



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

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 Prepare each of the DR Series Deduplication Appliances.....	5
2 Set Up NetVault.....	8
2.1 Procedure of backup data to source DR	8
2.2 Set up DR Native Replication from DR Console.....	14
2.3 Restore from Replication Target	17
3 Set Up the DR Series Deduplication Appliance Cleaner	21
4 Monitoring Deduplication, Compression and Performance	22
A Appendix.....	23
A.1 Authenticating to DR through CIFS	23

DRAFT



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".

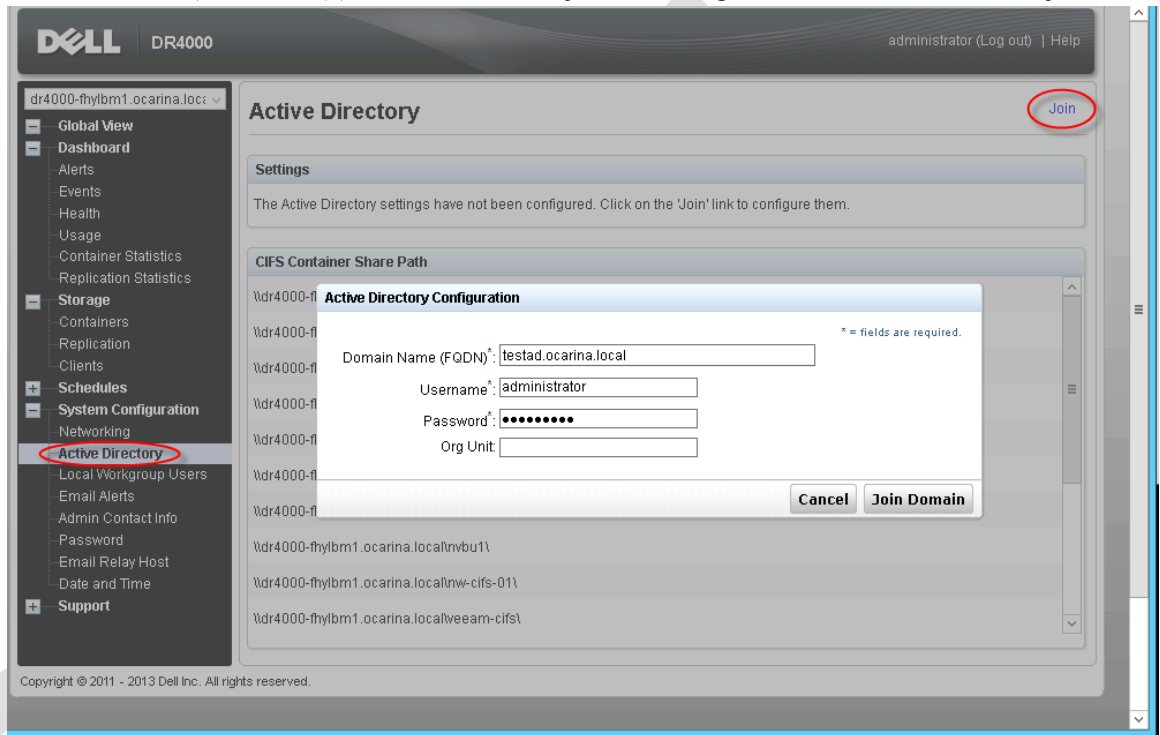
Note: The DR Series Deduplication Appliance/NetVault build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/ NetVault software version used.

DRAFT

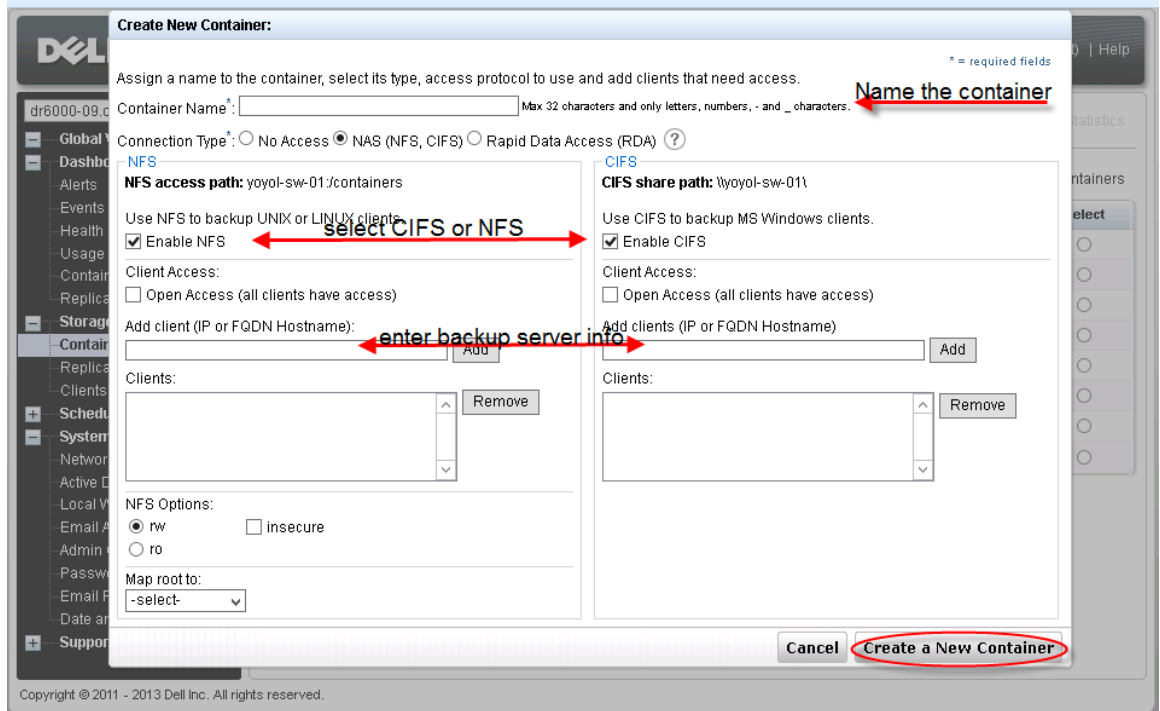


1 Prepare each of the DR Series Deduplication Appliances

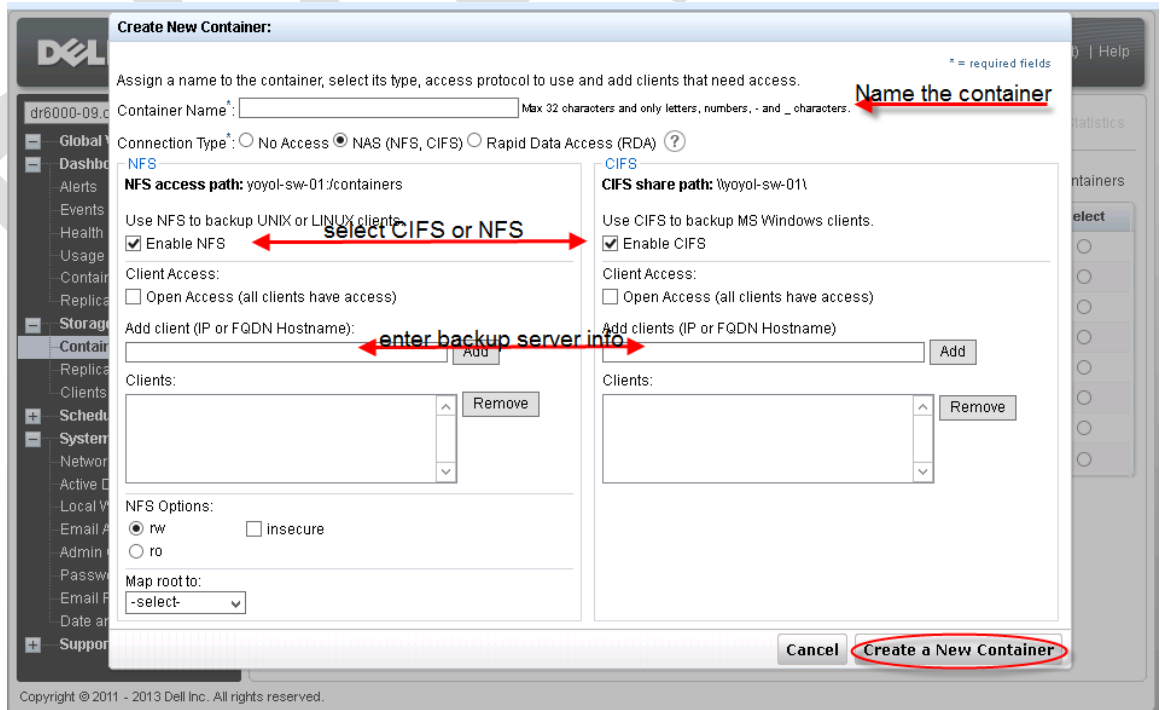
1. Add NetVault serve machine and DR Series Deduplication Appliance to the same domain (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment)
- DR Series Deduplication Appliance Console: **System Configuration -> Active Directory -> Join**



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**.



