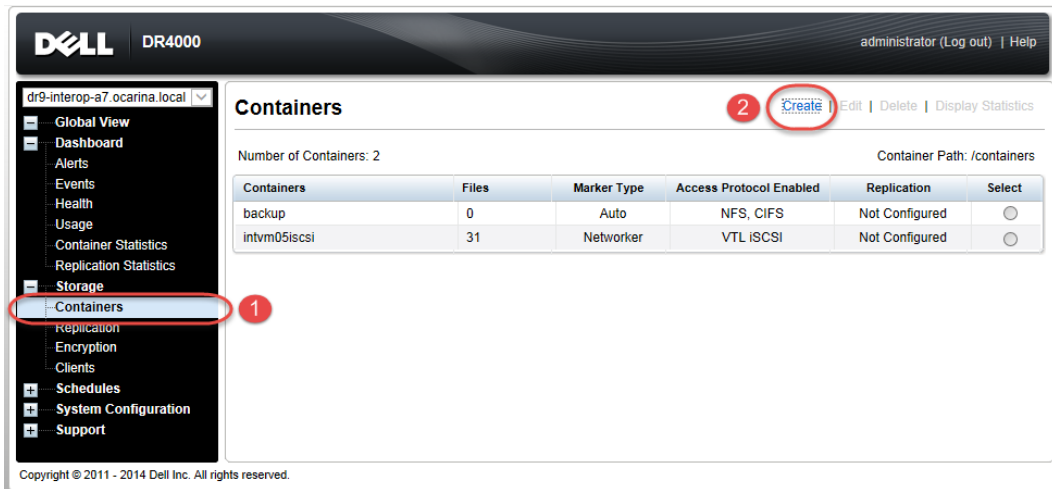
- Label all the media with labels and place them in their respective media pools for use.



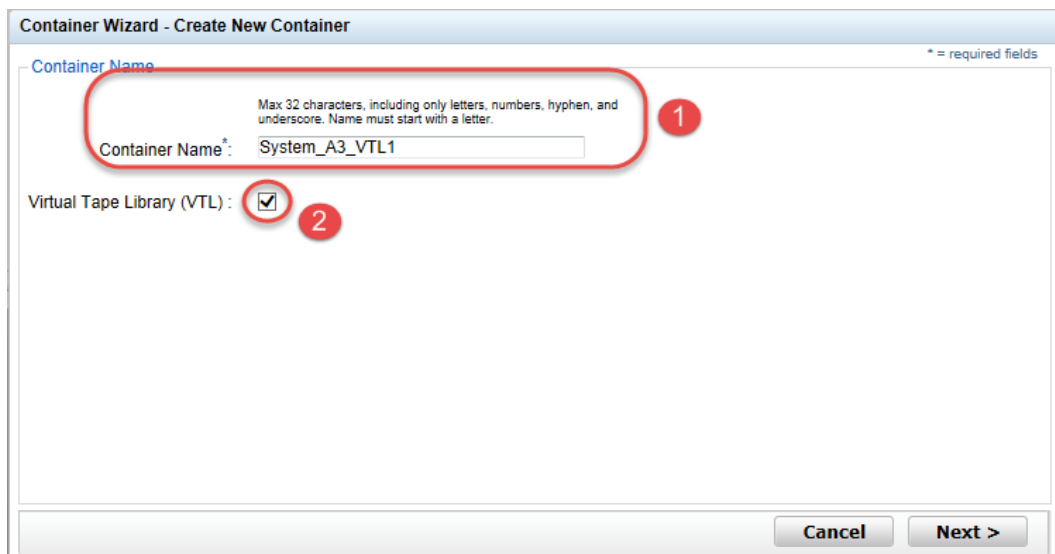
4 Creating and configuring NDMP target container(s) for Networker

4.1 Creating the NDMP VTL container for Networker use

1. Create and export the iSCSI container by selecting **Containers** in the navigation area of the GUI, and then clicking **Create** at the top of the page.



2. In the **Create New Container** wizard, enter the container name, select the **Virtual Tape Library (VTL)** container option, and click **Next**.



3. Select the NDMP **Access Protocol**. Specify the DMA **Access Control** information by providing the storage node or, media node IP Address or FQDN. Select the Marker Type as **Unix Dump** and click **Next**.

