



Setting Up Dell™ DR Series Deduplication Appliance on HP® Data Protector 7.0

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 Set Up HP Data Protector	12
2.1 Procedure for backing up Windows Environment.....	12
2.2 Procedure for backing up Unix/Linux Environment	16
3 Create a New Backup Job with DR Series Deduplication Appliance as the Target.....	17
4 Set up DR Native Replication & Restore from Target Container.....	23
4.1 Build Replication Relationship between DRs	23
4.2 Run backup to source DR (Optional: only when there is no backup data on the source DR container).....	25
4.3 Prepare Replication Target for restore.....	27
4.4 Restore from target DR.....	32
5 Set Up the DR Series Deduplication Appliance Cleaner	33
6 Monitoring Deduplication, Compression and Performance	34
7 Appendix.....	35
7.1 Create a Storage Device for CIFS.....	35
7.2 Create a Storage Device for NFS.....	37
7.3 User commands	37



Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for HP Data Protector 7.0. 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/HP Data Protector build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/ HP Data Protector software version used.

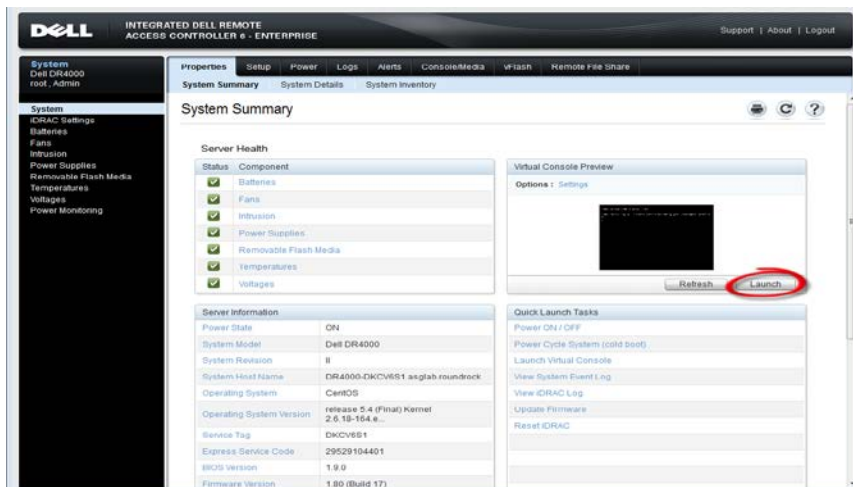


1 Install and Configure the DR Series Deduplication Appliance

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 in to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use user name and password of "**root/calvin**".



4. Launch the virtual console.



5. After 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).

```
Ocarina release 1 (EAR-1.00.00) Build: 32850
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:
```

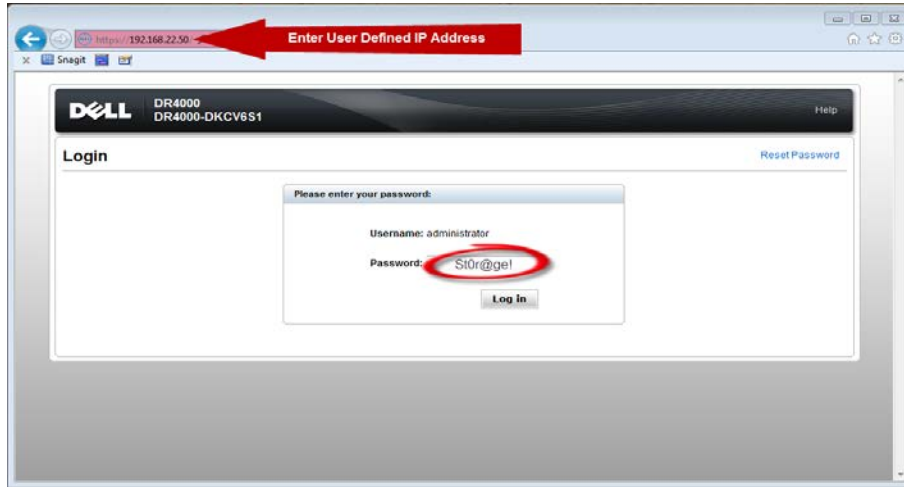
7. View the summary of preferences and confirm that it is correct.

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



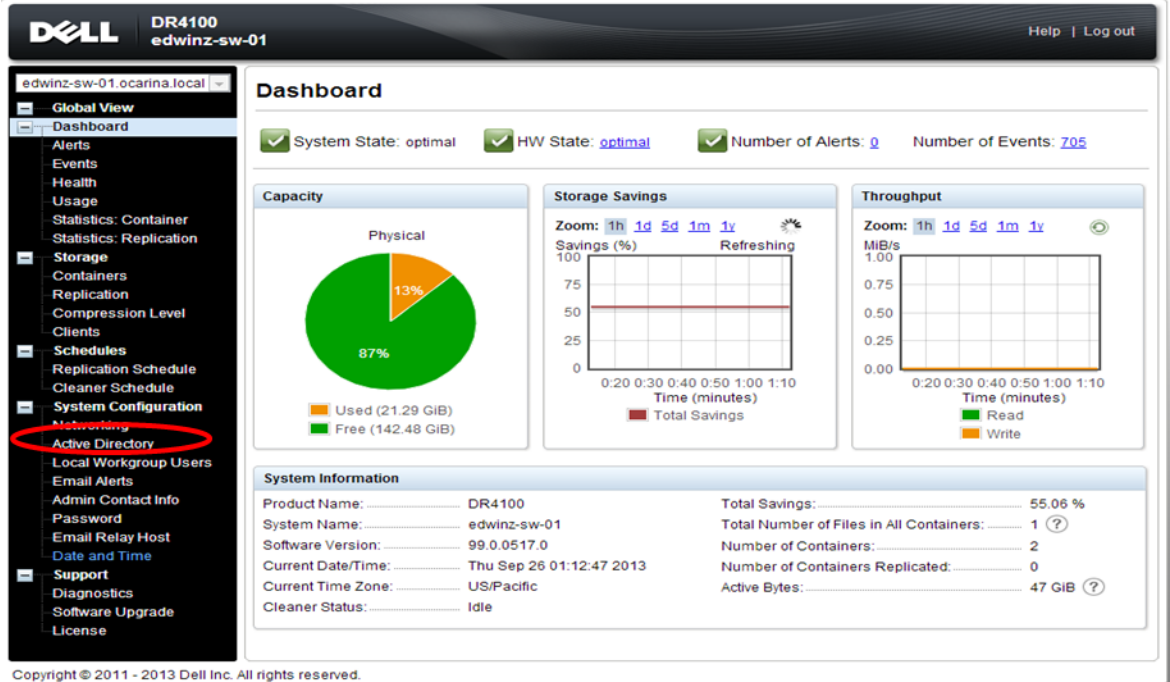
- Log on to DR Series Deduplication Appliance administrator console, using the IP address you just provided for the DR Series Deduplication Appliance, with username **administrator** and password **St0r@ge!** (The "0" in the password is the numeral zero).