- Confirm that the container is added.

Containers Create | Edit | Delete | Display Statistics

Message

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

Number of Containers: 22 Container Path: /containers

Containers	Files	NFS	CIFS	RDA	Replication	Select
2t	6				Not Configured	<input type="radio"/>
2tb	6				Stopped	<input type="radio"/>
aa1	15		✓		Stopped	<input type="radio"/>
aa2	0		✓		Not Configured	<input type="radio"/>
acronis-cifs	0		✓		Not Configured	<input type="radio"/>
backup	3	✓	✓		Not Configured	<input type="radio"/>
backup01	14		✓		Not Configured	<input type="radio"/>
nvbu-cifs-02	44		✓		Not Configured	<input type="radio"/>
nvbu	7	✓	✓		Stopped	<input type="radio"/>
nvbu1	7		✓		Stopped	<input type="radio"/>
nvbu_test	0	✓	✓		Not Configured	<input type="radio"/>
nw-cifs-01	37		✓		Not Configured	<input type="radio"/>
rda2	5			RDS	N/A	<input type="radio"/>
rep2	10				Stopped	<input type="radio"/>

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

Edit Container: nvbu_test * = required fields

Connection Type: No Access NAS (NFS, CIFS) Rapid Data Access (RDA) ?

NFS

NFS access path: 10.250.243.18:/containers/nvbu_test

Use NFS to backup UNIX or LINUX clients.

Enable NFS

Client Access:

Open Access (all clients have access)

NFS Options:

rw insecure

ro

Map root to:

root

CIFS

CIFS share path: \\10.250.243.18\nvbu_test

Use CIFS to backup MS Windows clients.

Enable CIFS

Client Access:

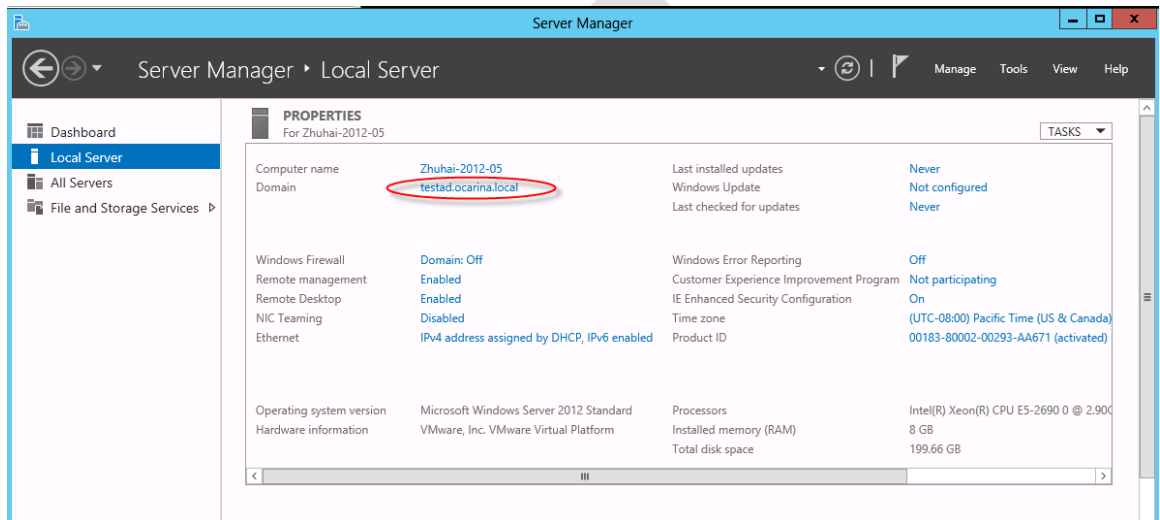
Open Access (all clients have access)



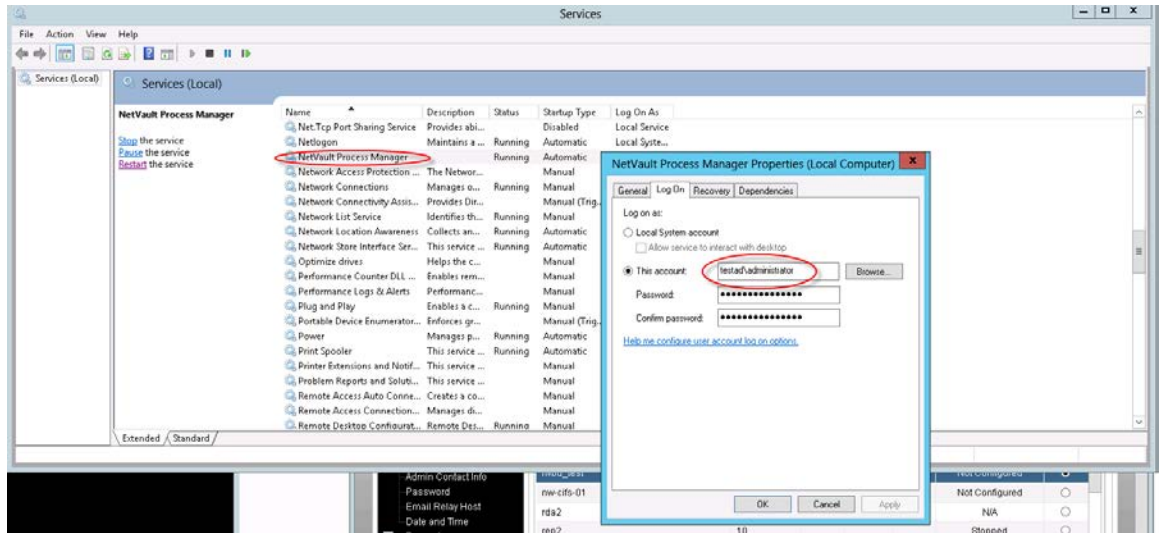
2 Set Up NetVault

2.1 Procedure of backup data to source DR

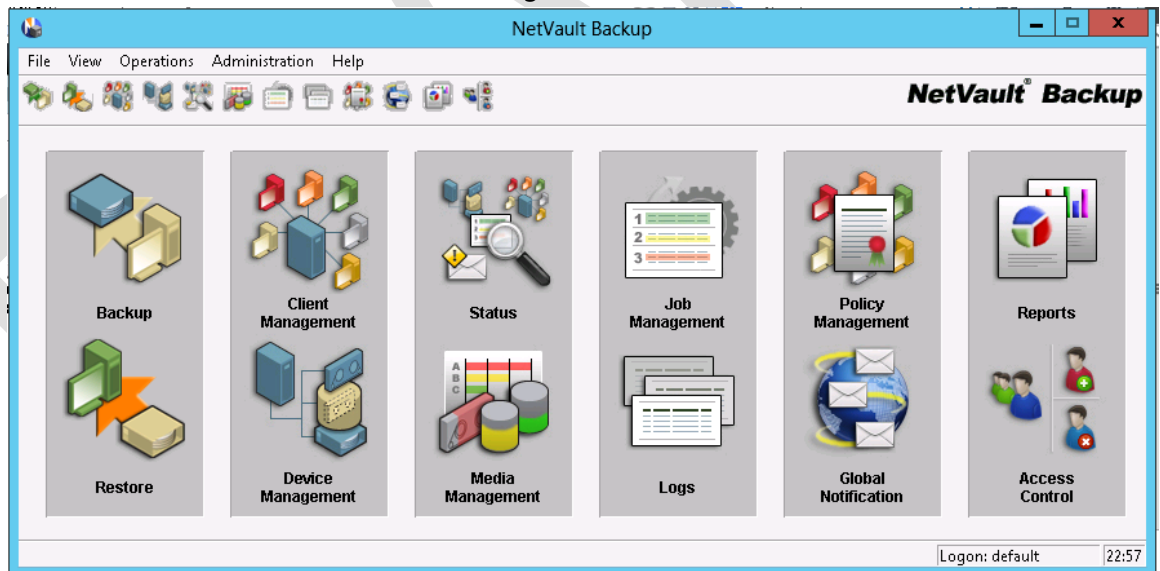
1. Add NetVault serve to the same domain as DR Series Deduplication Appliance (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment).
- NetVault Window 2012 server