Container Wizard - Create New Container

Configure Virtual Tape Library

Is OEM:

Tape Size: 800GB 400GB 200GB
 100GB 50GB 10GB

Access Protocol: NDMP iSCSI No Access

Access Control:

Marker Type: Unix Dump None

Container Name and Type
System_A3_VTL1
VTL

< Back Cancel Next >

4. Finalize the VTL creation request by clicking **Create a New Container**.

Container Wizard - Create New Container

Configuration Summary

Container Name and Type
Container Name: System_A3_VTL1
Connection Type: VTL

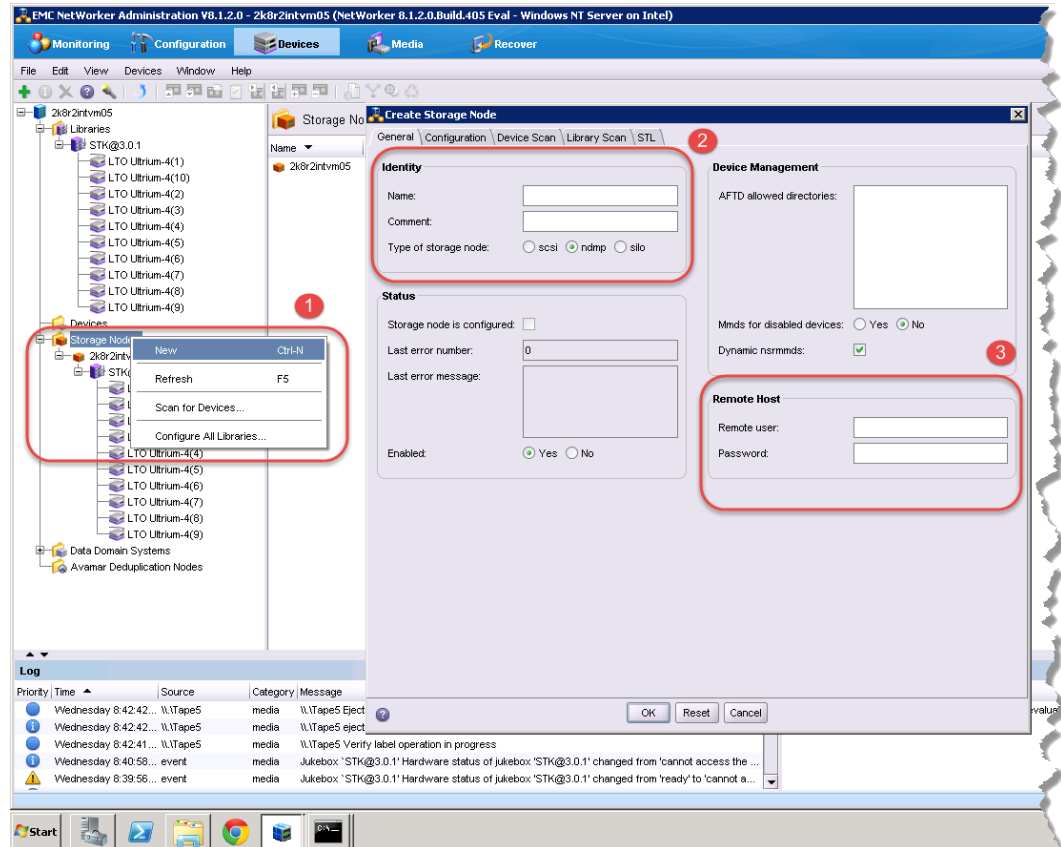
Virtual Tape Library
OEM: no
Tape Size: 10gb
Access Protocol: NDMP
Access Control: iqn.1991-05.com.microsoft.2k8r2intvm05
Marker Type: Networker

< Back Cancel Create a New Container



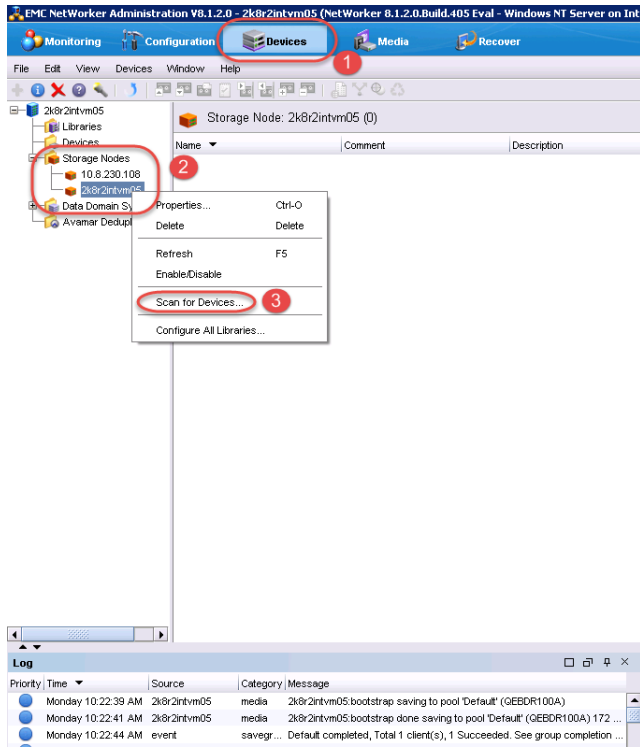
4.2 Configuring Networker to use the newly created NDMP VTL

1. Add the DR Series system as a storage node via NDMP.
 - a. Navigate to the **Devices** menu, select the **Storage Nodes** Sub-Tree object within the EMC Networker navigation pane, and add a new storage node.
 - b. In the **Create Storage Node** window enter the name of the node (this must be resolvable via DNS or host file resolution). Provide the logon credentials for the ndmp user account on the DR Series system.

