Setting Up Replication between Dell™ DR Series Deduplication Appliances with NetVault 9.2 as Backup Software

Dell Engineering
January 2014

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release

Table of contents

Executive summary

This paper provides information about how to set up replication between Dell DR Series Deduplication Appliances for NetVault 9.2 backup. 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/NetVault build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/ NetVault software version used.

1   Prepare each of the DR Series Deduplication Appliances

1. Add NetVault serve machine and DR Series Deduplication Appliance to the same domain (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment)

- DR Series Deduplication Appliance Console: **System Configuration**-> **Active Directory** -> **Join**
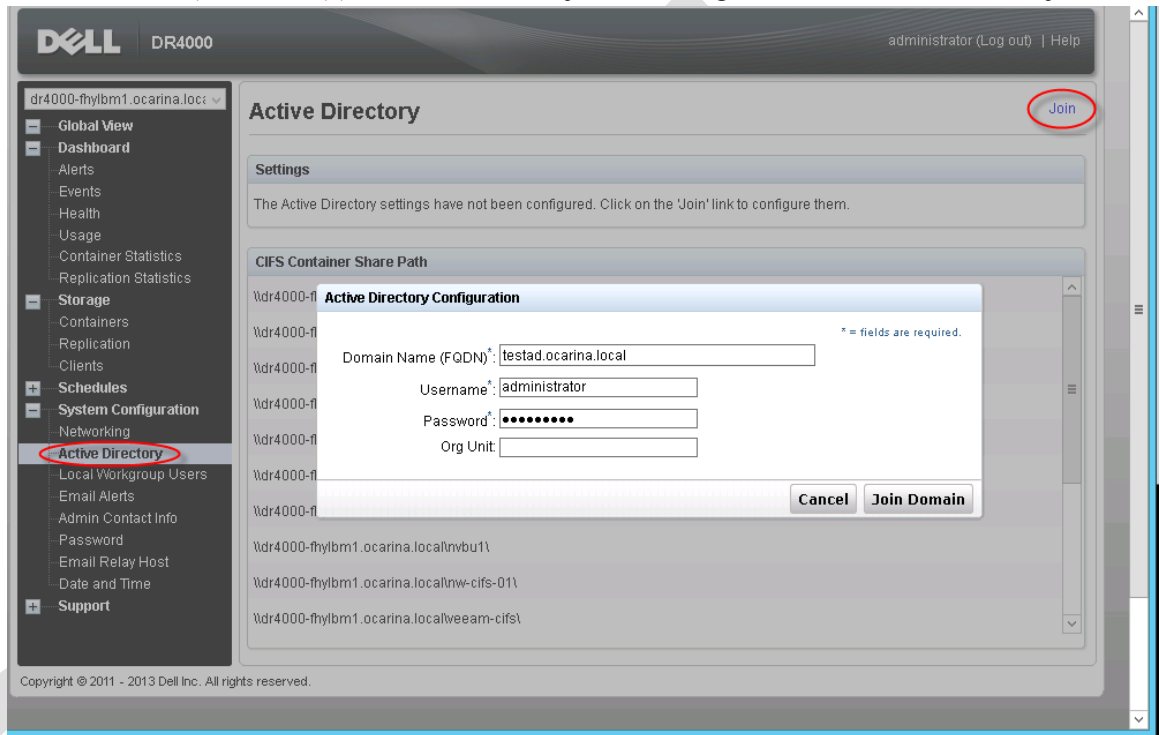
2. Create container in DR Series Deduplication Appliance console. Enter a **Container Name**, select **Enable CIFS** check box. NetVault supports CIFS and NFS protocols.
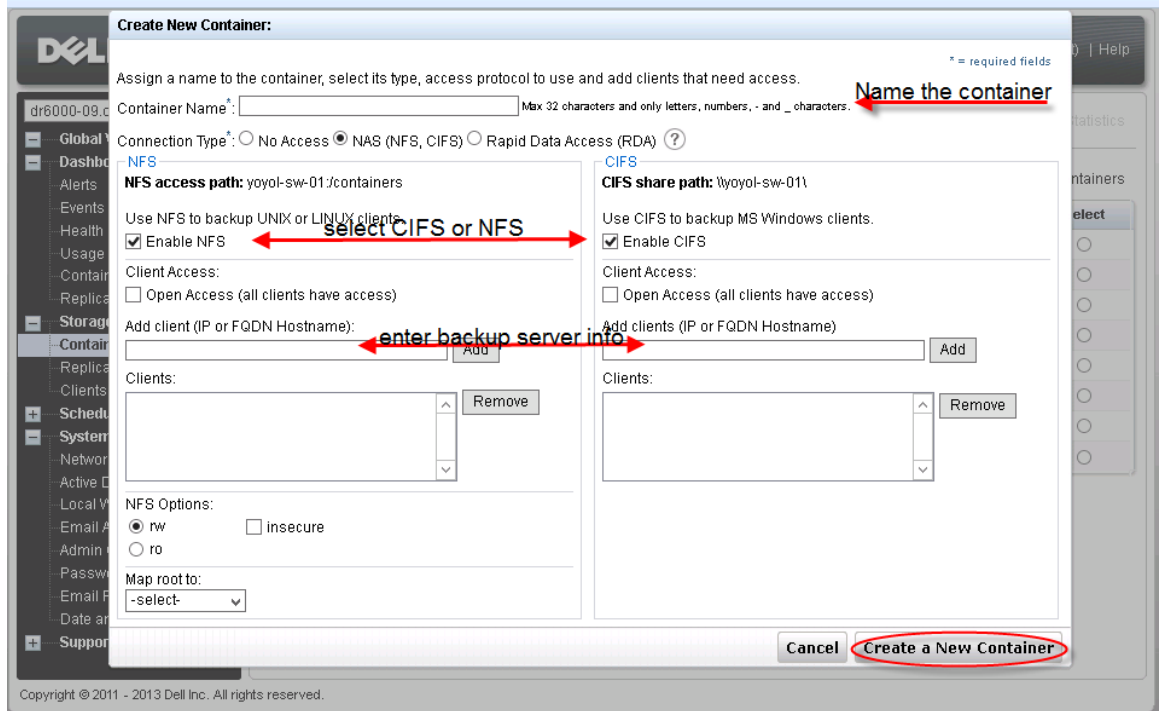
3. Select preferred client access credentials. Click **Create a New Container**.

4. Confirm that the container is added.

5. Click **Edit.** Note down the container share/export path, which you will use later to target the DR container. Click **Cancel** to exit.

2   Set Up NetVault

2.1   Procedure of backup data to source DR

1. Add NetVault serve to the same domain as DR Series Deduplication Appliance (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment).