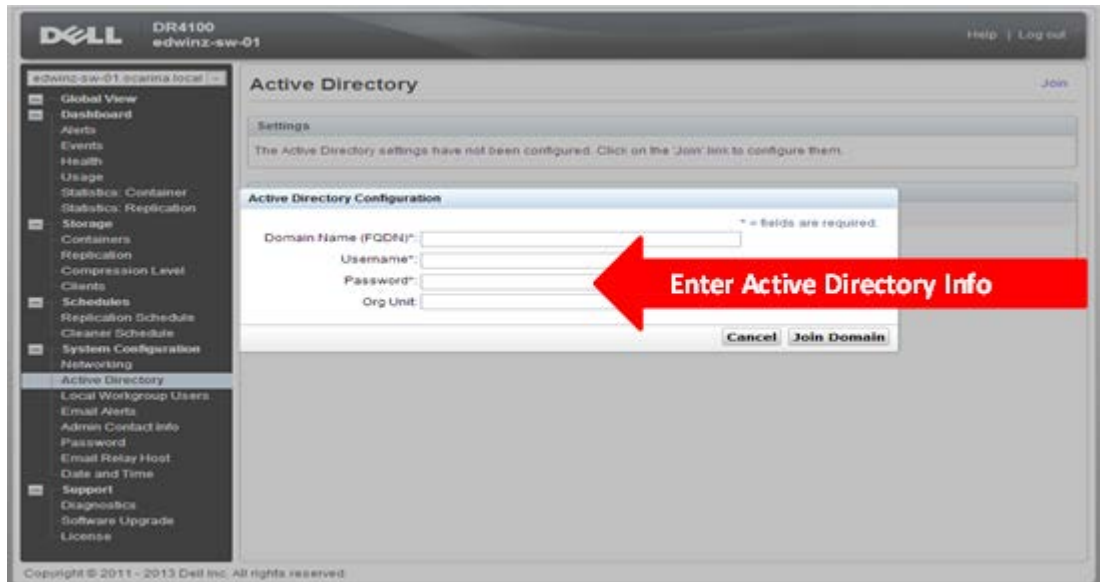
- Join the DR Series Deduplication Appliance to Active Directory.

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

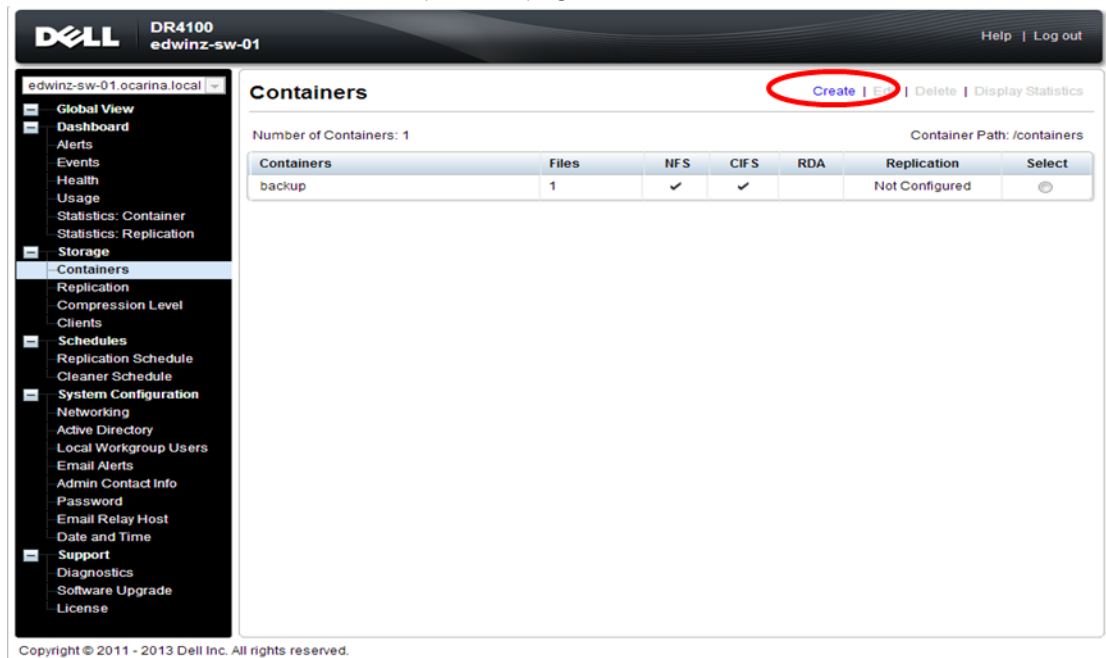
- Select **Active Directory** from the menu panel on the left side of the management interface.



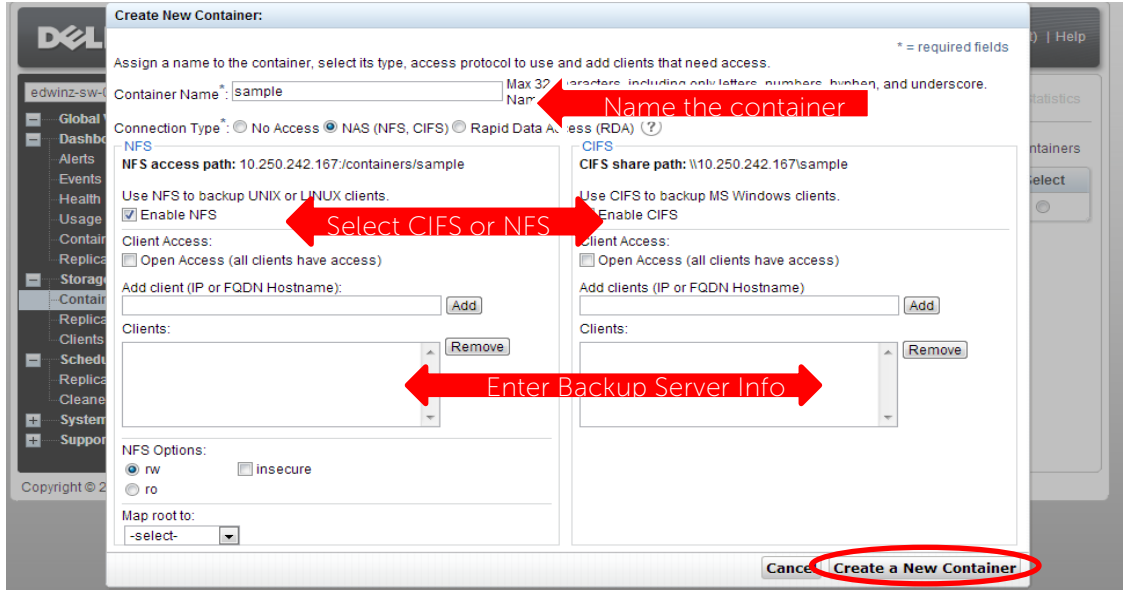
- Enter your Active Directory credentials.