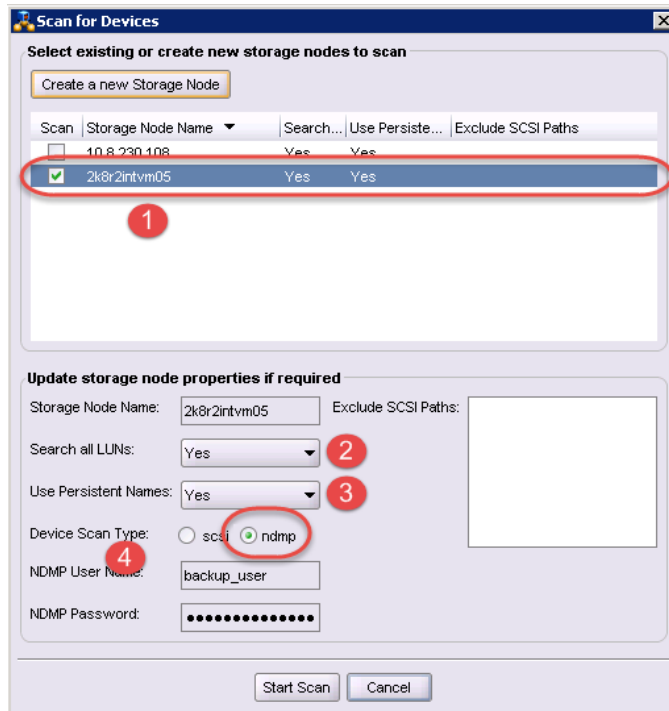


2. Access the **Devices** menu within the Networker Administration interface. Select the Storage Node that has the NDMP VTL configured for access. Select to **Scan for Devices**.

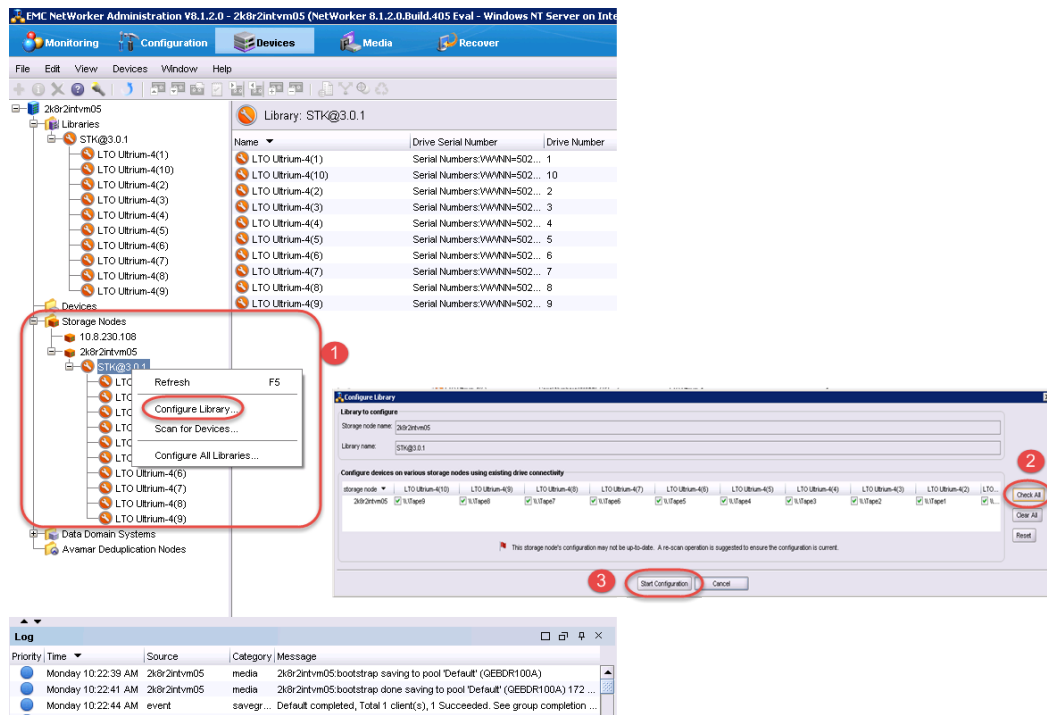




3. In the **Scan for Device** dialog box select the appropriate storage node with the settings to **Search all LUNs**, **Use Persistent Names** and **Device Scan Type** of **ndmp**.