- NetVault Window 2012 server

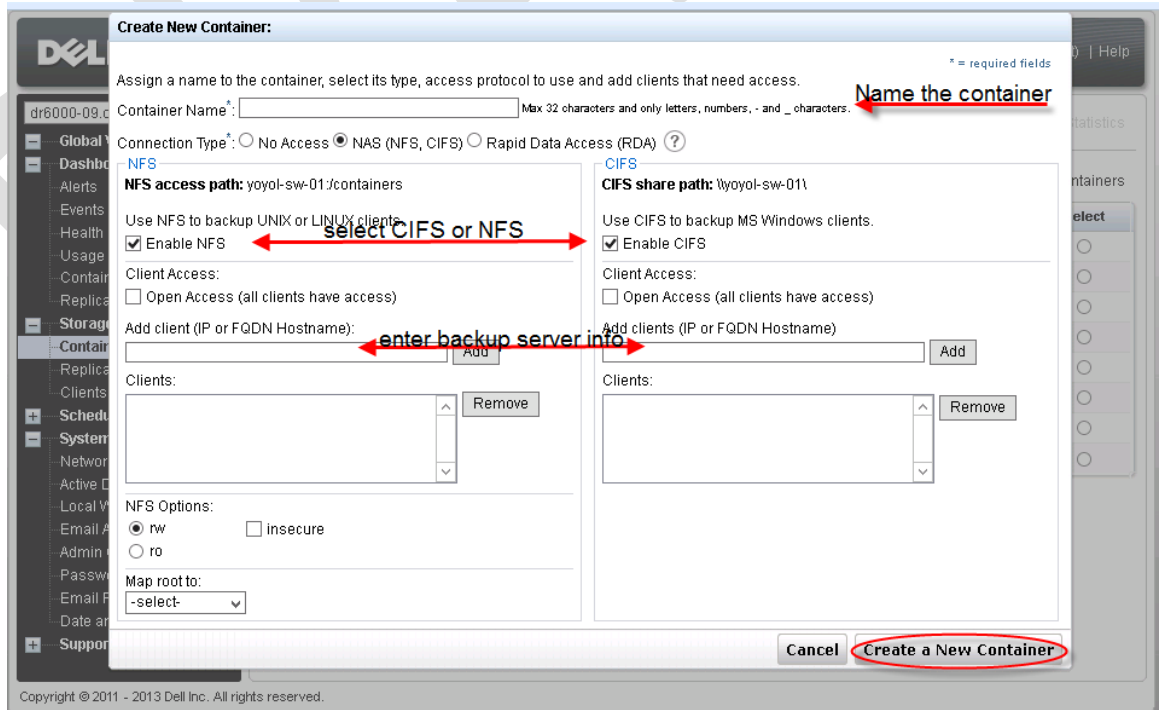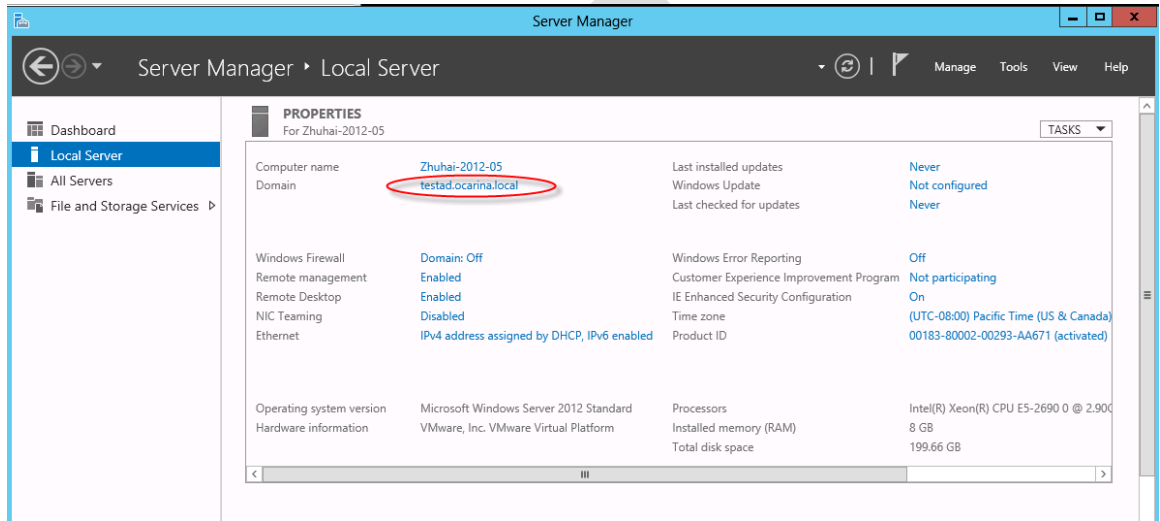2. On NetVault server, launch **Windows Services** console, set the logon information for '**NetVault Process Manager**' service. Enter CIFS credential that has access permission to DR container share(s), and then restart the service.
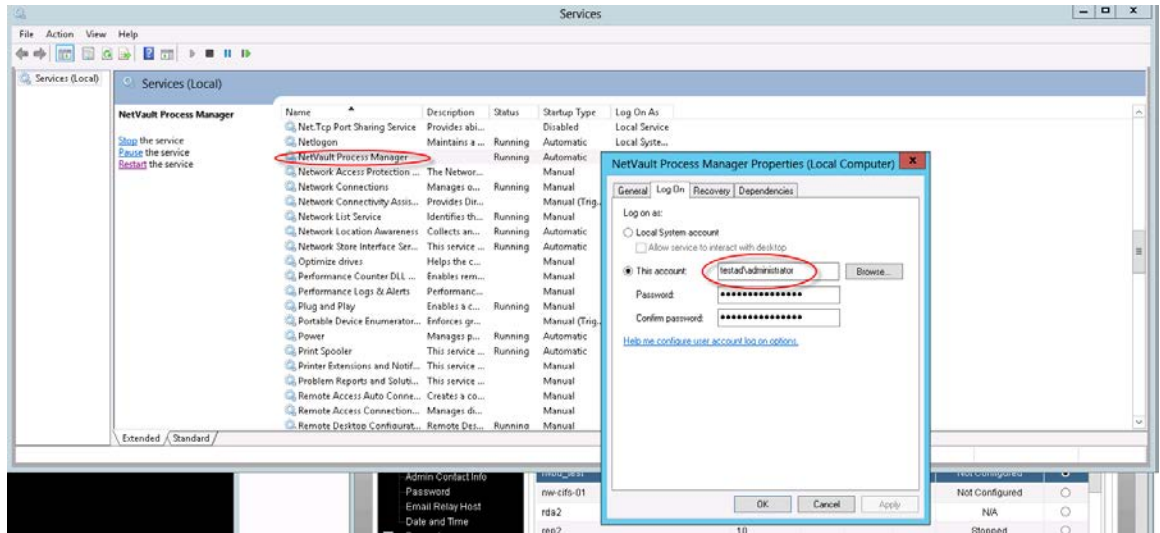
3. Launch **NVBU Console**, click **Device Management**
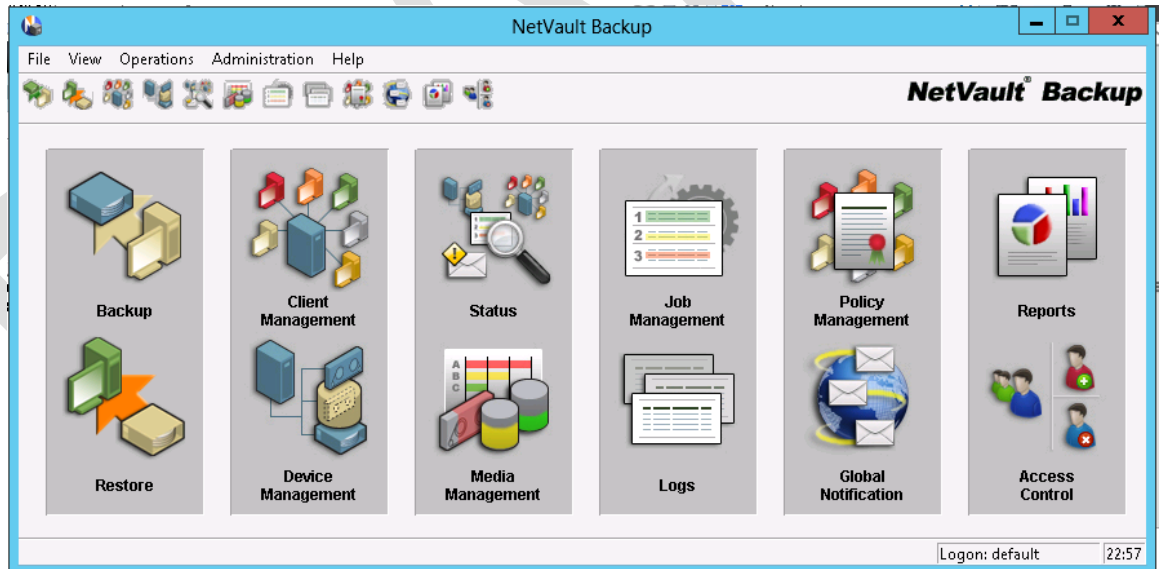
4. Choose **Add** menu, click **Add** -> **Add Library**. In the pop-up **Add Library** window, highlight a client, right click on that machine and choose **Create Virtual Library**
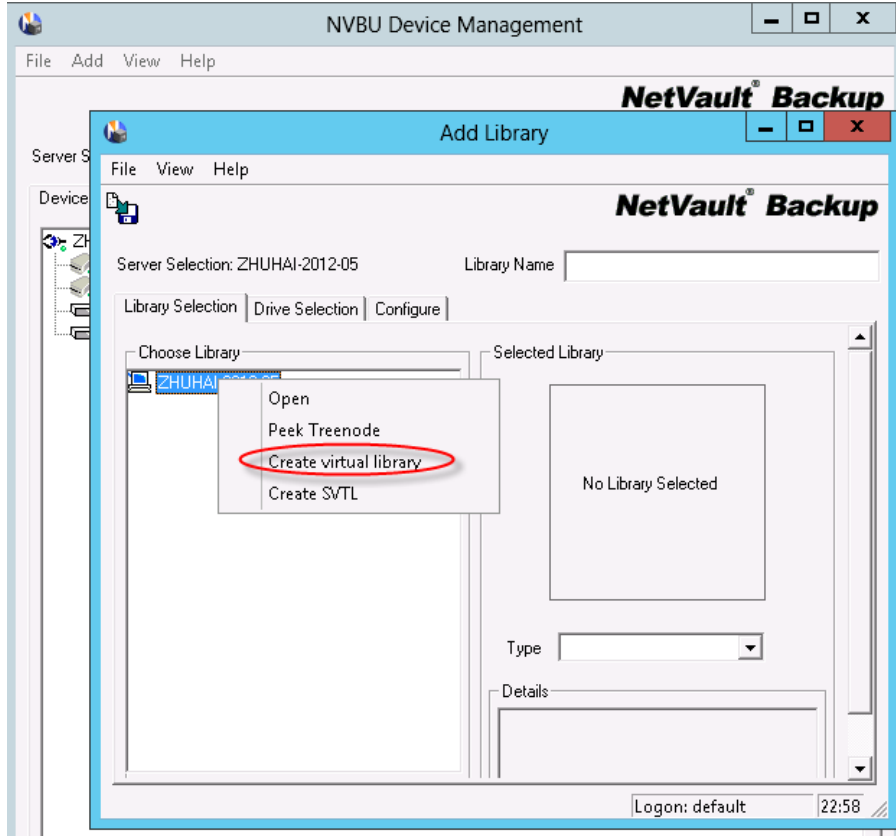
5. Enter source DR container share UNC path, configure other parameters, click **OK**.