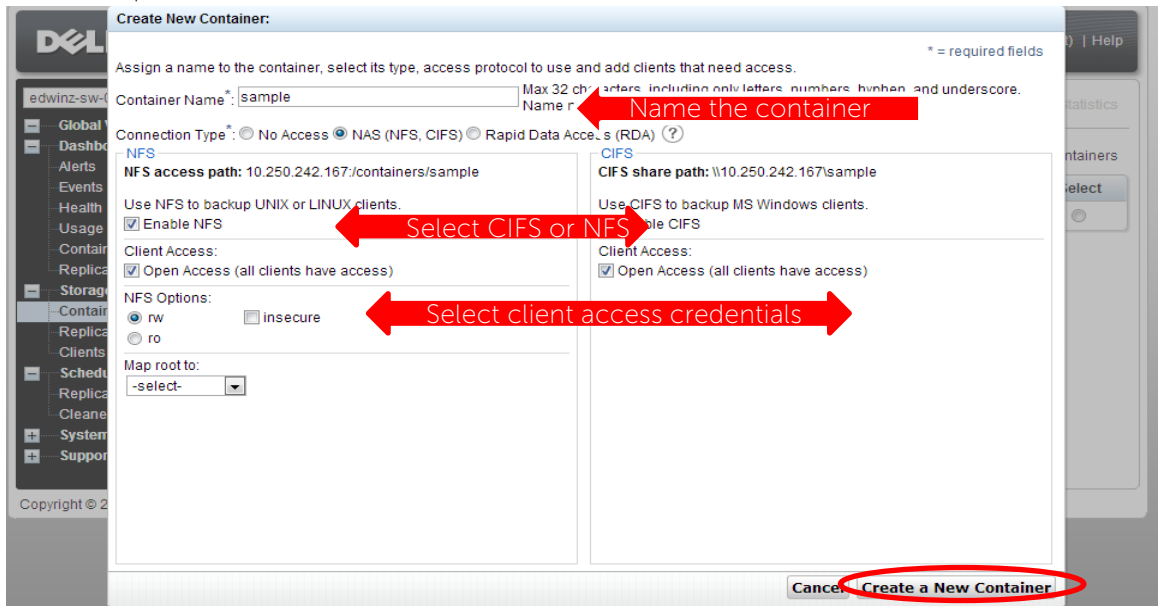
10. Create and mount the container. Select **Containers** in the tree on the left side of the dashboard, and then click the **Create** at the top of the page.



11. Enter a **Container Name** and choose **Connection Type**, select **Enable CIFS** or **Enable NFS** check box. HP Data Protector supports both CIFS and NFS protocols.



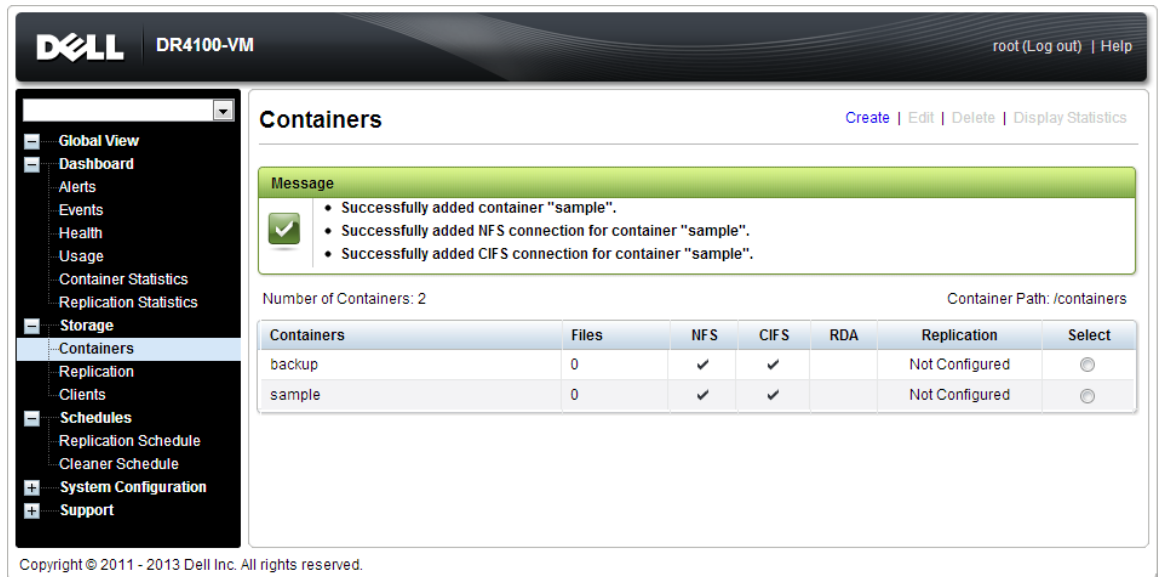
12. Select the preferred client access credentials.



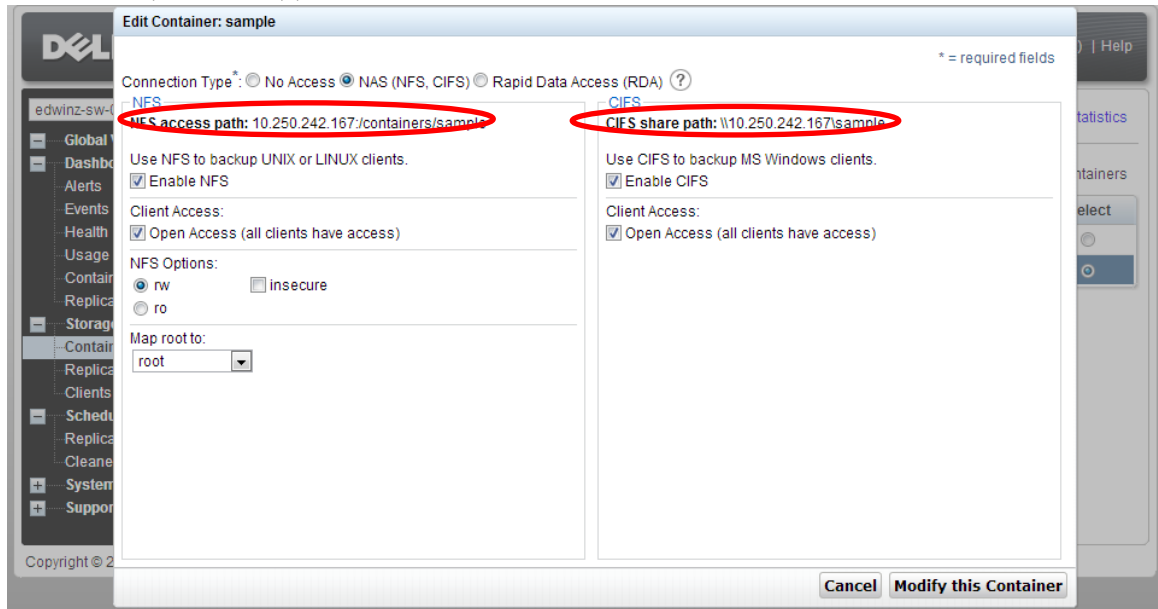
Note: For improved security, Dell recommends adding IP addresses for the following (Not all environments will have all components):
 Backup console (HP Data Protector Server, HP Data Protector Clients)