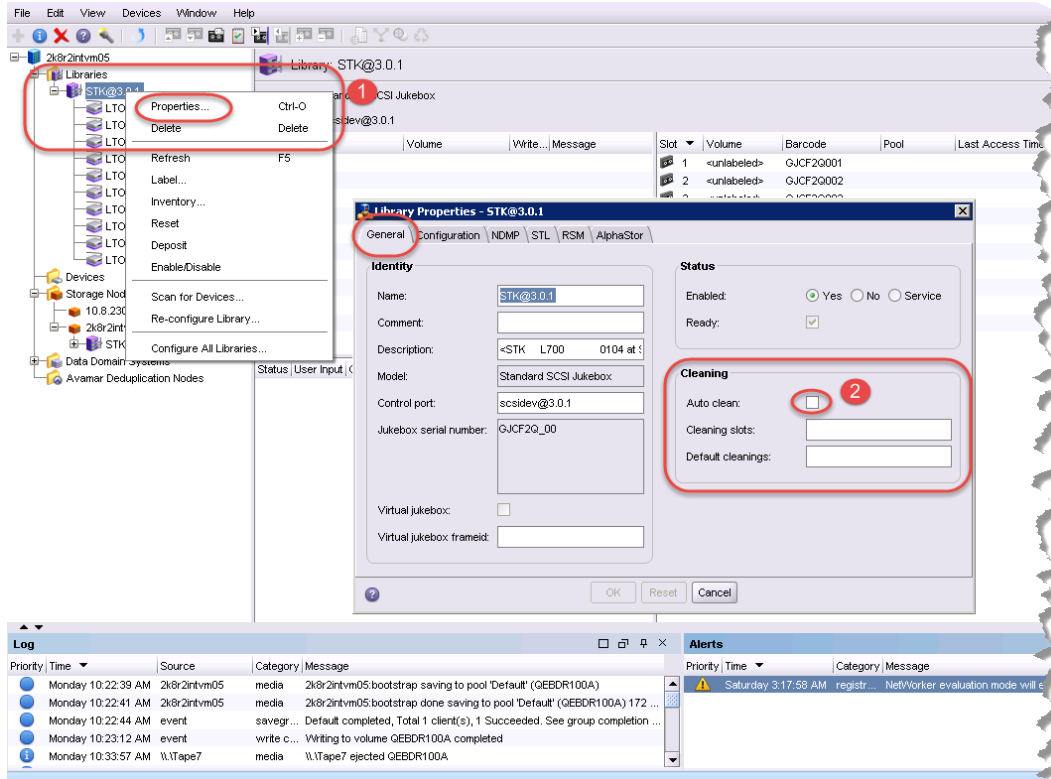


- After the device scan, the NDMP VTL should now appear and can be configured for use. Select the library within the storage nodes navigation tree and proceed with the **Configure Library** option. In the **Configure Library** dialog box, **Check All** drives and click the **Start Configuration** button.