Setting Up Replication between Dell™ DR Series Deduplication Appliances with NetVault 9.2 as Backup Software | January 2014
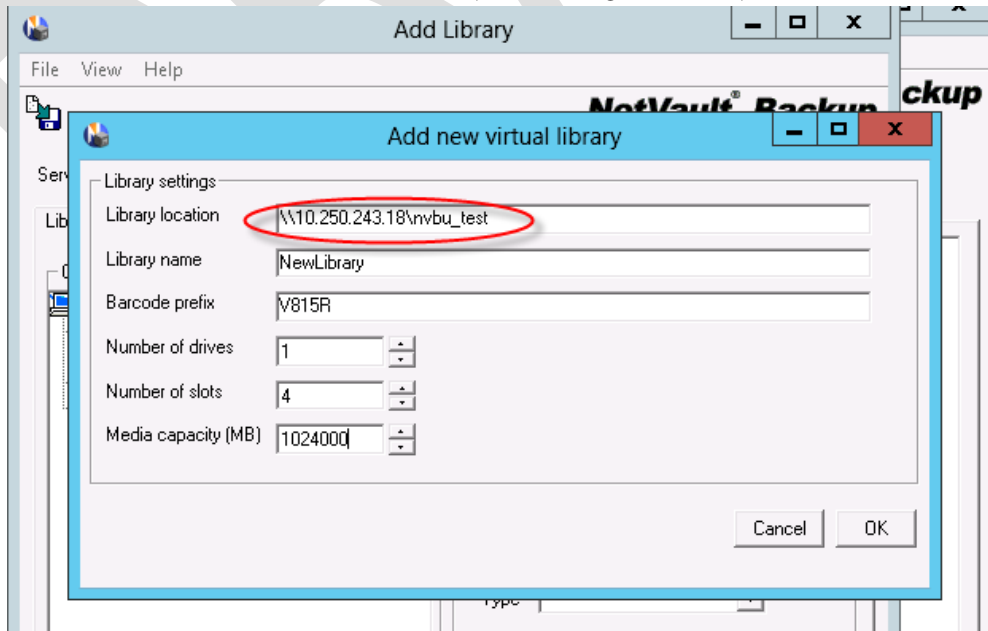
6. On **Library Selection** tab, right click the newly created library, choose **Select**.
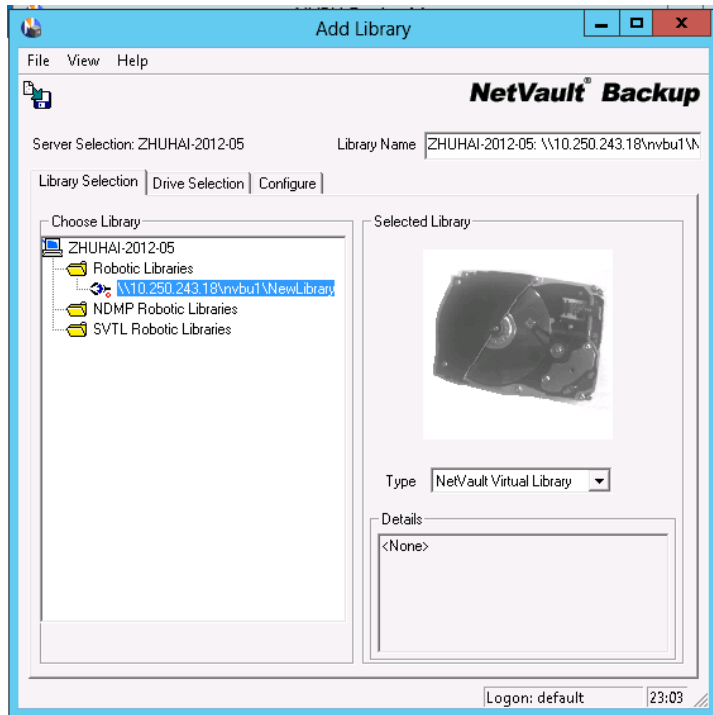
7. On **Drive Selection** tab, pick each of the Drives available for the library, right click on the drive(s), choose **Select.** Make sure all drives are configured in Configure tab, and the library is added successfully. **Save** the library. Verify that the library device is **Online**.
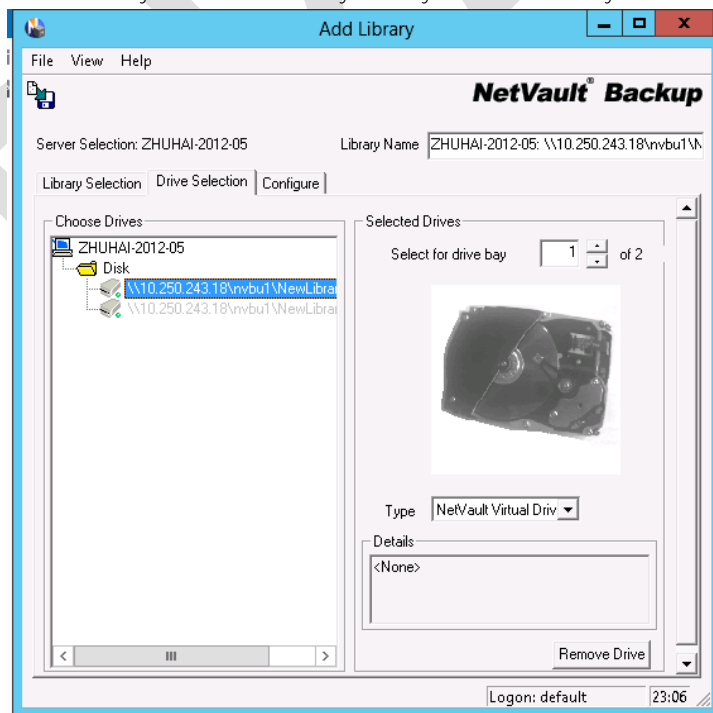
8. Create backup job by clicking **Backup** button on NVBU Console. In Backup job creation window, choose the source DR container library device under **Target** tab.
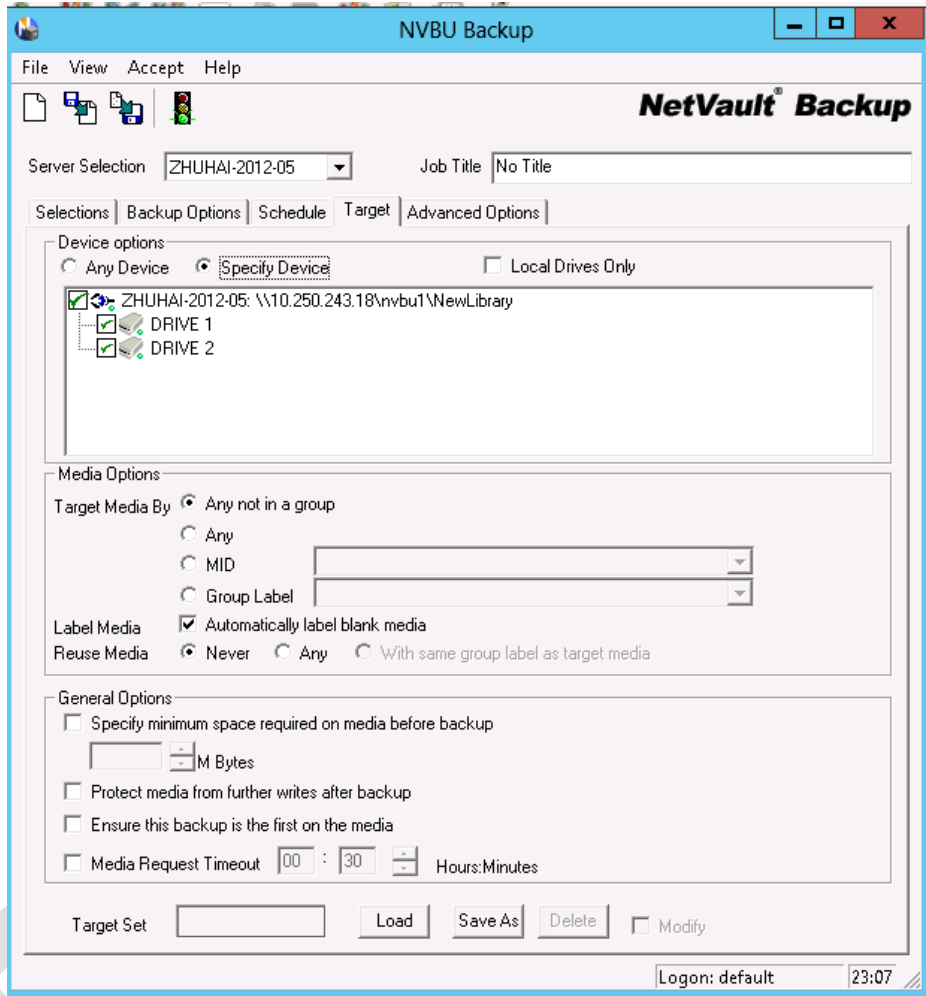
9. On Advanced Options, uncheck **Enable Deduplication.**
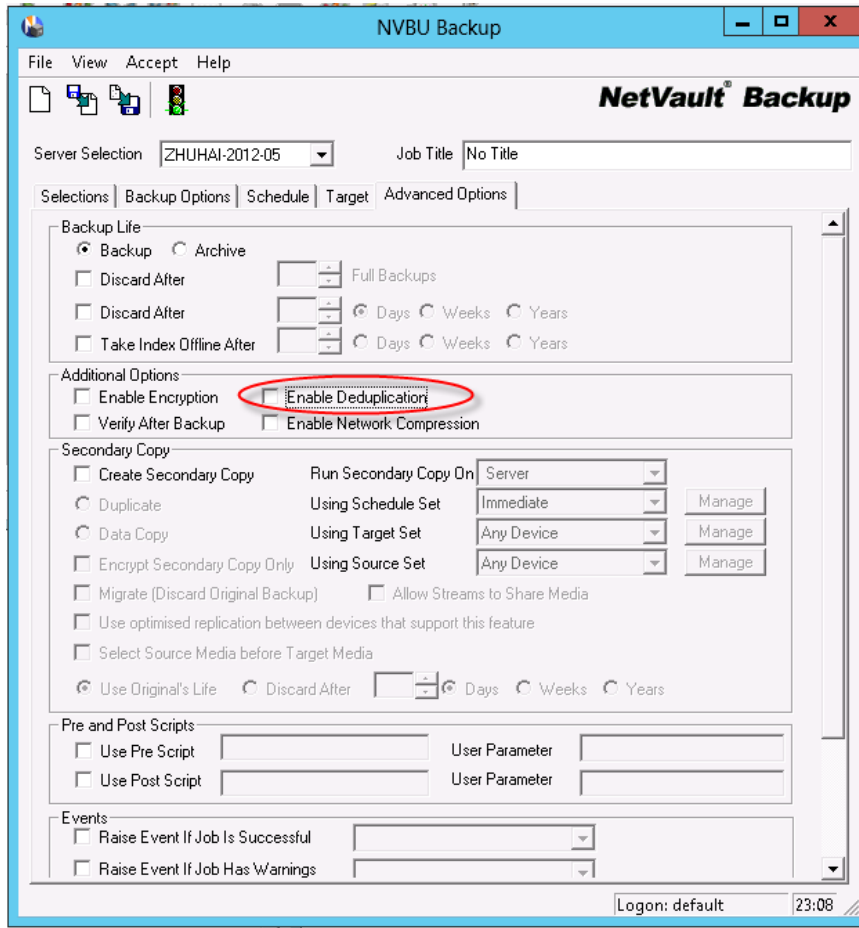
10. After the backup job is completed, a restore point will appear in **NVBU Restore**.