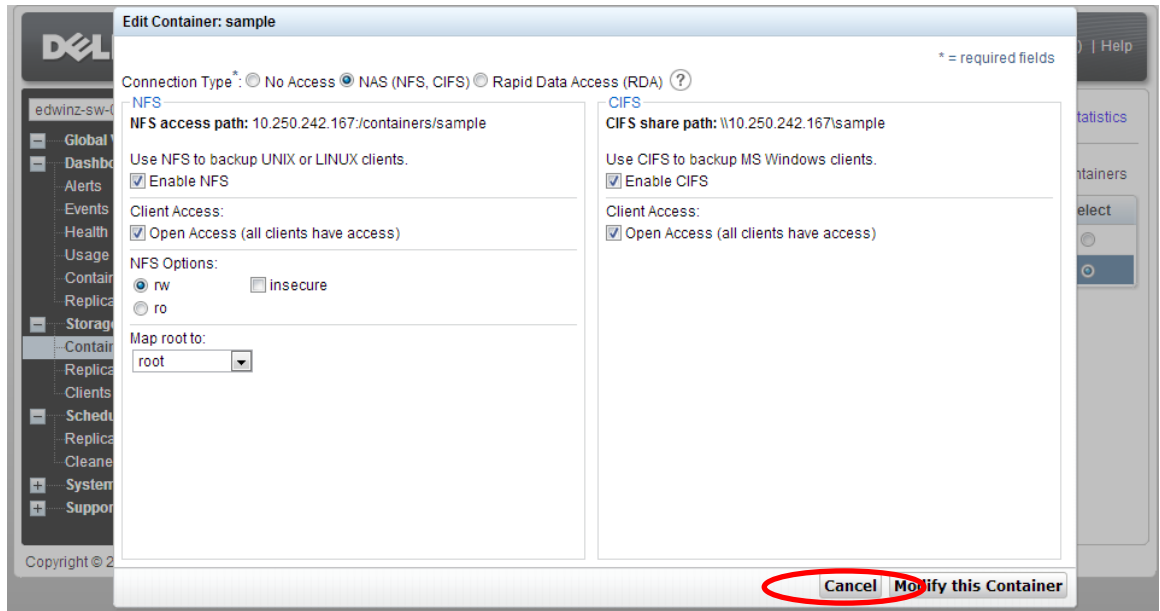
13. Click **Create a New Container**. Confirm that the container is added.



14. Click **Edit**. Note down the container share/export path, which you will use later to target the DR Series Deduplication Appliance.



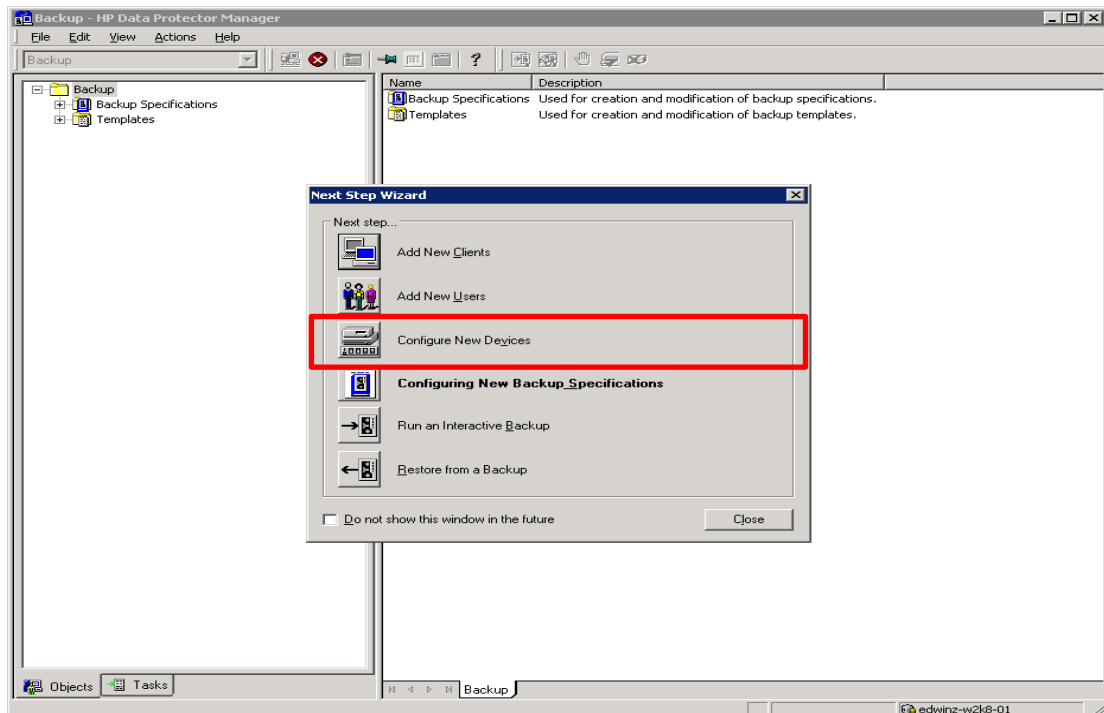
15. Click **Cancel** to exit.