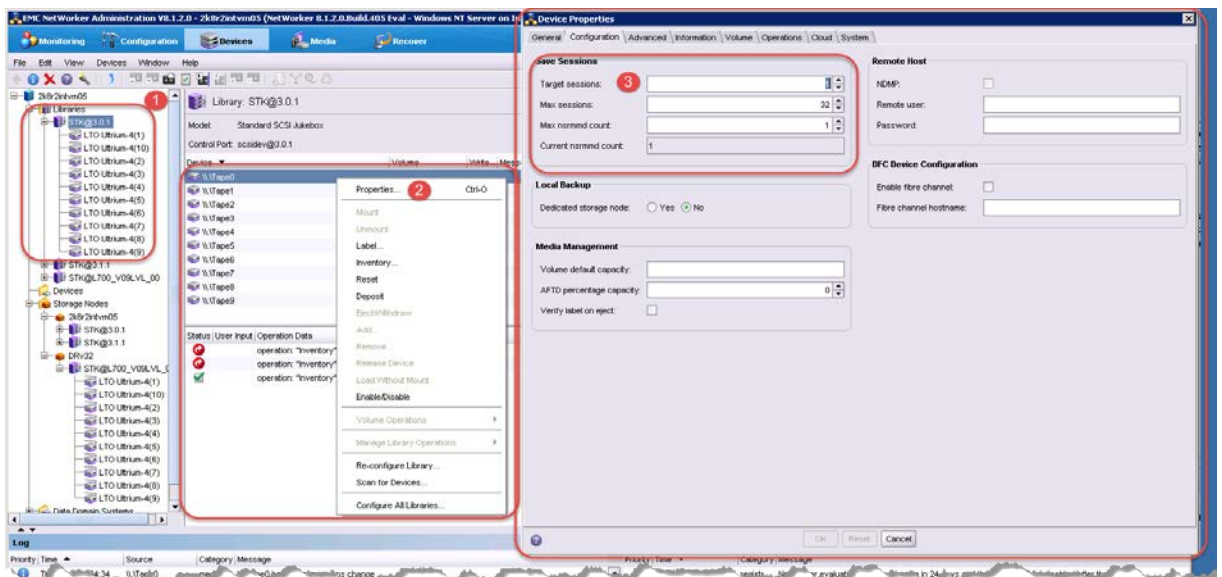


- The VTL should now appear ready for use. By default, the cleaning option is enabled, and it must be disabled. Within the navigation tree, select the Library, and then select the **Properties** option. In the dialog box, disable the **Auto-clean** option and omit the default slot and cleanings settings. Click **OK** to save the changes.

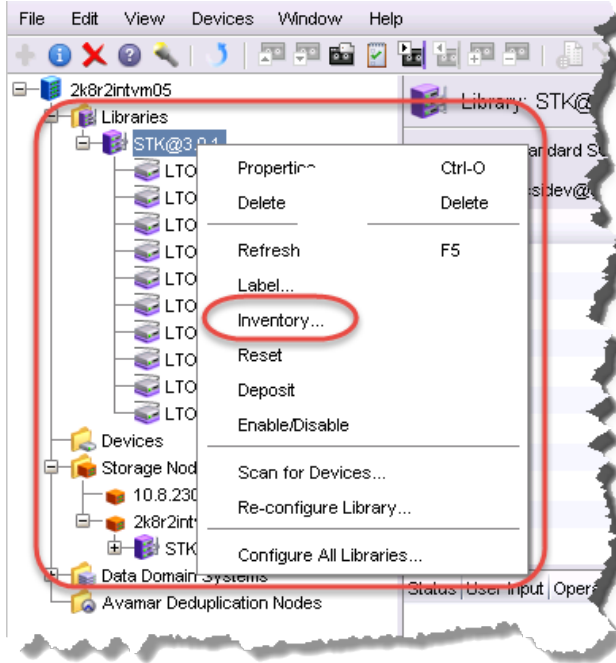




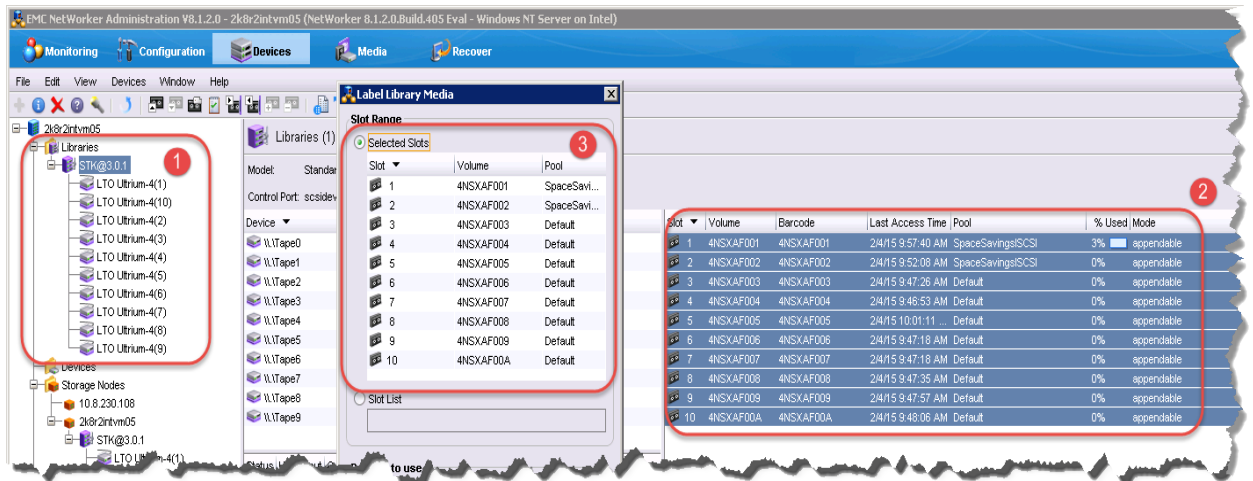
- After the library has been configured, the individual tape drives must be configured so that they service only one target session at any given time. Multiplexing to virtual tape drives has an adverse effect on deduplication and thus requires that each drive only handle a single target session.



- Proceed by conducting a full inventory of the library.



- Label all the media and place them in their respective media pools for use.