Setting Up Replication between Dell™ DR Series Deduplication Appliances with NetVault 9.2 as Backup Software |
January 2014
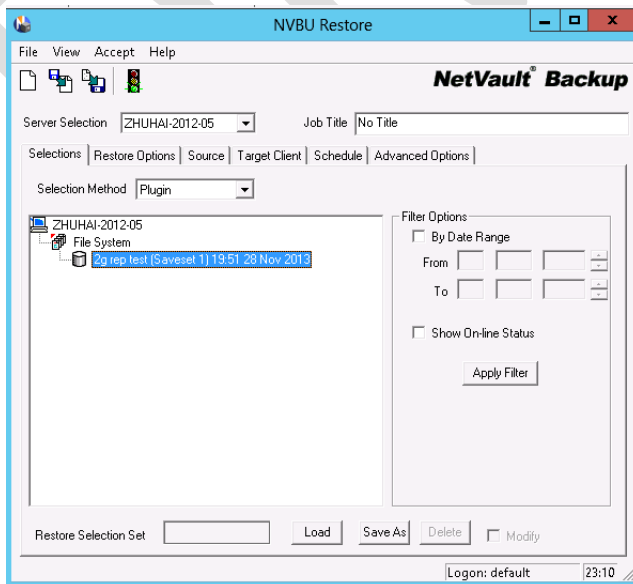
2.2 Set up DR Native Replication from DR Console