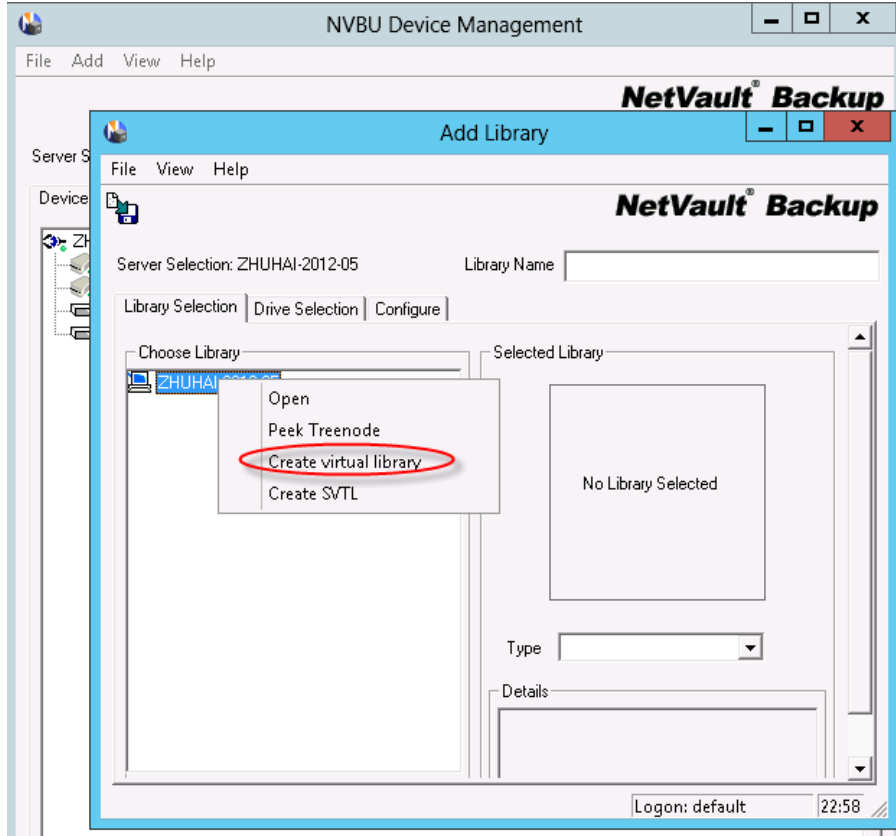
2. On NetVault server, launch **Windows Services** console, set the logon information for '**NetVault Process Manager**' service. Enter CIFS credential that has access permission to DR container share(s), and then restart the service.



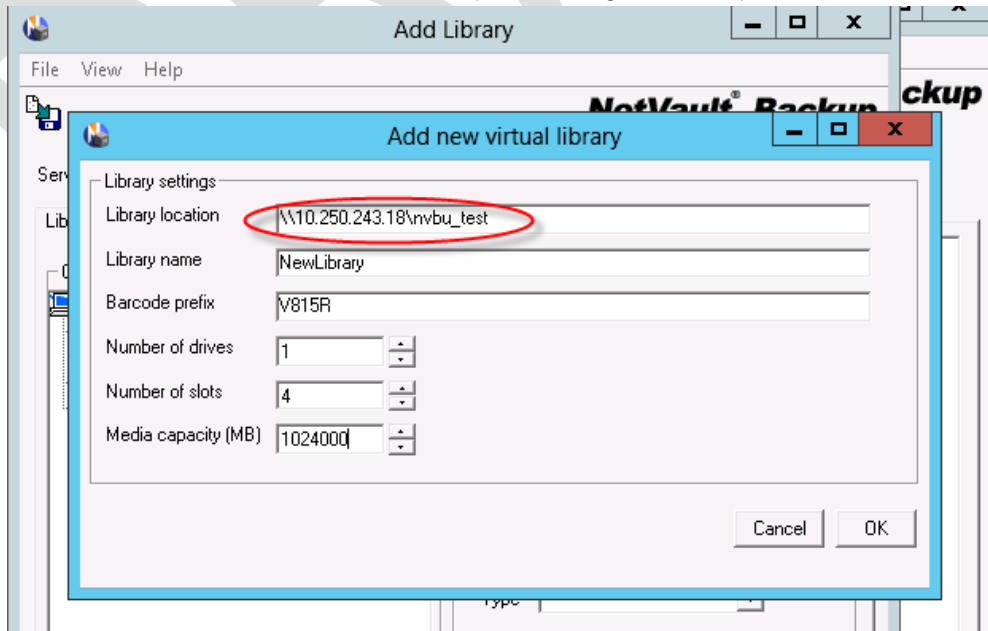
3. Launch **NVBU Console**, click **Device Management**



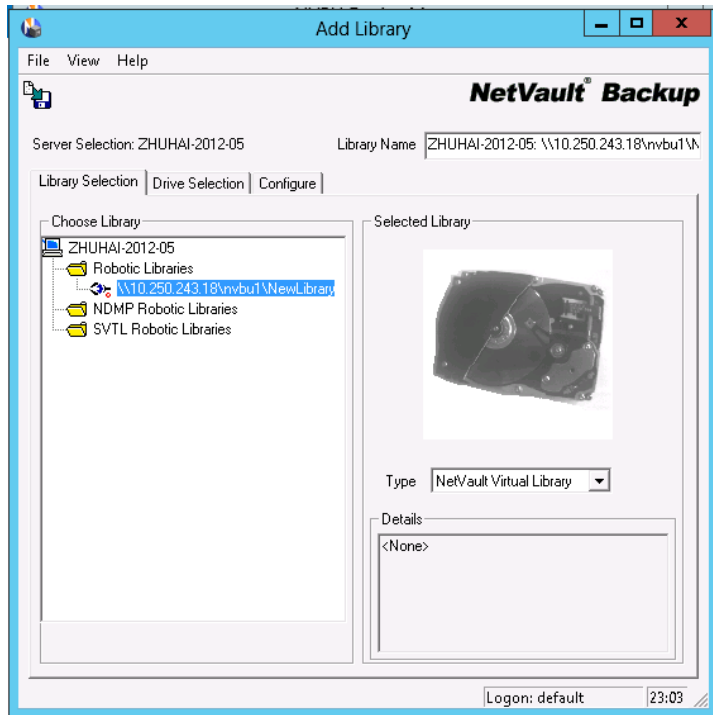
4. Choose **Add** menu, click **Add** -> **Add Library**. In the pop-up **Add Library** window, highlight a client, right click on that machine and choose **Create Virtual Library**



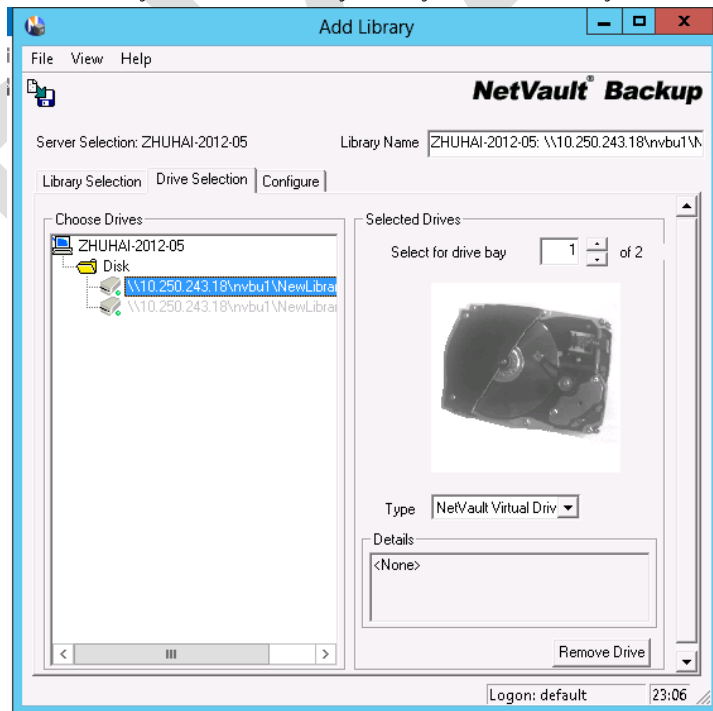
5. Enter source DR container share UNC path, configure other parameters, click **OK**.