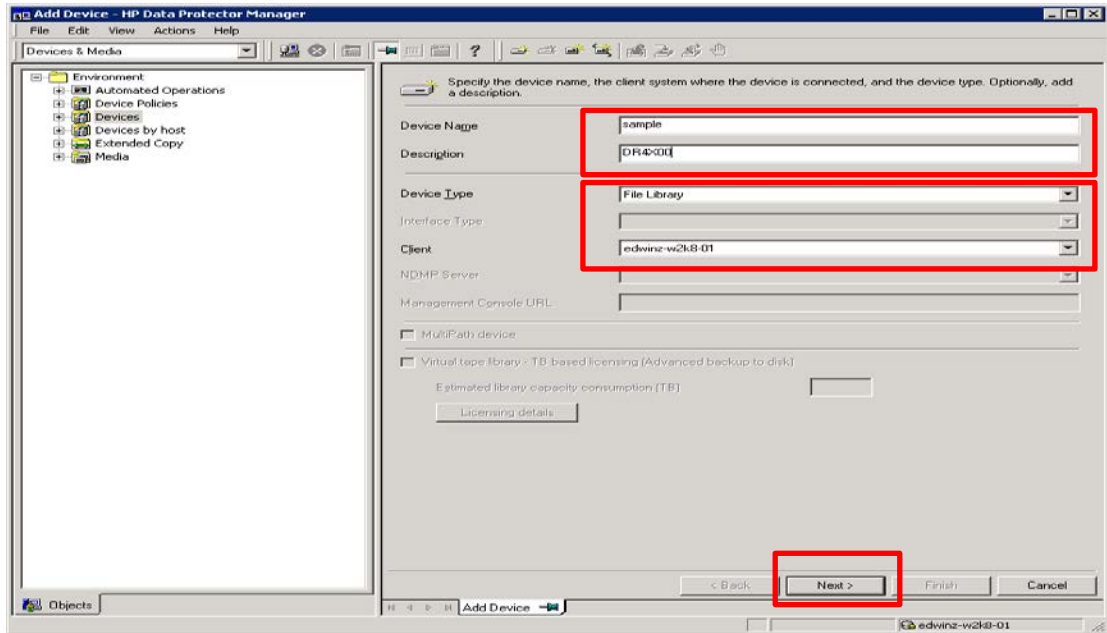
2 Set Up HP Data Protector

2.1 Procedure for backing up Windows Environment

1. Open **HP Data Protector Manager**. Click **Configure New Devices**, which goes to **Devices & Media** menu.



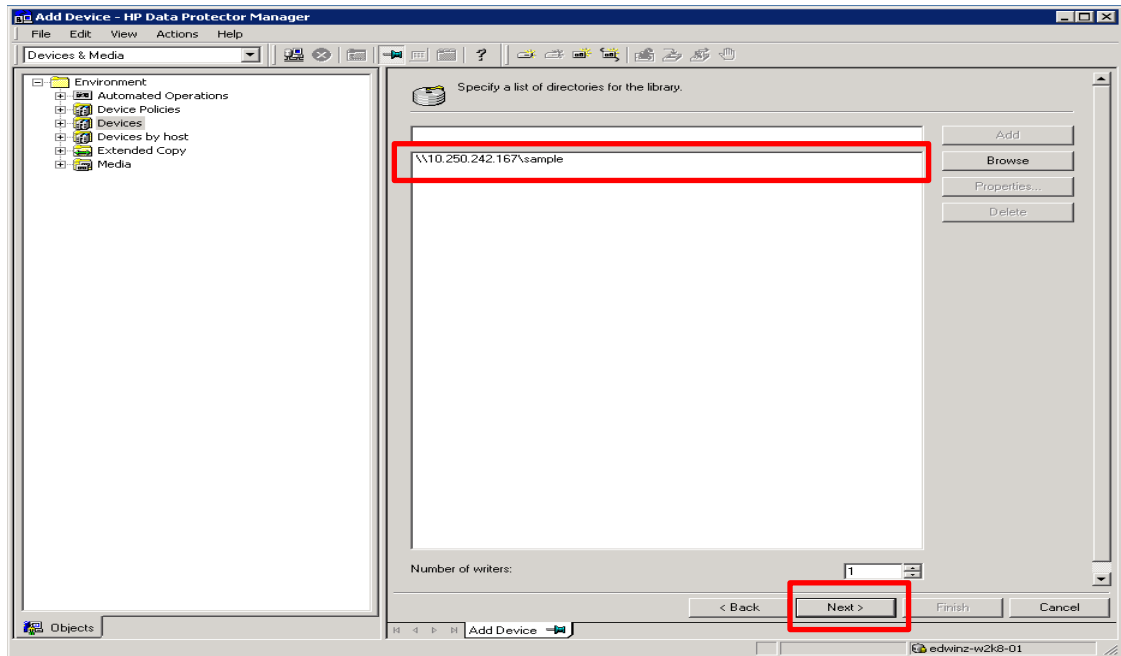
2. Right-click **Devices** and choose **Add Device**. In the next window, specify the **Device Name** and **Description** that identifies the **File Library Device**. Select **File Library** for the **Device Type**, and enter info for the **Client**. Click **Next**.



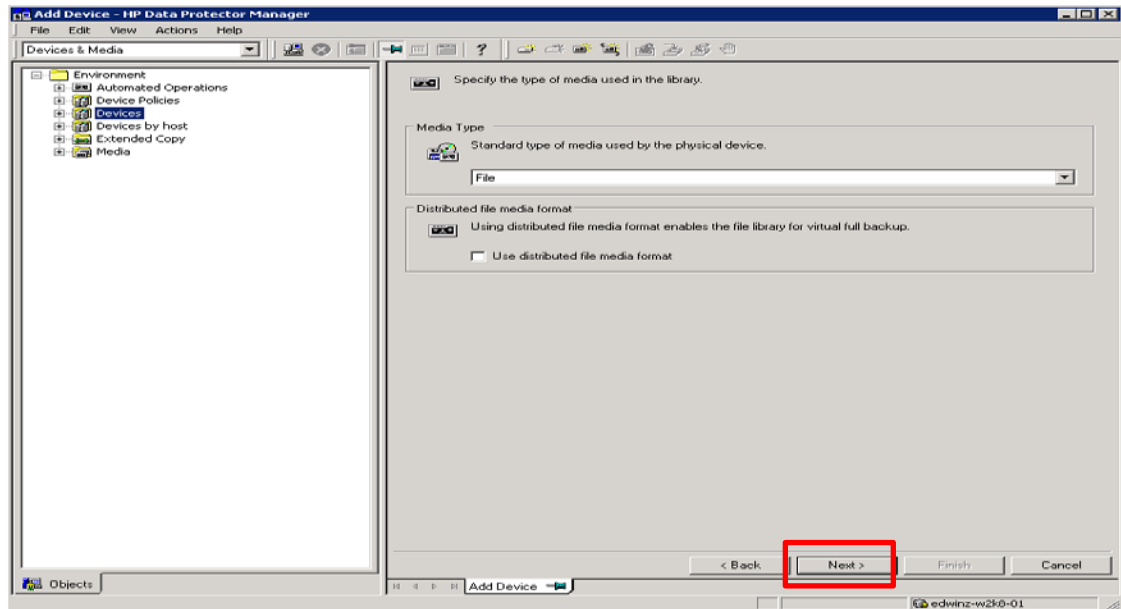
Note: The Windows service account for HP Data Protector requires appropriate permissions to the DR container share for the step below to complete successfully. See **Appendix A** for setting up the HP Data Protector service account correctly. This should be done before the next step.



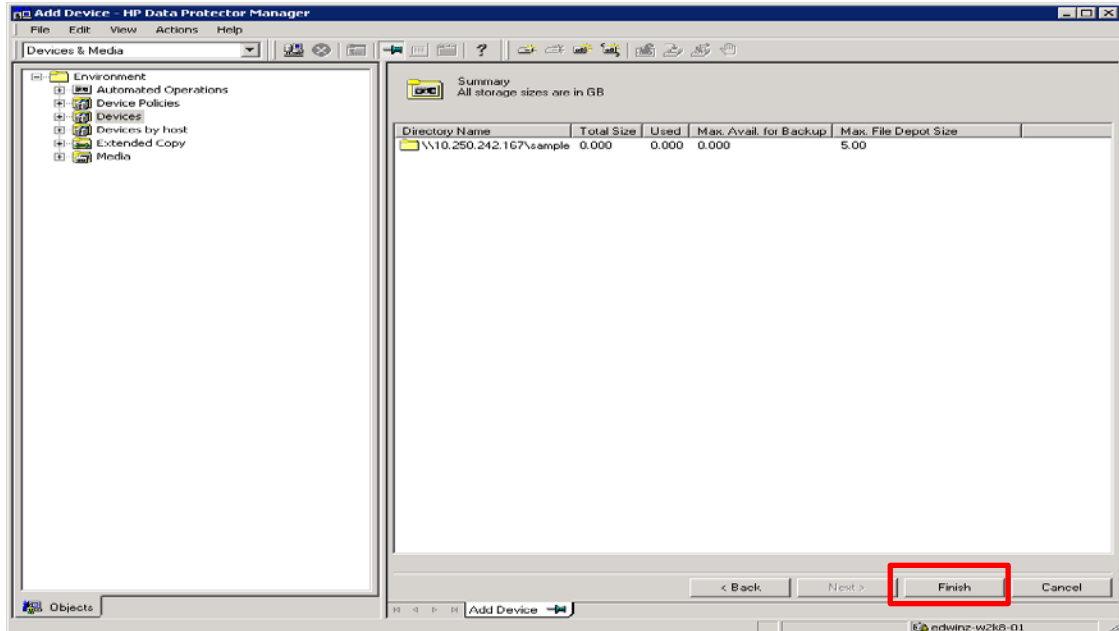
- The next window asks for the path to the library that is the UNC path to the DR container share as described below. Specify a list of directories for the library. You can also specify the number of writers for the library, it defaults to 1. Click **Properties** to assign proper values to the file library parameters, including **Maximal File Depot Size**. Click **Next**.