1. On source DR console, go to **Replication** -> **Create**
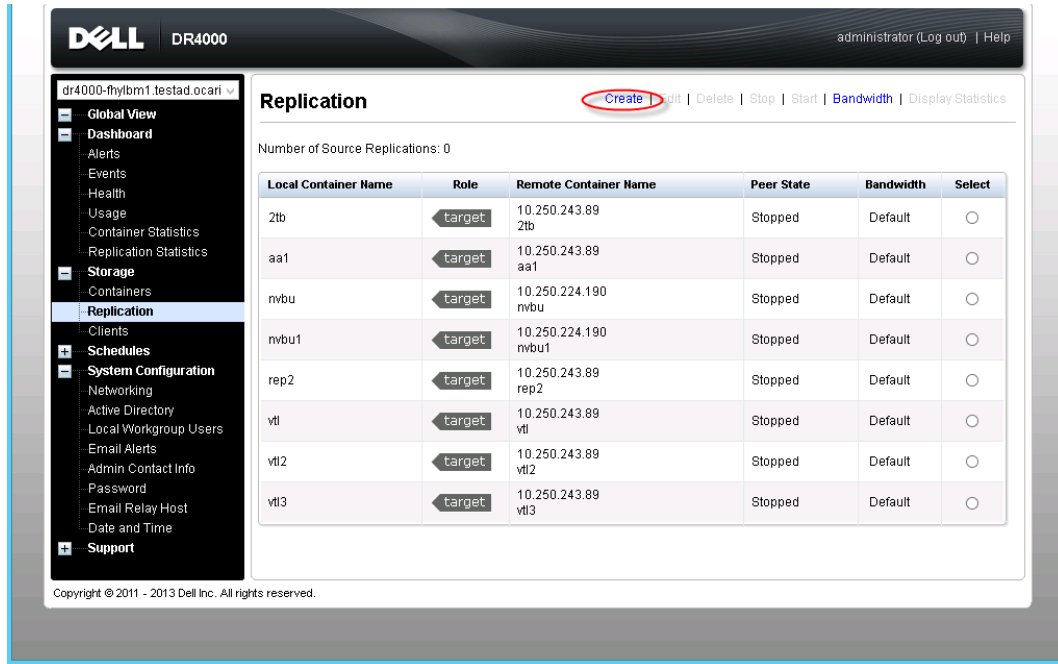
2. Select the source container in step1, choose **Source** in step 3, choose '**Create container on remote system**' in step4. Enter target DR hostname/IP and management credential, click Create Replication.
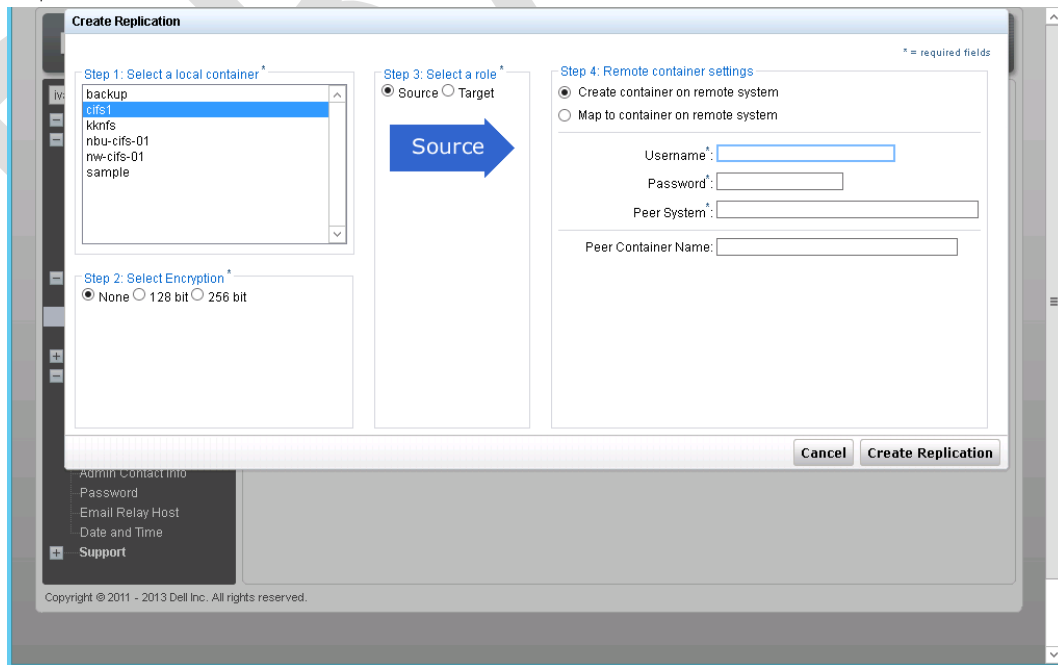
3. Make sure replication session is created successfully, and **Peer Status** is **Online**. Check **Replication Status** from **Replication Statistics** menu.

4. Once **Replication Status** is **INSYNC**, stop the replication.

5. Modify target container on target DR management console and **Enable CIFS** share path
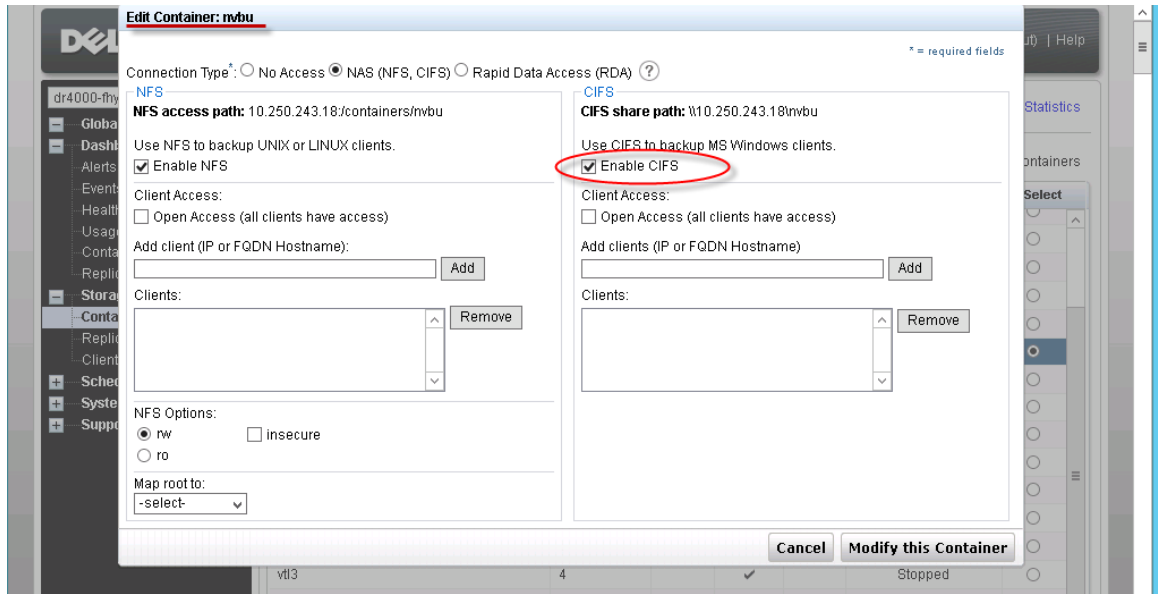
6. Add target DR to the same domain as NetVault Server, add target DR into Active Directory Domain (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment).
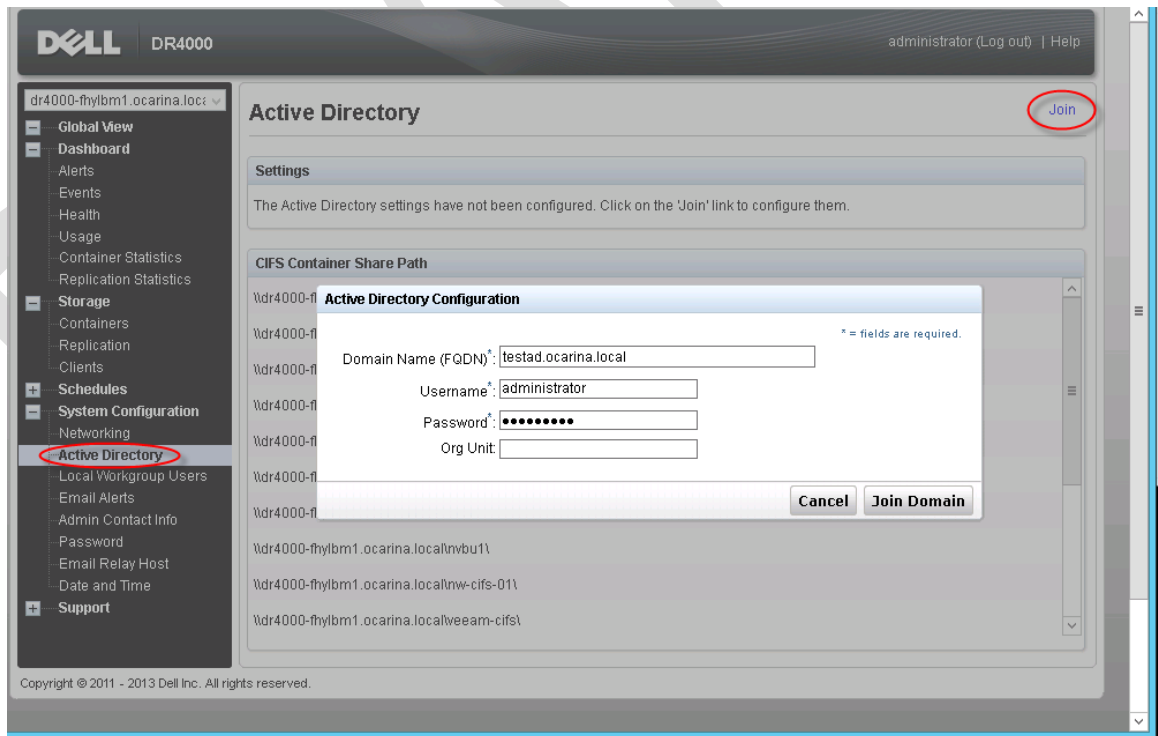
2.3 Restore from Replication Target