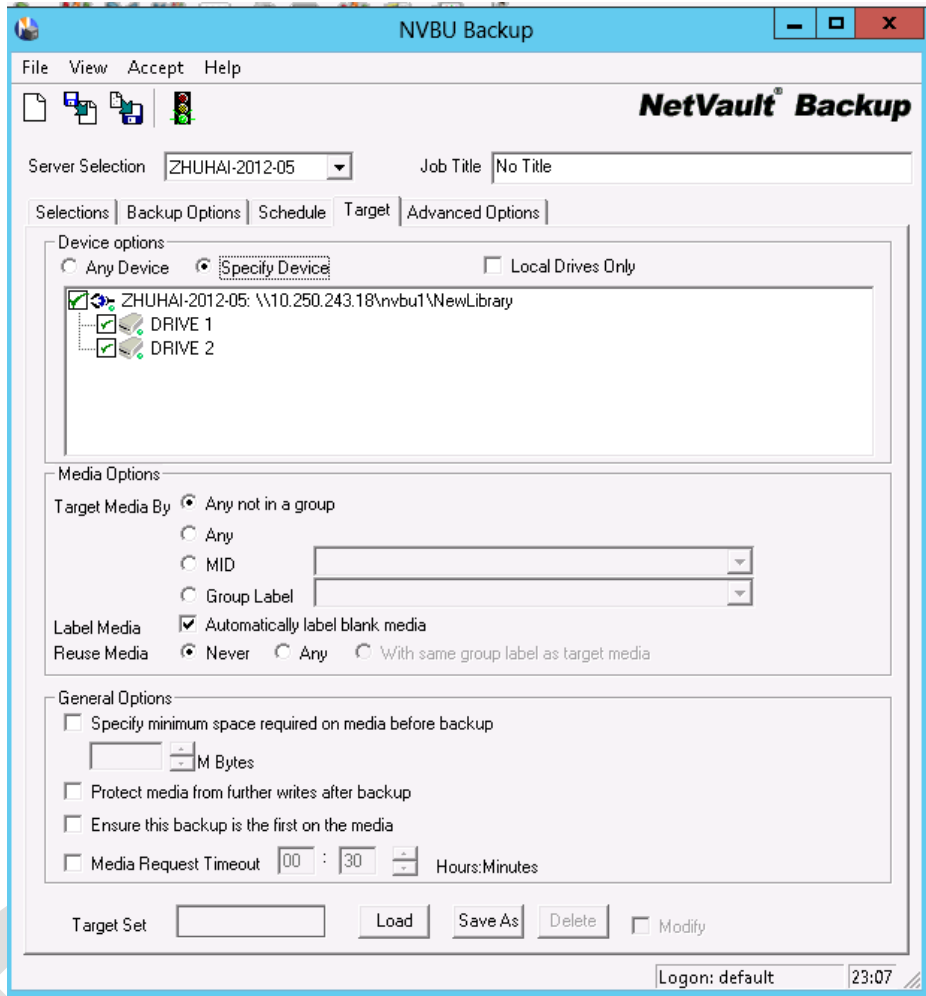
6. On **Library Selection** tab, right click the newly created library, choose **Select**.



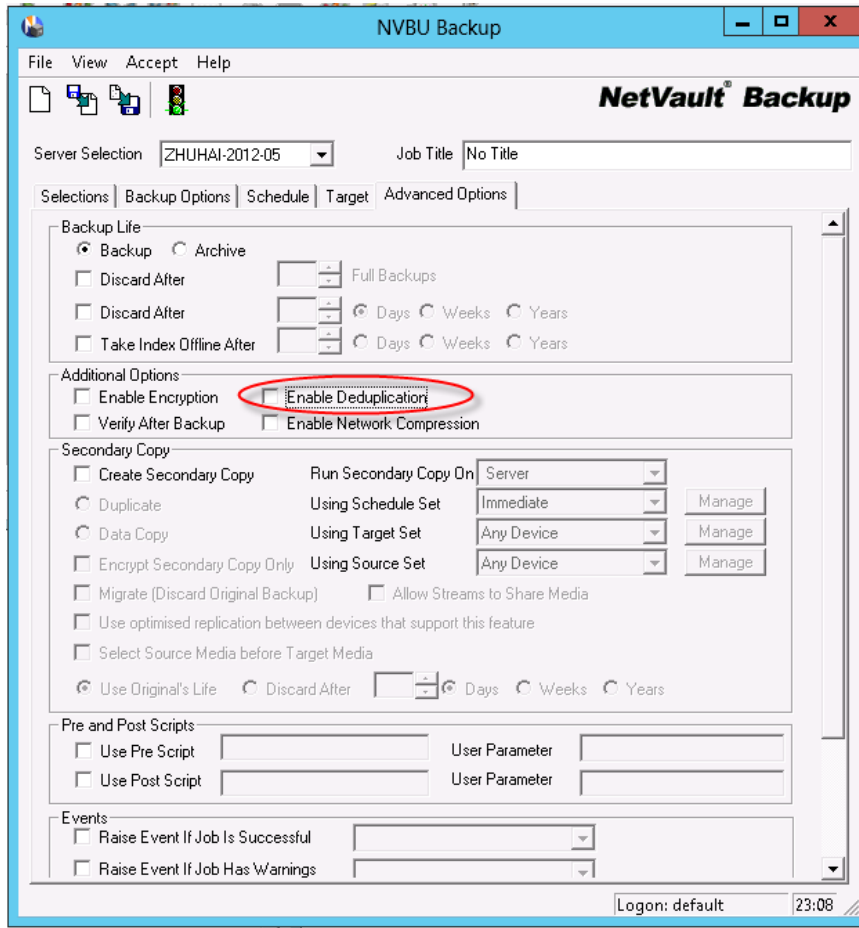
7. On **Drive Selection** tab, pick each of the Drives available for the library, right click on the drive(s), choose **Select**. Make sure all drives are configured in Configure tab, and the library is added successfully. **Save** the library. Verify that the library device is **Online**.



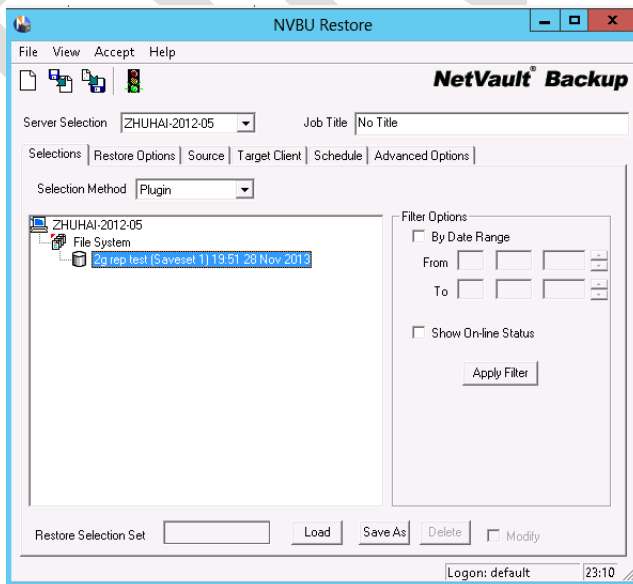
8. Create backup job by clicking **Backup** button on NVBU Console. In Backup job creation window, choose the source DR container library device under **Target** tab.