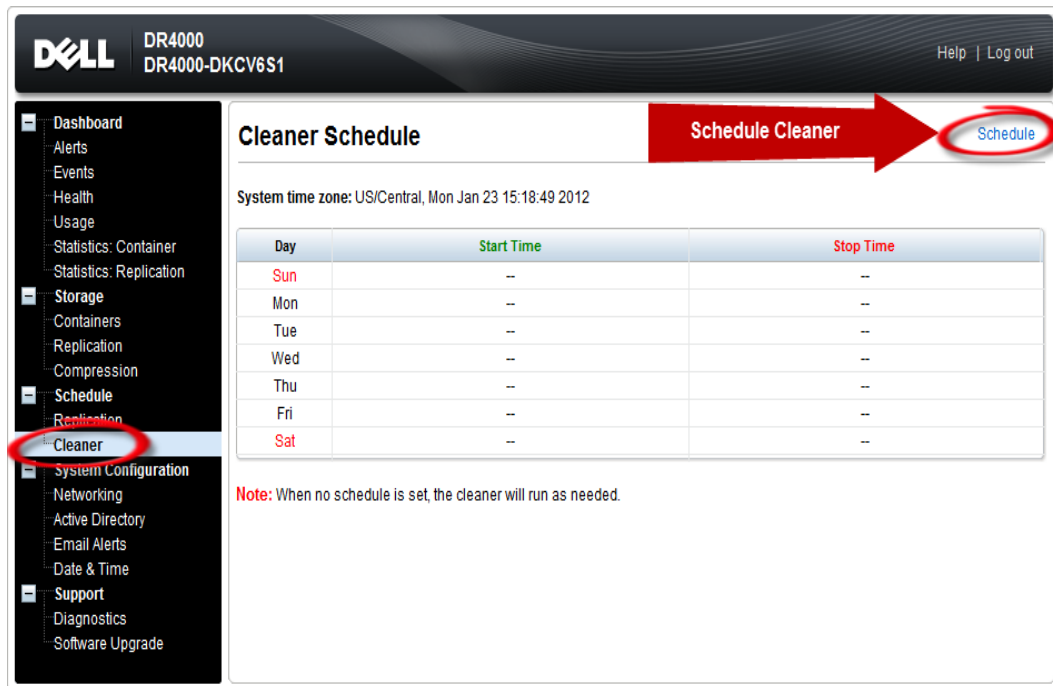


5 Setting up the DR Series system cleaner

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files are 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 the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place, and generally after a backup job has completed.



Dell DR4000 DR4000-DKCV6S1 Help | Log out

Cleaner Schedule **Schedule Cleaner** **Schedule**

System time zone: US/Central, Mon Jan 23 15:18:49 2012

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

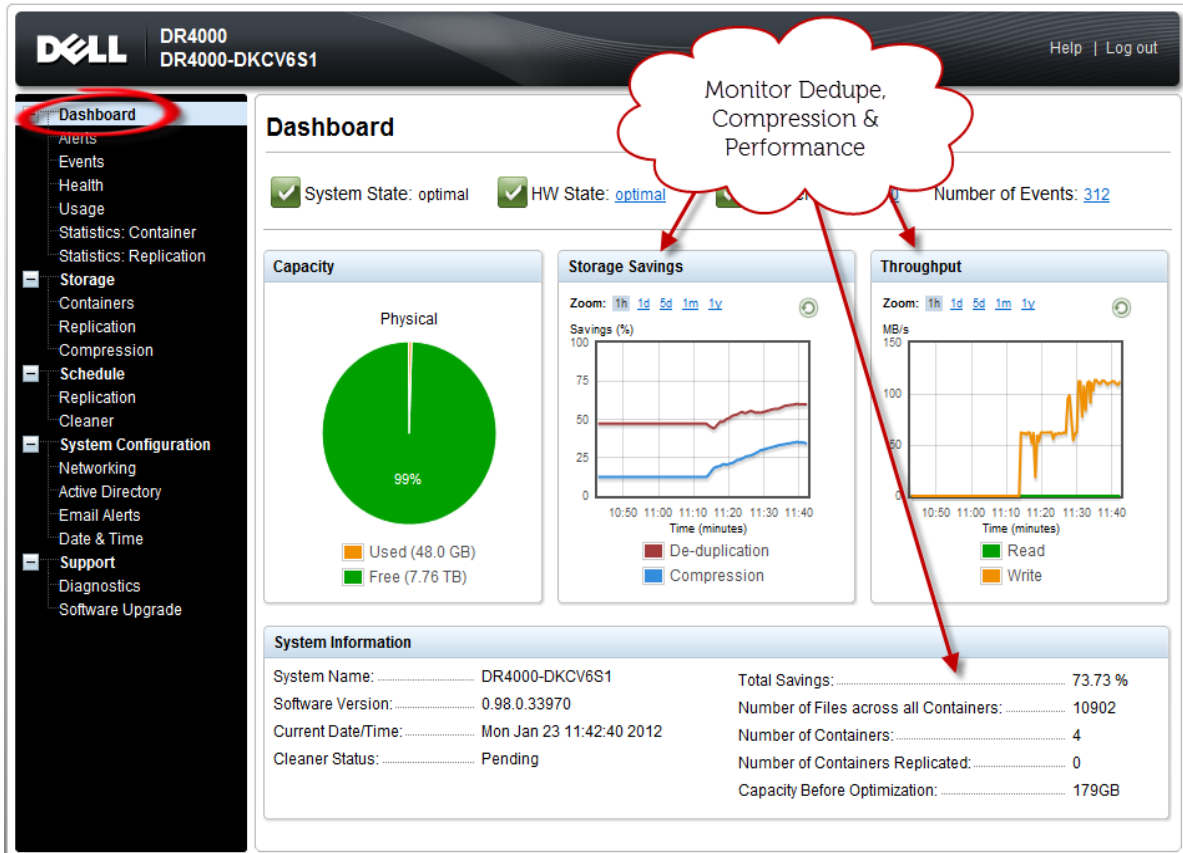
Note: When no schedule is set, the cleaner will run as needed.