1. Launch **NVBU Console**, go to **Device Management**, **Remove** the source VTL.
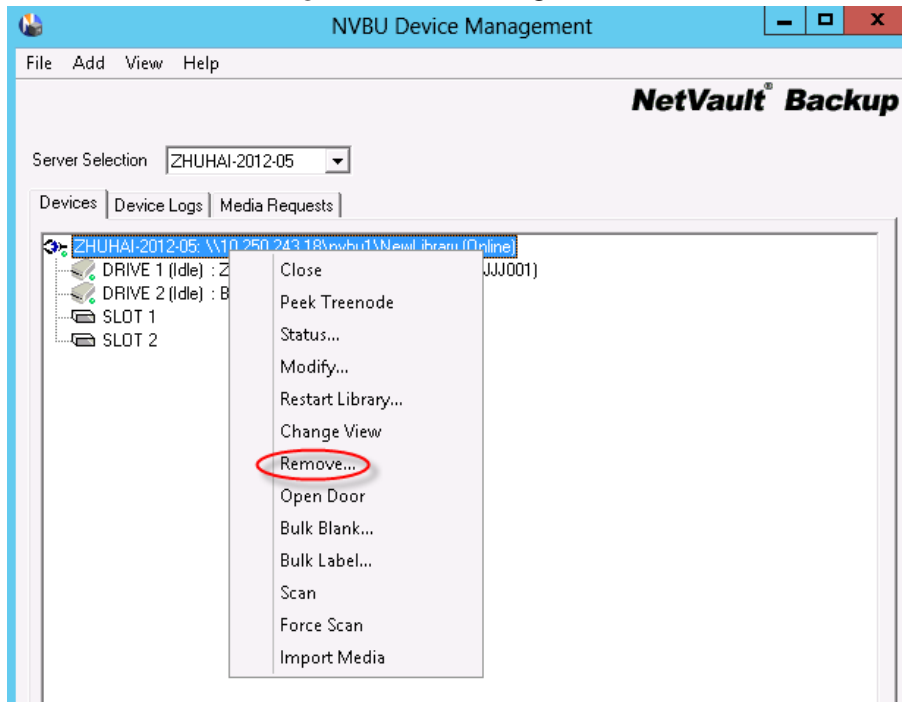
2. Modify C:\Program Files (x86)\Quest Software\NetVault Backup\config\diskdevices.cfg, change the following locations to point to target DR IP or hostname. Save diskdevices.cfg after the modification is completed.

   [libraries]
   location=\\10.250.243.18\nvbu1\NewLibrary

   [drives]
   location=\\10.250.243.18\nvbu1\NewLibrary\drives\1
   location=\\10.250.243.18\nvbu1\NewLibrary\drives\2

3. In NVBU **Device Management** menu, click **Add** - > **Auto-Configure Device**
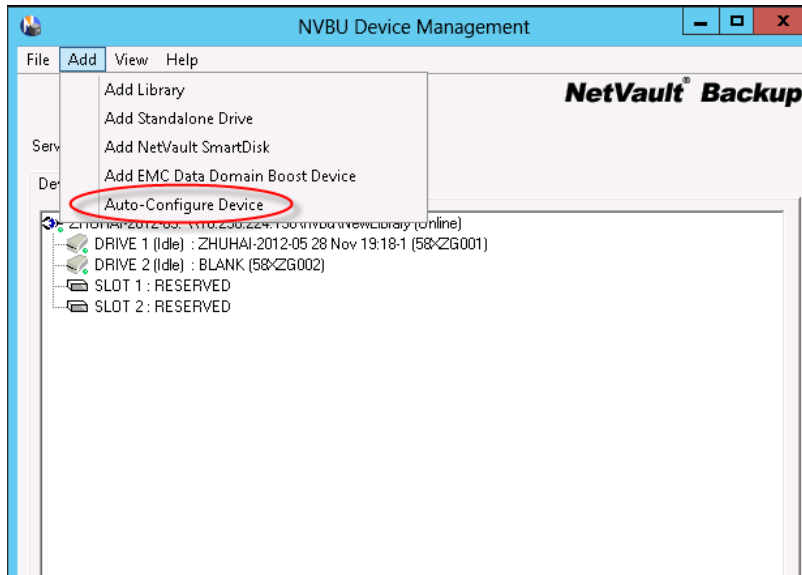
4. NVBU will detect the target library with **Re-scan for devices**

Setting Up Replication between Dell™ DR Series Deduplication Appliances with NetVault 9.2 as Backup Software |
January 2014
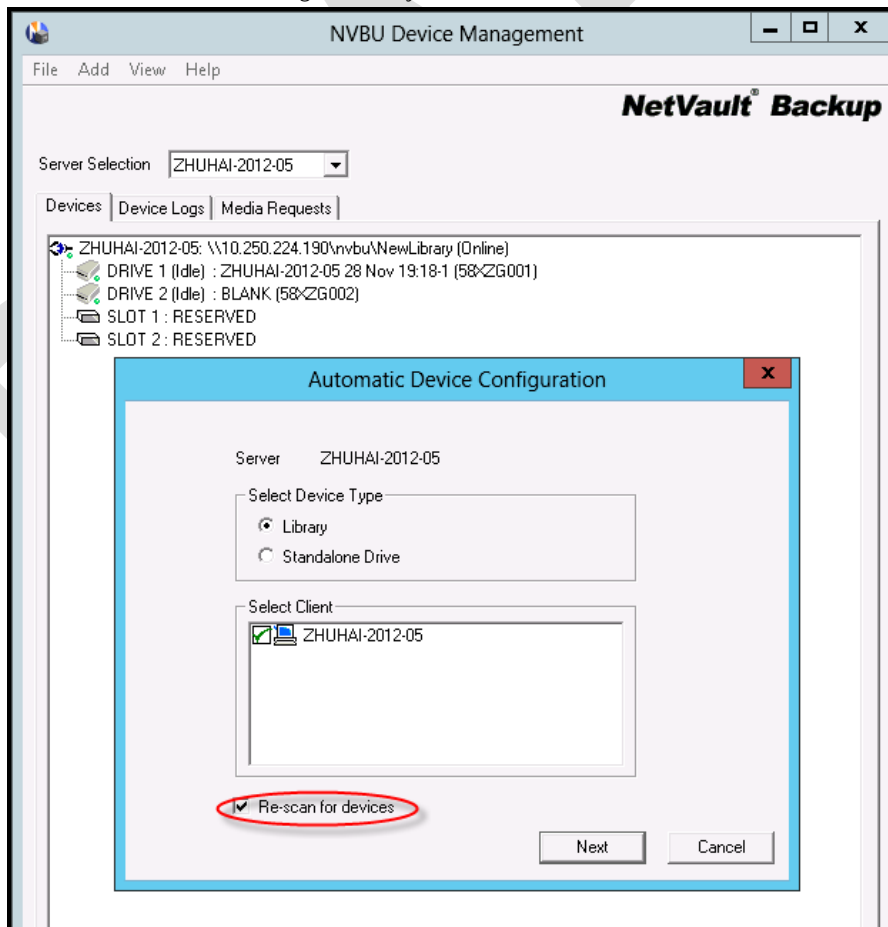
5. The target container device show as **Online** in **Device Management** UI
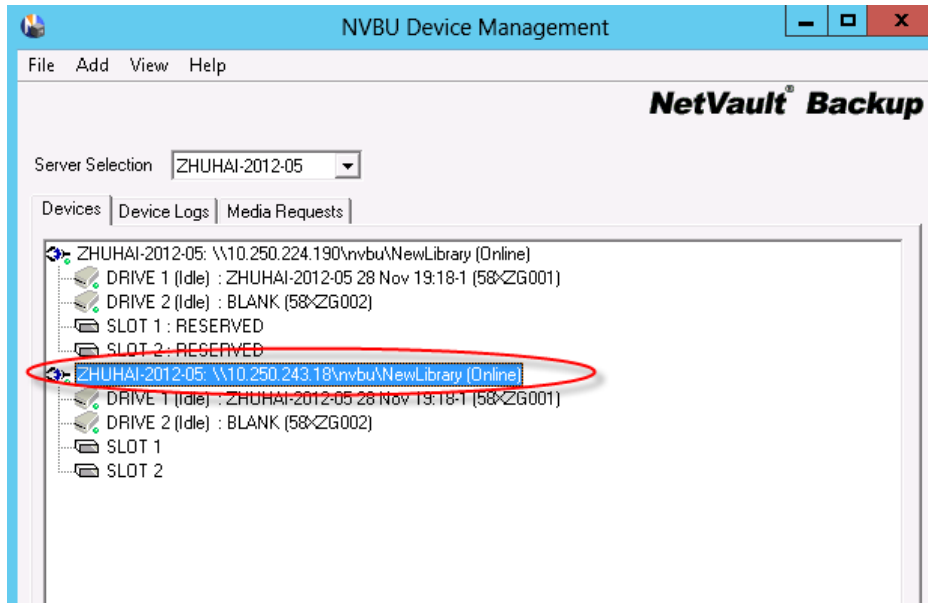
6. From **NVBU Console**, click **Restore**. On **Selections** tab, choose data set that needs to be restored.