- The **Media Type** default is **File**. Click **Next**.



5. Click **Next**. The **Summary** window shows the total physical storage size of that particular File Library Device on the DR container.



6. Click **Finish**. In next windows click **Close** to close it.

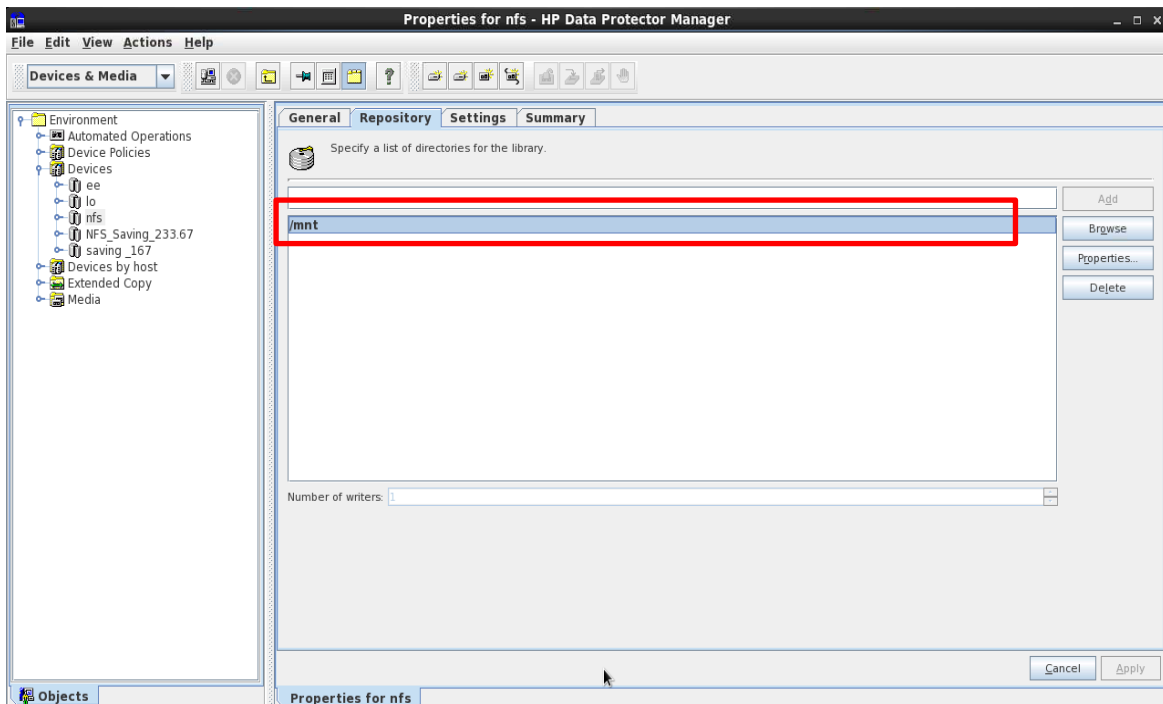
2.2 Procedure for backing up Unix/Linux Environment

NOTE:

Make sure that you can mount/verify the NFS share from the UNIX/Linux client system. Please see **Appendix B** for how to mount/verify the NFS share.

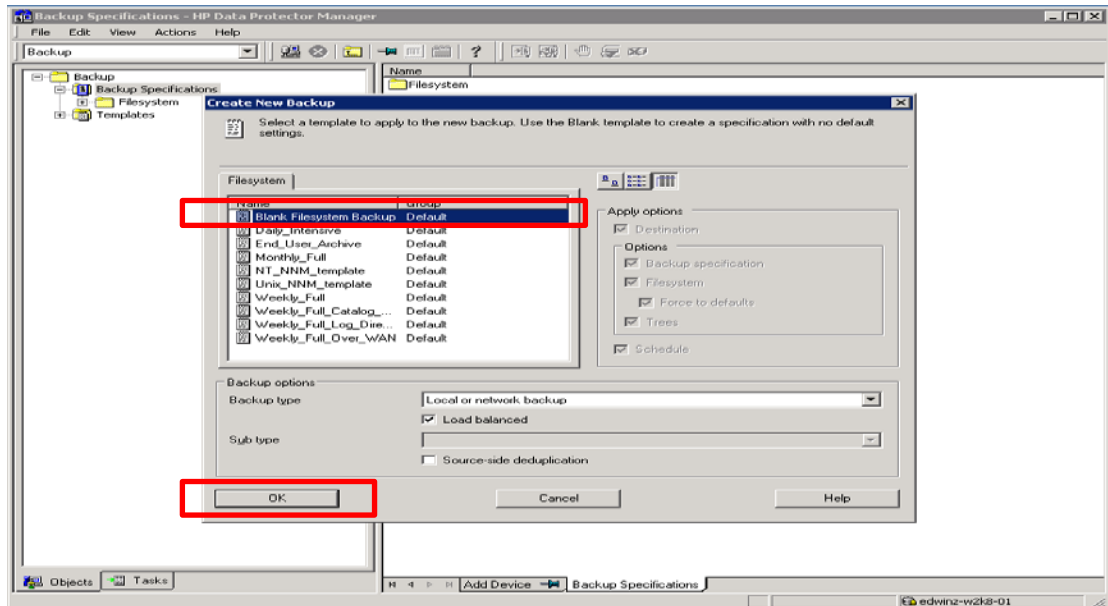
The procedure for the Unix/Linux Environment is very similar to the procedure for the Windows Environment. One difference is that in **Step#3**, enter the UNIX path of the DR container export is used instead of a UNC path, as described below.

For other details, please refer to the Procedure for backing up Windows Environment.