9. On Advanced Options, uncheck **Enable Deduplication**.

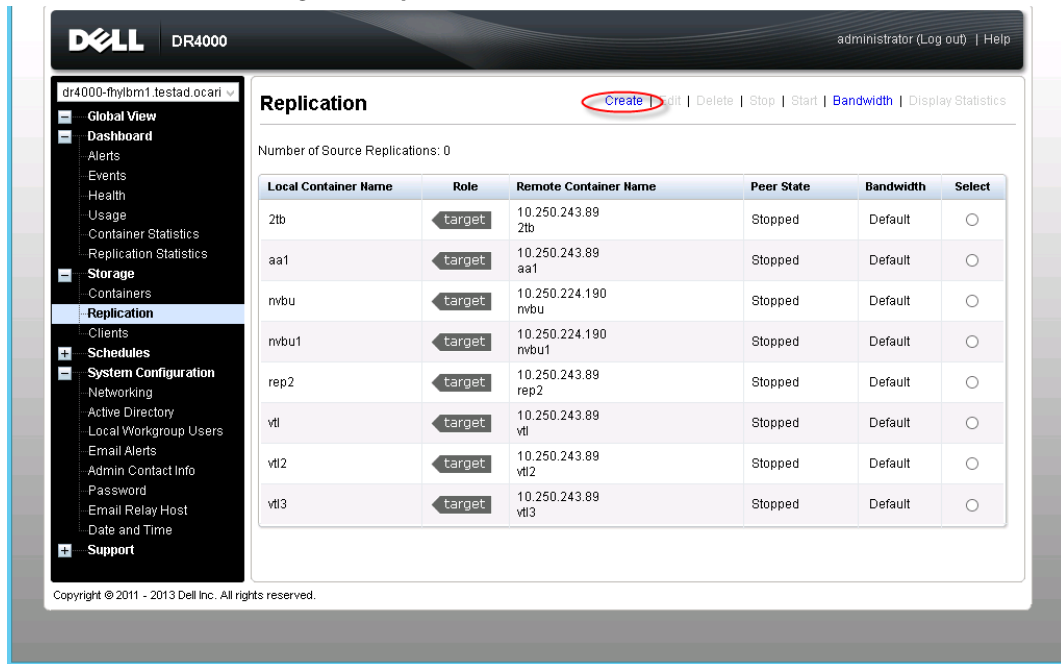


10. After the backup job is completed, a restore point will appear in **NVBU Restore**.

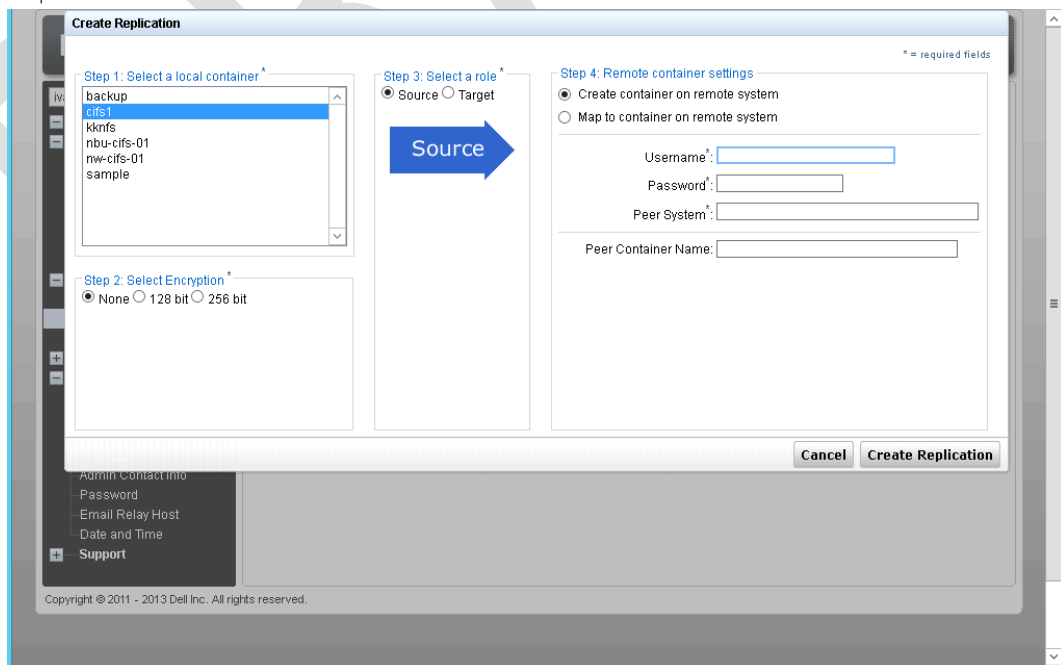


2.2 Set up DR Native Replication from DR Console

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.

Replication Statistics

Container Filter: All Name Peer System

Headers:

Peer Status Replication Status Time To Sync Progress %
 Replication Throughput Network Throughput Network Savings Last Time In Sync
 Peer Container Peer System Encryption

Reset **Apply Filter**

Container	Progress %	Network Throughput	Network Savings	Peer Status	Replication Status
nwbu	100	0 KiB/s	93.34	Stopped	INSYNC
nwbu1	100	1 KiB/s	100.00	Online	INSYNC

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

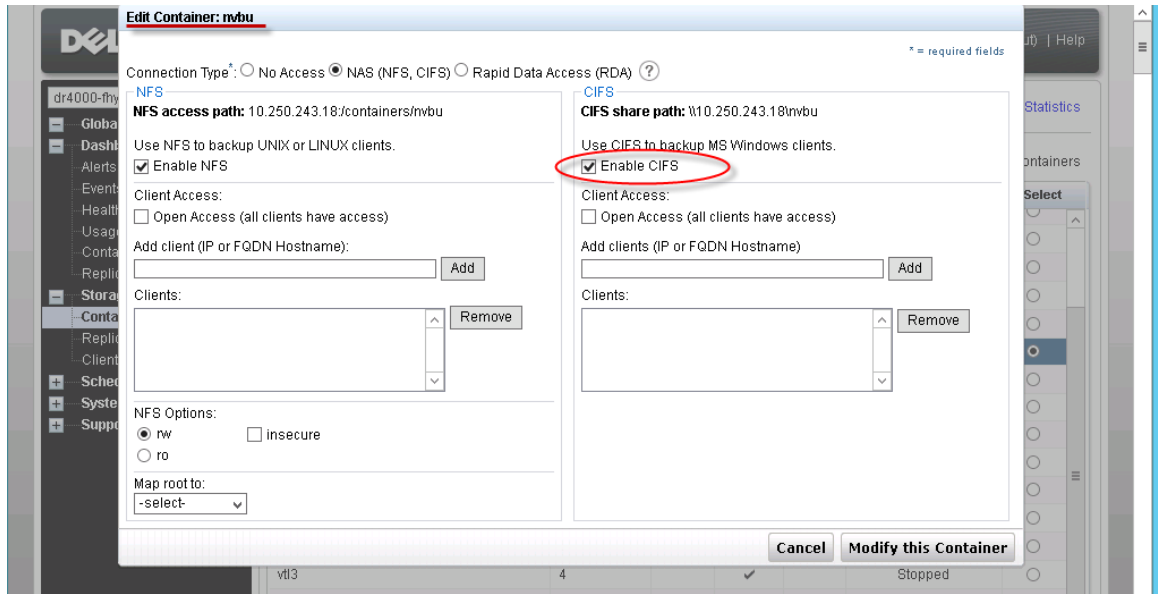
Replication [Create](#) | [Edit](#) | [Delete](#) | **Stop** | [Start](#) | [Bandwidth](#) | [Display Statistics](#)