Setting Up Replication between Dell™ DR Series Deduplication Appliances with NetVault 9.2 as Backup Software |
January 2014
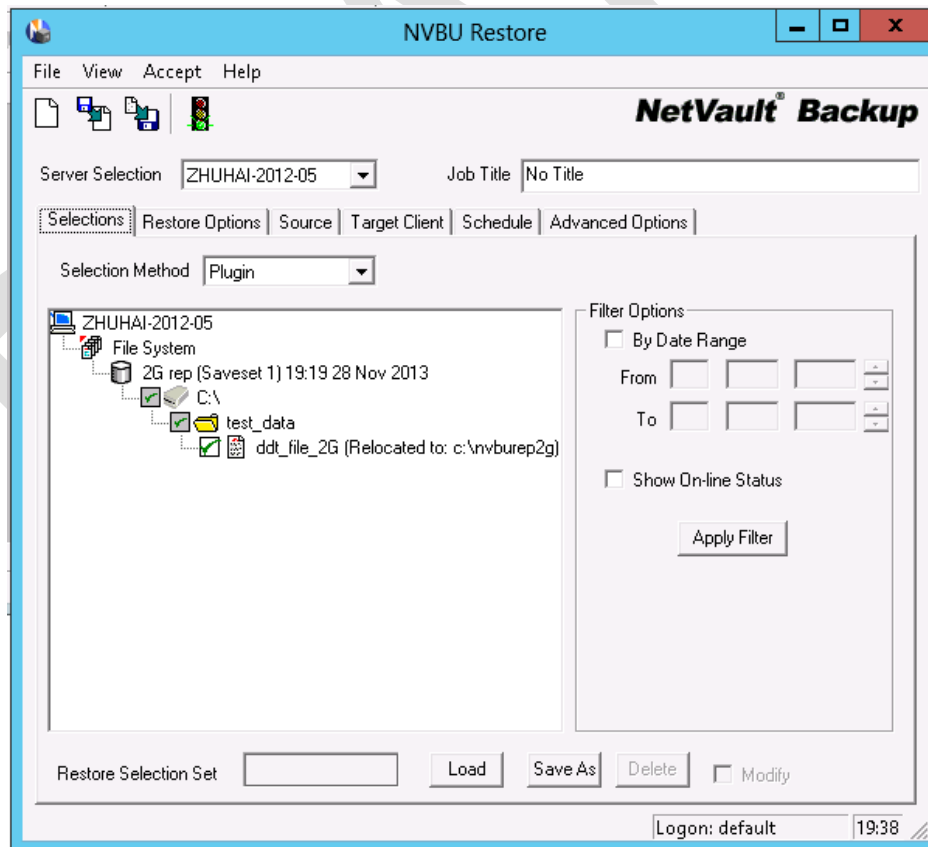
7. On **Source** tab, choose the target library device.
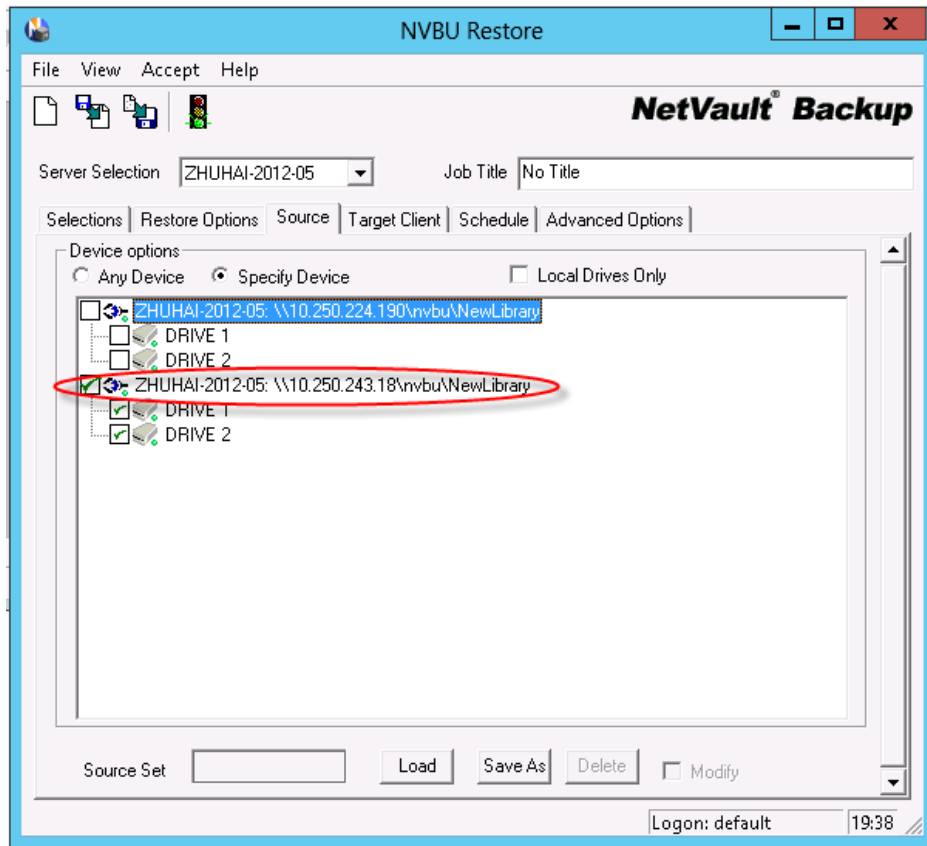
8. Verify from **NVBU Console** -> **Logs** that restore from target container is completed successfully.
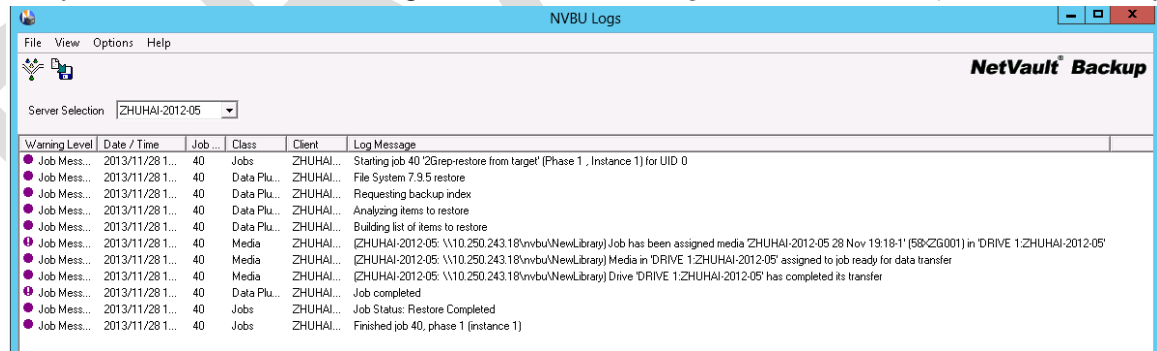
3   Set Up the DR Series Deduplication Appliance Cleaner

The cleaner will run during idle time. If you workflow does not have a sufficient amount of idle time on a daily basis then you should consider scheduling the cleaner which will force it to run during that scheduled time.