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.



A Managing VTL protocol accounts and credentials

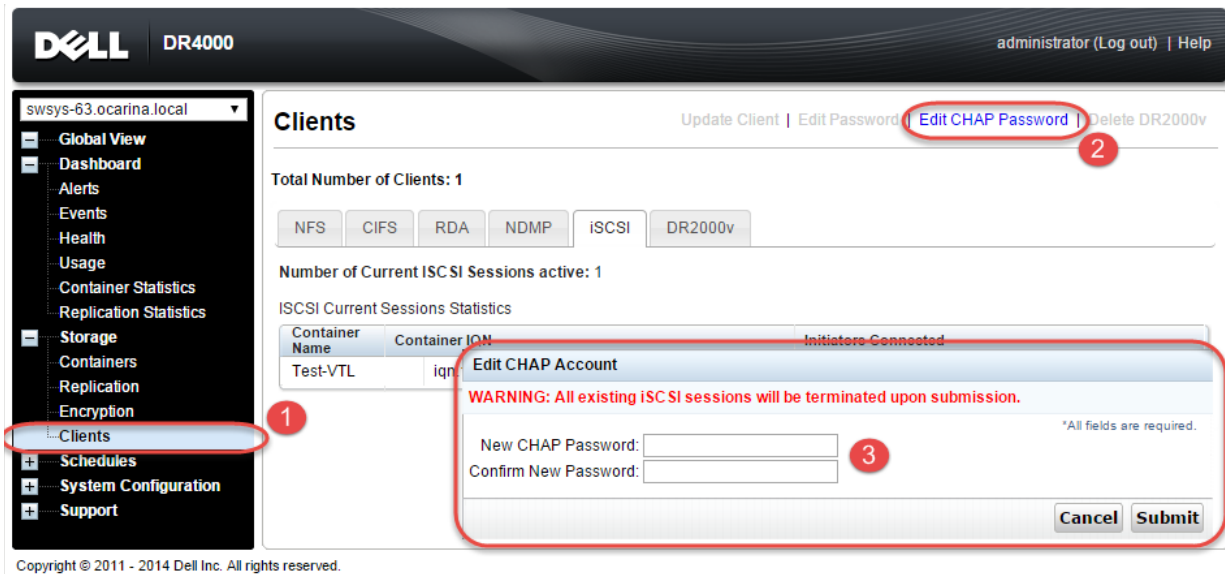
A.1 iSCSI account details and management

By default the iSCSI Username will be the **hostname** of the DR and can be confirmed by reviewing the output of the `iscsi -account --user` command. For example:

```
>iscsi --account --user  
user: dr9-interop-a7
```

The default iSCSI Password is “**St0r@geIscsi**”. This can be modified by navigating to the **Clients** Navigation option and selecting the **iSCSI** tab under the **Clients** menu. Select the **Edit CHAP Password** and fill in the new password as needed.

IMPORTANT NOTE: iSCSI CHAP Passwords must be between 12 and 16 characters long.