Number of Source Replications: 1

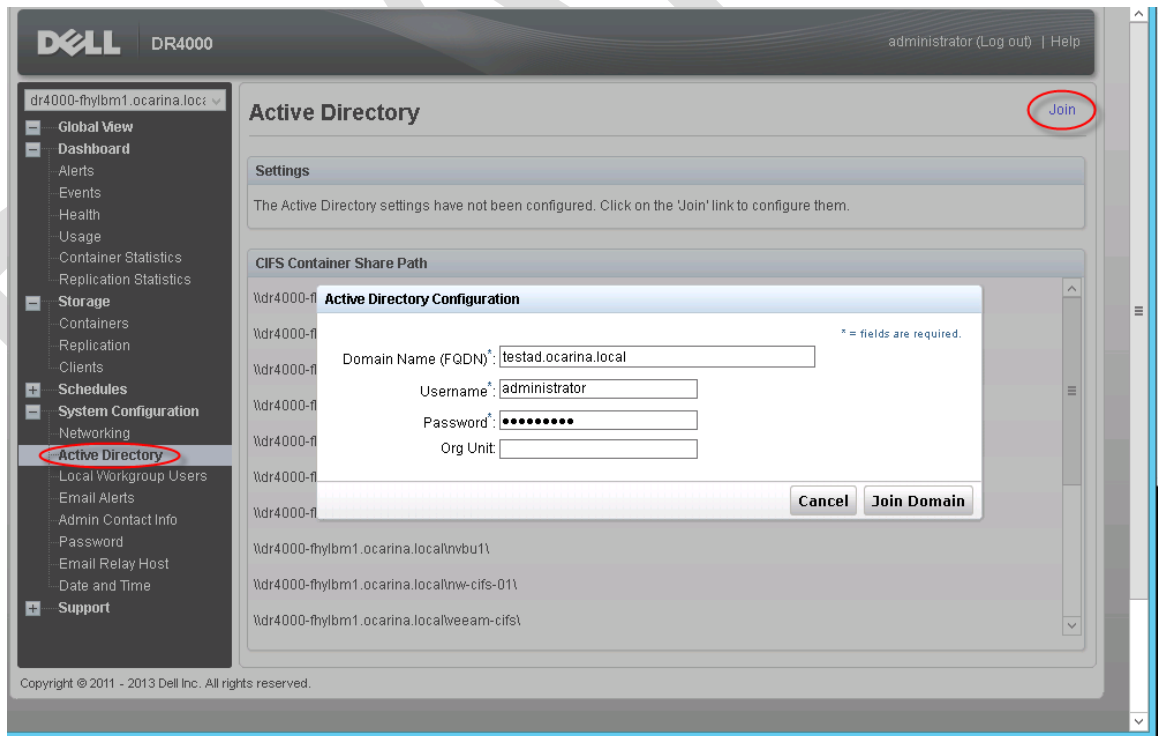
Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
nwbu	source	10.250.243.18 nwbu	Online	Default	<input checked="" type="radio"/>
nw-cifs-01	target	10.250.225.79 nw-cifs-01	Disconnected	Default	<input type="radio"/>



5. Modify target container on target DR management console and **Enable CIFS** share path

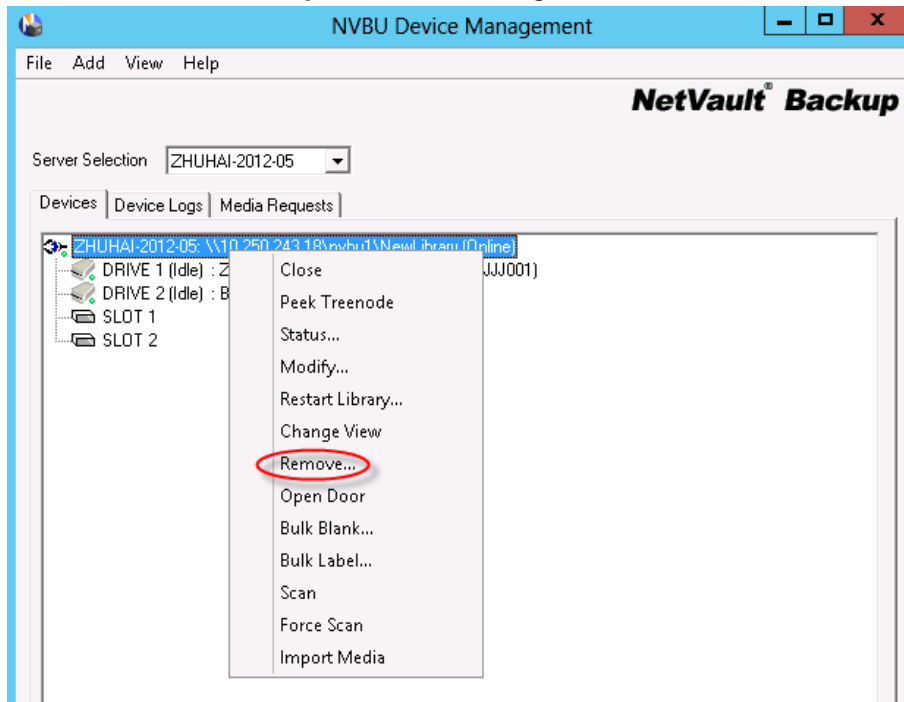


6. Add target DR to the same domain as NetVault Server, add target DR into Active Directory Domain (Optional: only applies when both DR and NVBU server are in Active Directory Domain environment).



2.3 Restore from Replication Target

1. Launch **NVBU Console**, go to **Device Management**, **Remove** the source VTL.



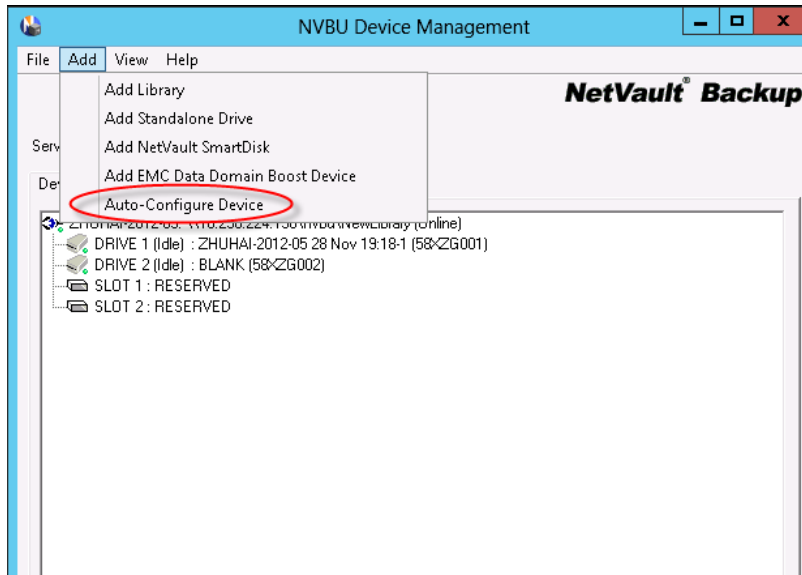
2. Modify C:\Program Files (x86)\Quest Software\NetVault Backup\config\diskdevices.cfg, change the following locations to point to target DR IP or hostname. Save diskdevices.cfg after the modification is completed.

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

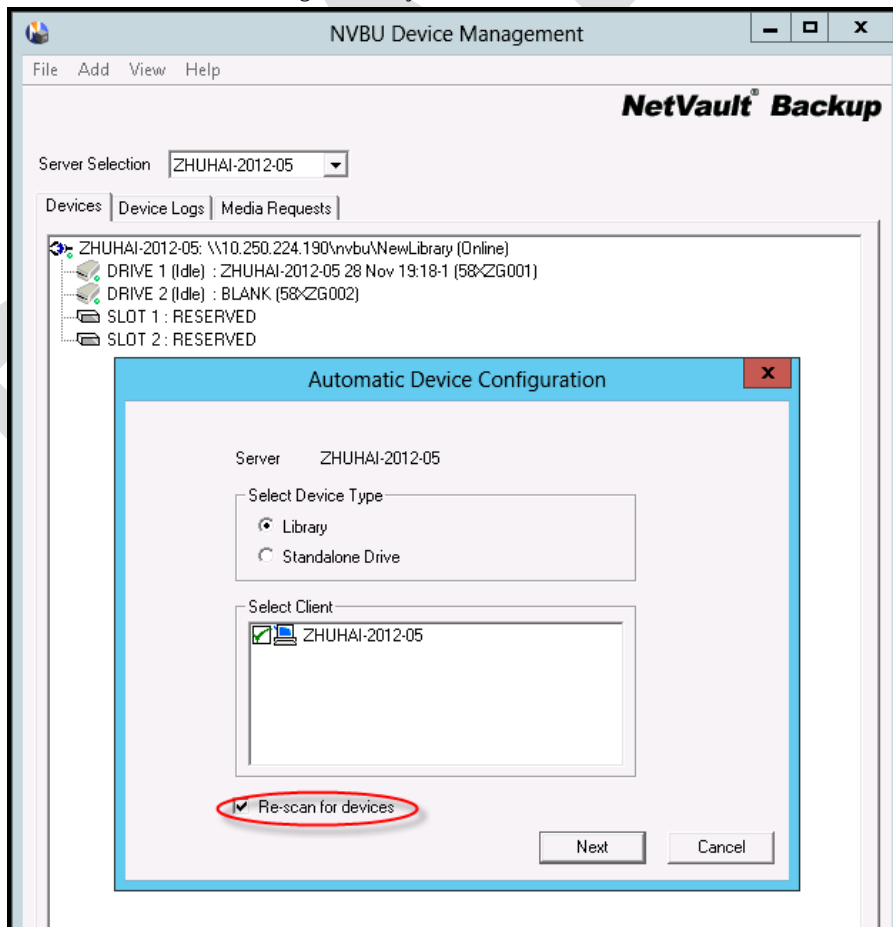
```
[drives]  
location=\\10.250.243.18\nvbu1\NewLibrary\drives\1  
location=\\10.250.243.18\nvbu1\NewLibrary\drives\2
```