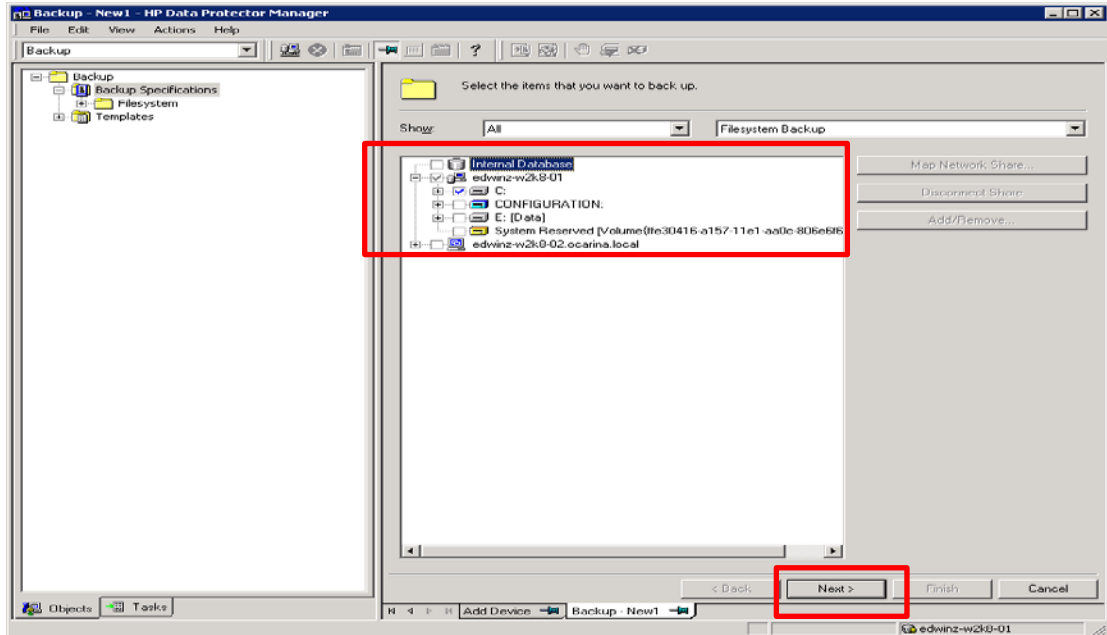


3 Create a New Backup Job with DR Series Deduplication Appliance as the Target

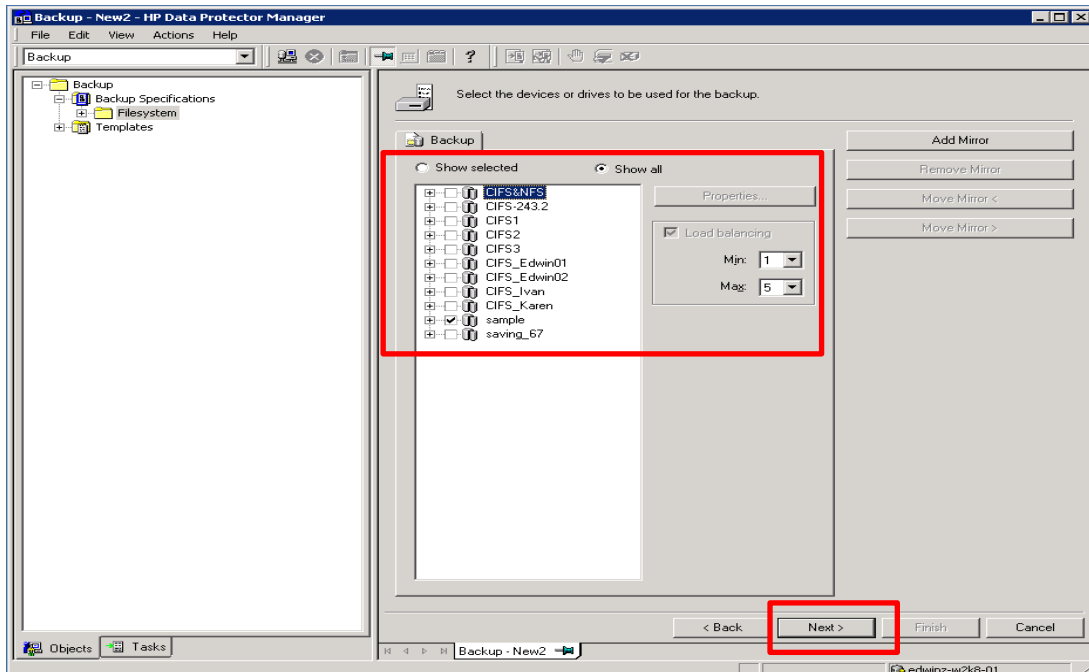
1. In the **Context List** drop-down menu, click **Backup**. In **Scoping Pane**, expand **Backup** and then click **Backup Specifications**. In expanded sub-tree view, right-click the **Filesystem** item and select **Add Backup**.



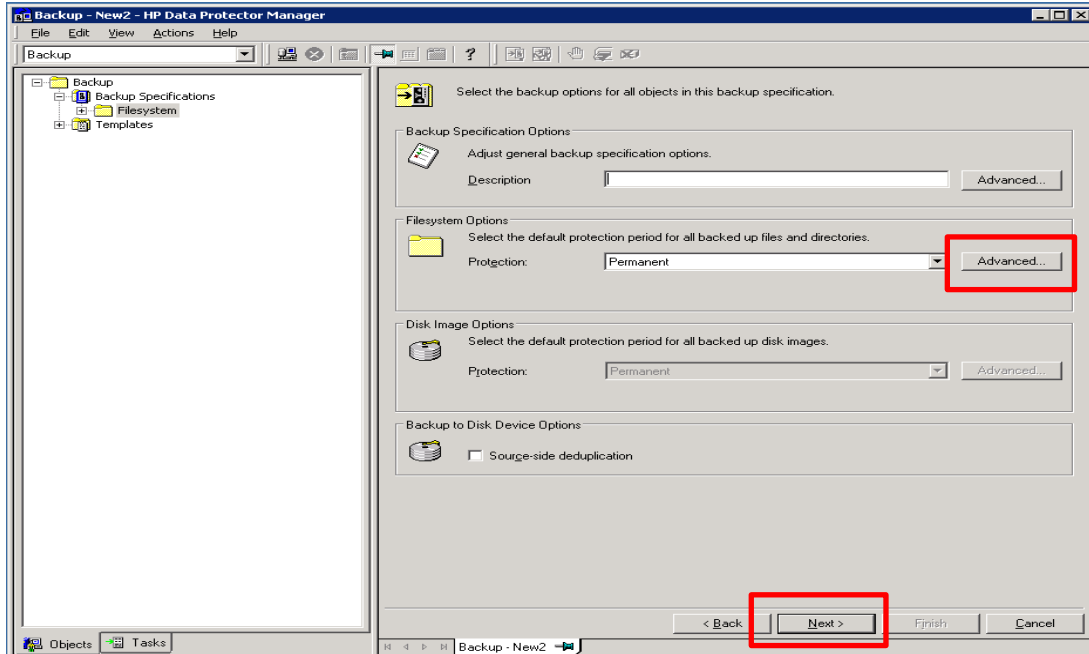
2. Select the **Blank Filesystem Backup** template and click **OK**. Check any source data set that needs to be backed up. In this example, it's the whole local "C:\:" drive. Then click **Next**.