If necessary you can do the following procedure as described in the screenshot to force the cleaner to run. Once all the backup jobs are setup the DR Series Deduplication Appliance cleaner can be scheduled. The DR Series Deduplication Appliance cleaner should run at least 6 hours per week when backups are not taking place, generally after a backup job has completed.

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

4 Monitoring Deduplication, Compression and Performance

After backup jobs have completed, the DR Series Deduplication Appliance tracks 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. Backup jobs with a 12-week retention will average a 15x ratio in most cases.
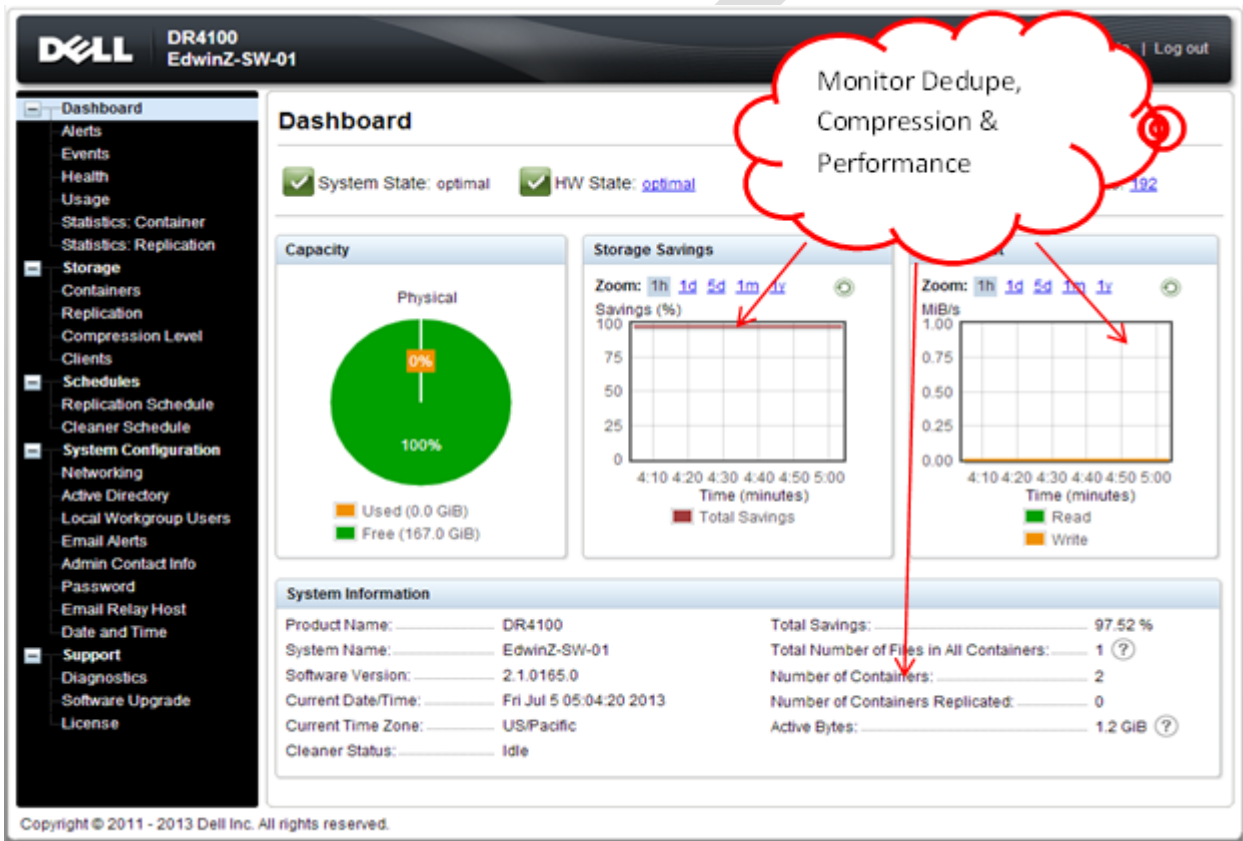
A   Appendix

A.1   Authenticating to DR through CIFS

There are two options for NVBU to authenticate to DR Series Deduplication Appliance through CIFS.

1. **DR joined into domain**: Integrate NVBU Server and DR Series Deduplication Appliance with Active Directory
   a. Ensure the AD user has appropriate ACLs to the DR Series Deduplication Appliance Container share
   b. Set the NVBU service to run with this AD user <Domain\User>

2. **DR is standalone CIFS server**: Make sure Windows NVBU services and DR Series Deduplication Appliance have the same username and password defined in Local Workgroup Users.
   Also make sure this CIFS user has appropriate access permission to the DR Series Deduplication Appliance container share. NVBU services will use this user to authenticate to DR Series Deduplication Appliance share in Workgroup mode.

   a. To set the password for local CIFS administrator on the DR Series Deduplication Appliance, log on to the DR using SSH.
      i. Log on with username Administrator and password St0r@ge!
      ii. Run the following command:
          Authenticate --set --user administrator

```
administrator@EdwinZ-SW-01 > authenticate  --set --user administrator
Enter new password for CIFS user administrator:
Re-enter new password for CIFS user administrator:
Changed administrator's password.
administrator@EdwinZ-SW-01 >
```

NOTE: The CIFS administrator account is a separate account from the administrator account used to administer the appliance. After an authentication method is chosen, set the NVBU service account to use the CIFS administrator account.

   b. Launch Microsoft Services Snap-in by clicking **Start > Run > Services.msc > Enter**.
   c. Locate the NVBU Services. Right-click **Properties** and click the Log On tab.
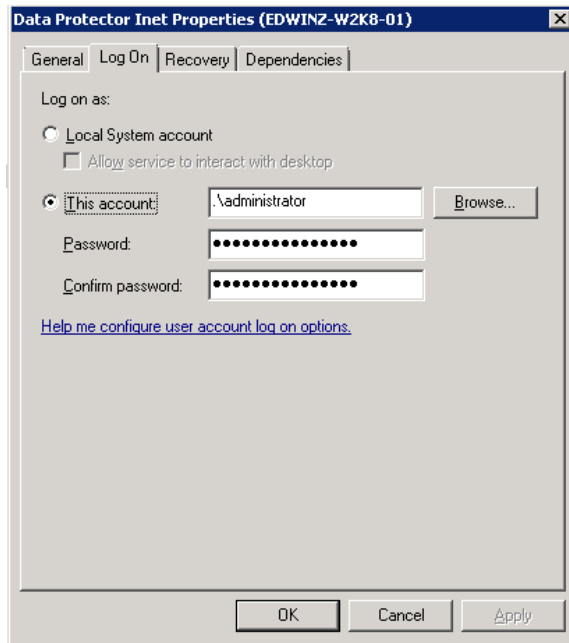
> **NOTE**: Do this step only when no backups are currently running, as restarting the services causes backup jobs to fail. Double-click on the services one at a time.
>
> If you are using local workgroup account rather than the AD account, make sure that there is a ".\"in front of the user name.

    d.   Click **OK**.

    e.   After changes, choose **Stop/Start** to restart the services.