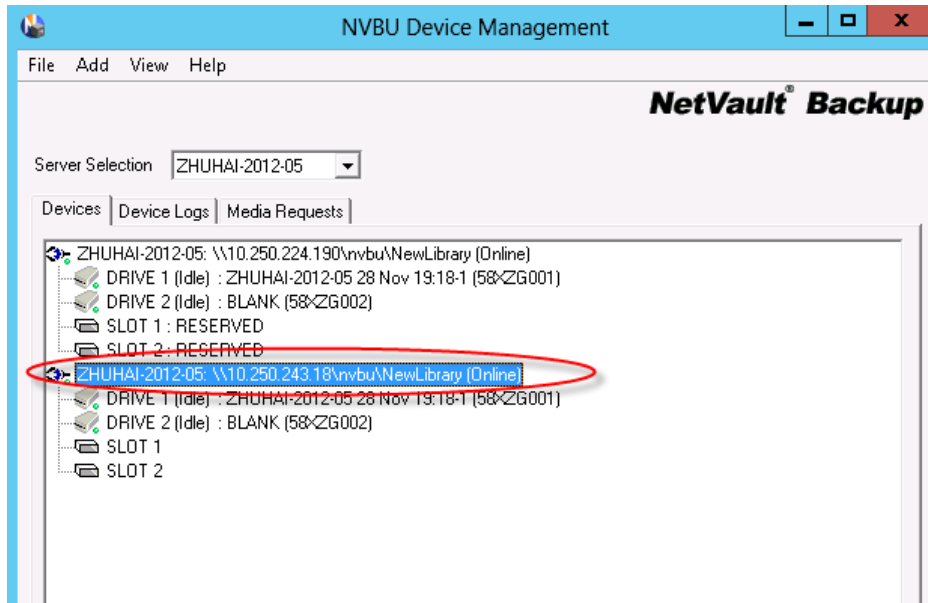
3. In NVBU **Device Management** menu, click **Add -> Auto-Configure Device**



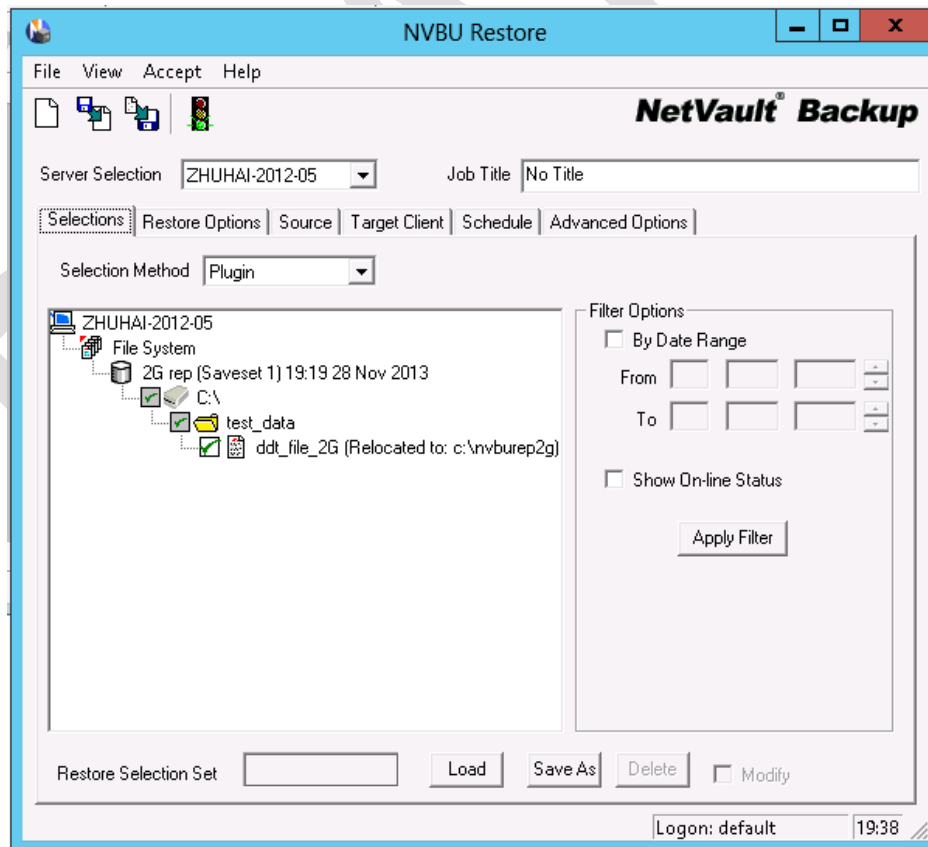
4. NVBU will detect the target library with **Re-scan for devices**



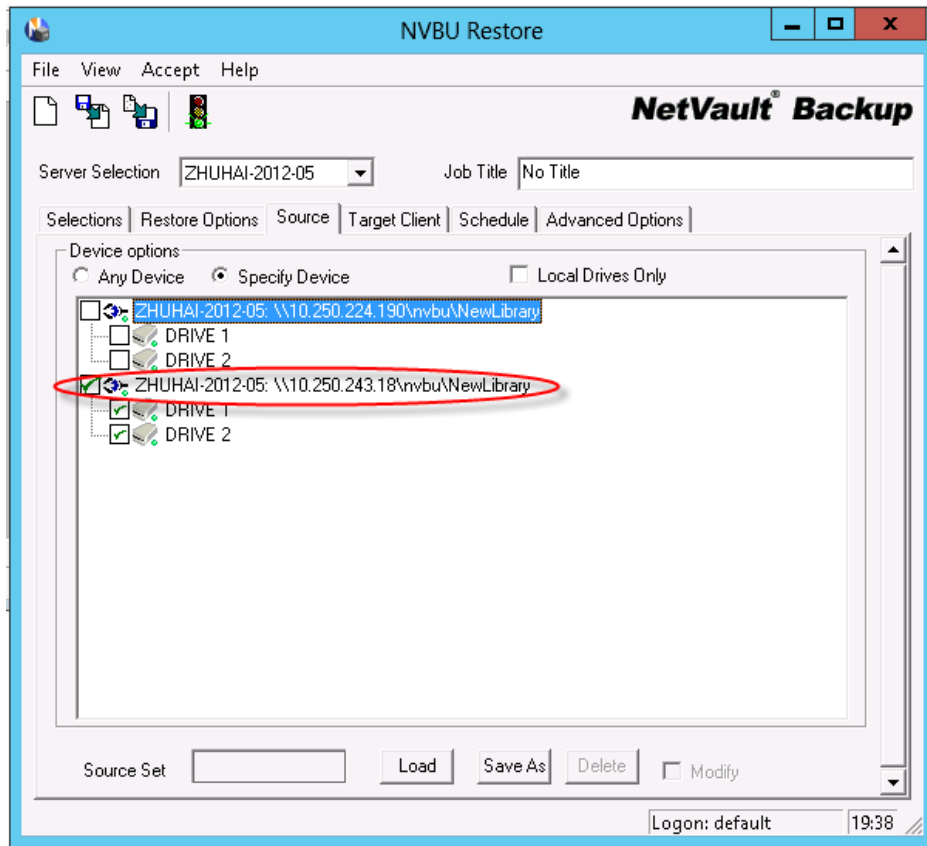
5. The target container device show as **Online** in **Device Management** UI