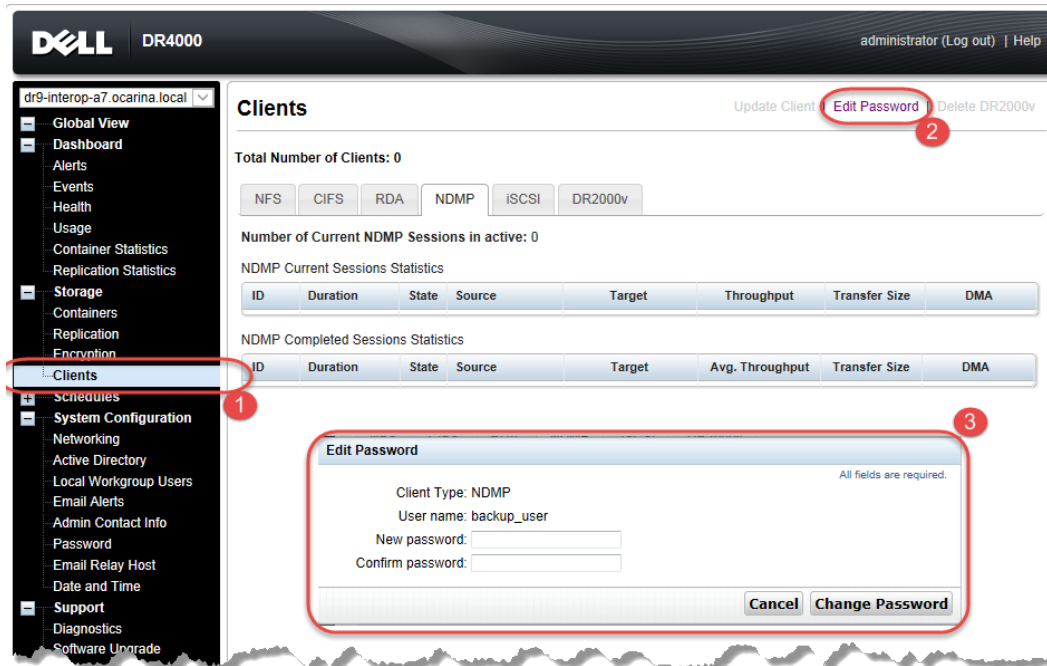
Alternatively, you may also use the “`iscsi -setpassword`” cli tool to change the iSCSI CHAP Password setting as shown in the following example:

```
> iscsi --setpassword  
WARNING: All existing iSCSI sessions will be terminated!  
Do you want to continue? (Yes/no) [n]?  
Enter new CHAP password:#####  
Re-type CHAP password:#####
```



A.2 NDMP account details and management

The default username for the NDMP service is **"backup_user"** and can be confirmed using the web UI interface:



Or, by using the following commands:

ndmp -show command:

```
administrator@dr9-interop-a7 > ndmp --show
```

```
NDMP User:      backup_user
```

```
NDMP Port:     10000
```

The default password is St0r@ge! and can be modified by running the `ndmp -setpassword` command:

```
> ndmp --setpassword
```

```
Enter new NDMP password:#####
```

```
Re-type NDMP password:#####
```

```
NDMP password successfully updated.
```



A.3 VTL default account summary table

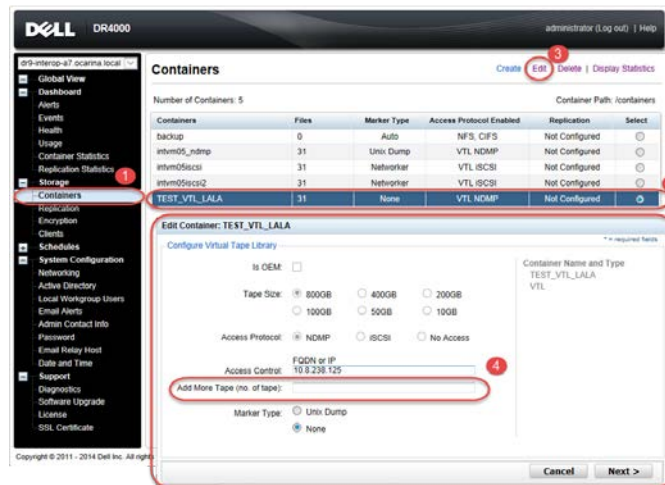
Service	Account	Default Credentials	CLI Modifier
NDMP	backup_user	St0r@ge!	ndmp --setpassword
iSCSI	<Appliance Hostname>	St0r@ge!iscsi	iscsi -setpassword



B Adding VTL media

B.1 Adding the VTL media to the container

To add media to an existing VTL container navigate to the **Containers** menu option. Select and edit the target VTL container. Use the resulting dialog box field **Add More Tape (no of Tape)** field to input the number of tapes to add to the VTL container.



Alternatively you may also use the “vtl --create_carts” cli command for this operation:

```
> vtl --create_carts --name TEST_VTL_LALA --tapes 10  
Created 10 cartridges
```

B.1.1 VTL media count guidelines

Type	Capacity	Max number of Tapes supported
LTO-4	800GiB	2000
LTO-3	400GiB	4000
LTO-2	200GiB	8000
LTO-1	100Gib	10000
LTO-1	50Gib	10000
LTO-1	10GiB	10000



B.2 Updating Networker to identify newly added VTL media

After the VTL media has been added to the target VTL container NetWorker must now be updated to be able to use media. Select the VTL and conduct an inventory update. Input the new range created (e.g. 10 new tapes would result in 20 Slots) and select the option to reinitialize the library.