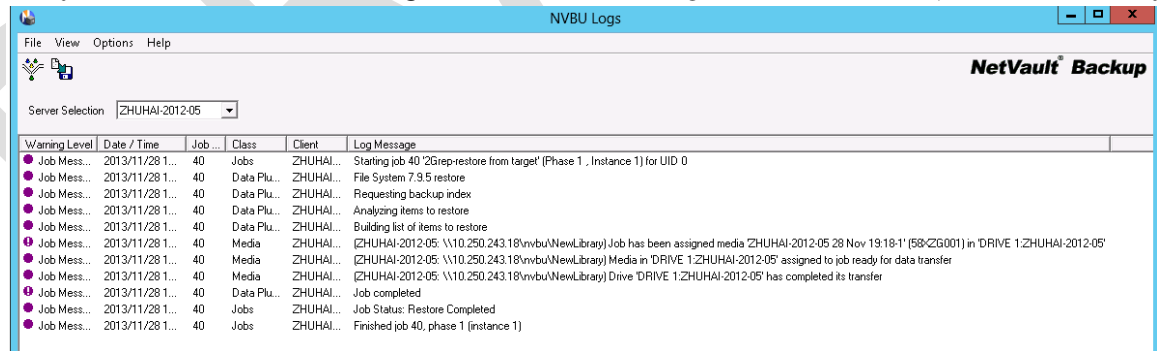
6. From **NVBU Console**, click **Restore**. On **Selections** tab, choose data set that needs to be restored.



- On **Source** tab, choose the target library device.



- 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 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 DR4100 web interface. The top header includes the Dell logo, the model 'DR4100', and the user 'EdwinZ-SW-01'. There are 'Help' and 'Log out' links. The left sidebar menu has categories: Dashboard, Alerts, Events, Health, Usage, Statistics: Container, Statistics: Replication, Storage, Containers, Replication, Compression Level, Clients, Schedules, Replication Schedule, Cleaner Schedule (highlighted with a red box), System Configuration, Networking, Active Directory, Local Workgroup Users, Email Alerts, Admin Contact Info, Password, Email Relay Host, Date and Time, Support, Diagnostics, Software Upgrade, and License. The main content area is titled 'Cleaner Schedule'. It shows the system time zone as 'US/Pacific, Fri Jul 5 05:00:41 2013'. A note states: 'Note: When no schedule is set, the cleaner will run as needed.' Below this is a table with columns 'Day', 'Start Time', and 'Stop Time'. The table rows are: Sun, Mon, Tue, Wed, Thu, Fri, Sat, all with '--' in the Start and Stop Time columns. To the right of the table is an 'Edit Schedule' button, which is highlighted with a red box. A large red arrow points from the text 'Schedule Cleaner' to the 'Edit Schedule' button.

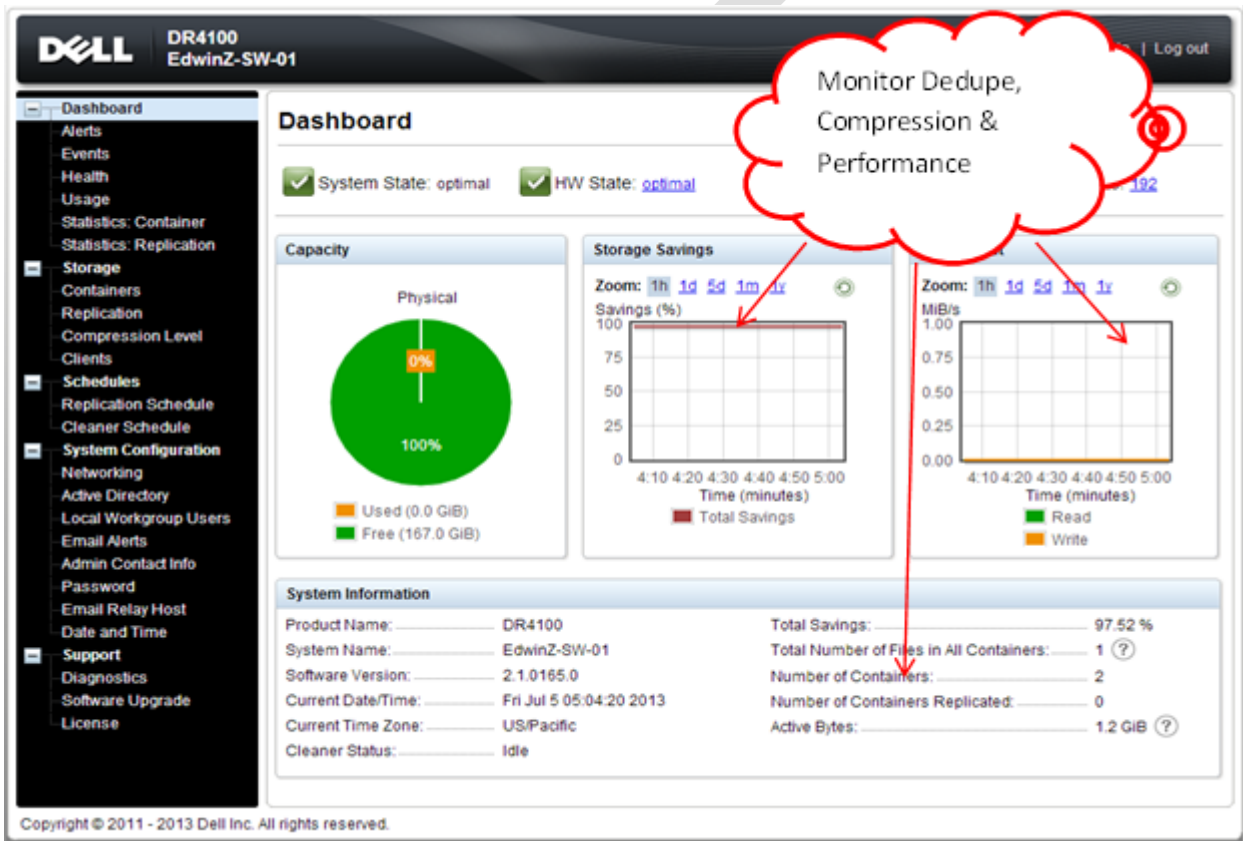
Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--



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>

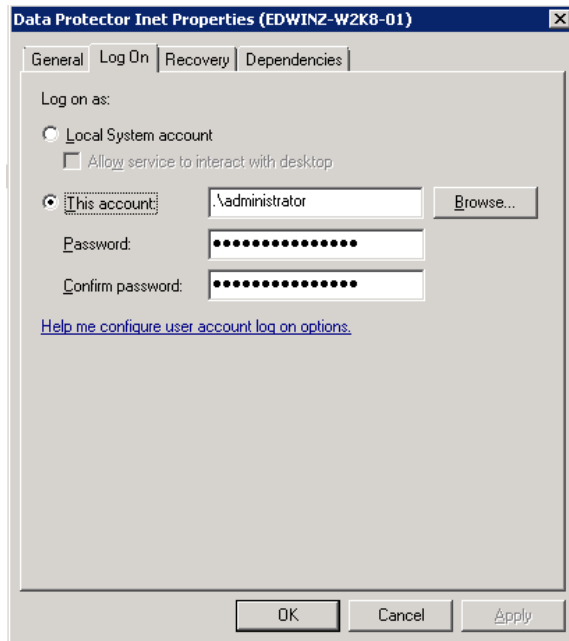
2. **DR is standalone CIFS server:** Make sure Windows NVBU services and DR Series Deduplication Appliance have the same username and password defined in Local Workgroup Users. Also make sure this CIFS user has appropriate access permission to the DR Series Deduplication Appliance container share. NVBU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