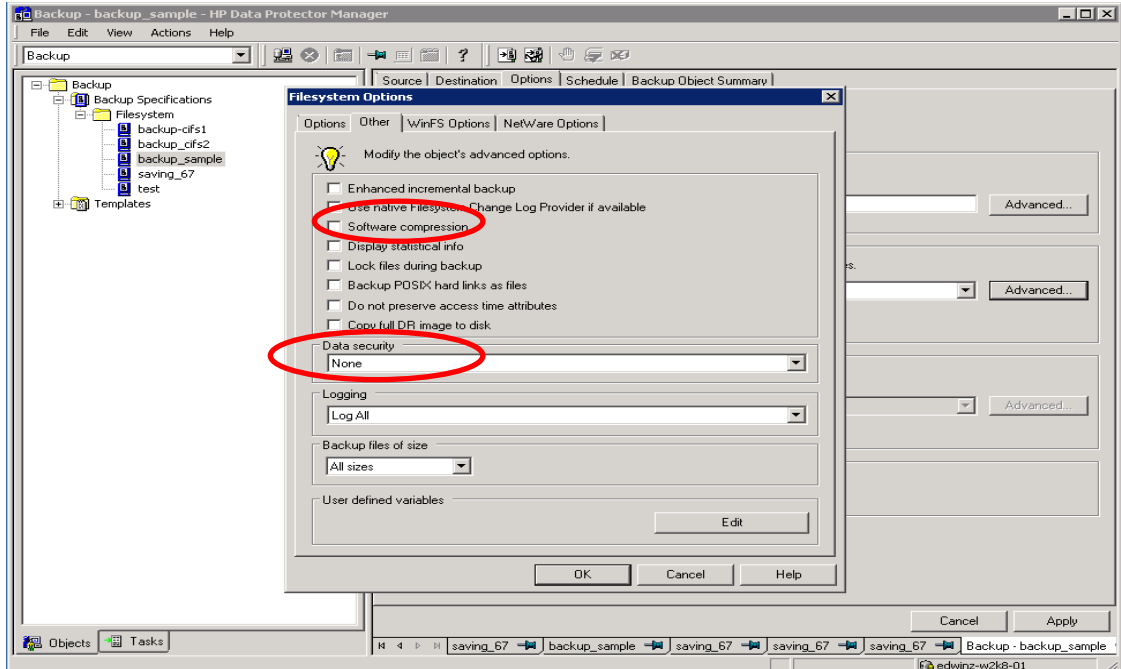
3. Select the devices or drives to be used as the backup target. In this example, it's the DR container share/export created in previous section. Check **Properties** and define other parameters, then click **Next**.



4. Check and verify on **Backup Specification Options** through **Advanced** button. Then in **Filesystem Options** section, click on **Advanced**.



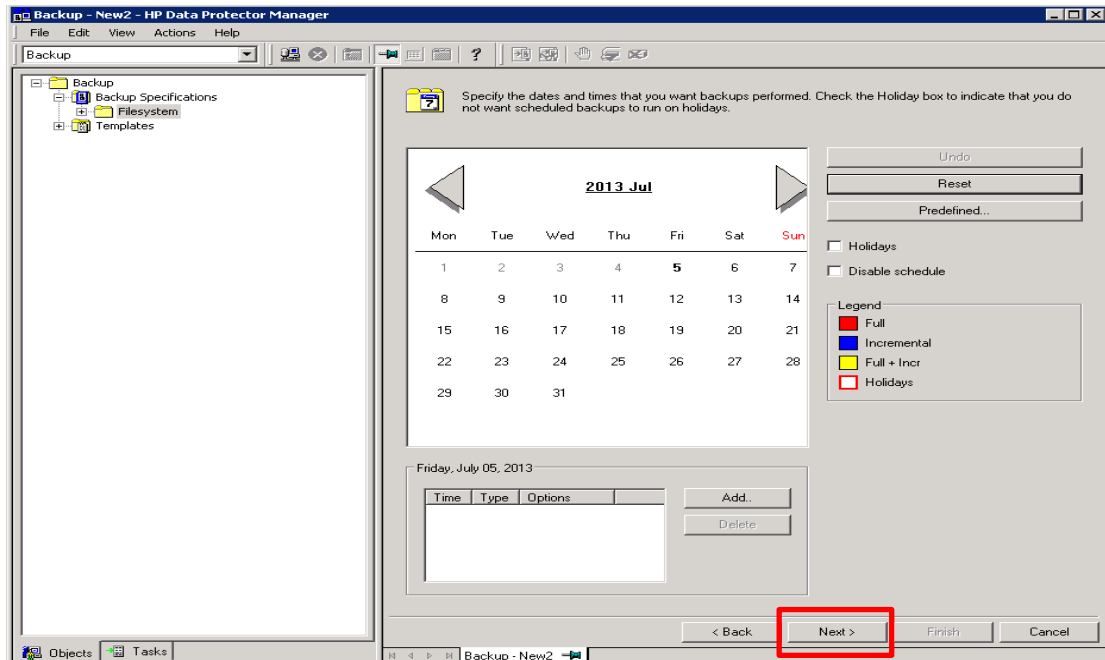
5. In **Filesystem Options**, click **Other** tab, make sure "**Software compression**" is unchecked, and "**Data security**" is set to **None**.



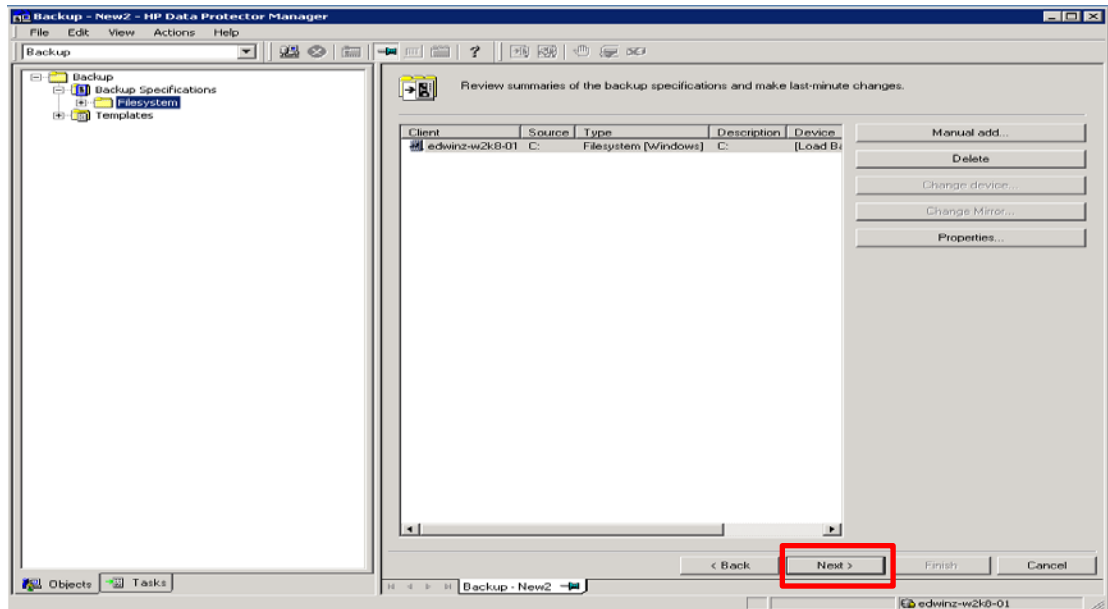
Note: Always Disable **'Software compression'**, as DR Series Deduplication Appliance has compression built in and does not require any compression on HP Data Protector. In general, additional data compression on backup software will have negative impact on total savings on DR Series Deduplication Appliance.

Set **'Data security'** to **None**, as enabling encryption before the data stream is sent to the DR Series Deduplication Appliance device will make the data not deduplicatable. This will put significant negative impact on total savings on DR Series Deduplication Appliance.

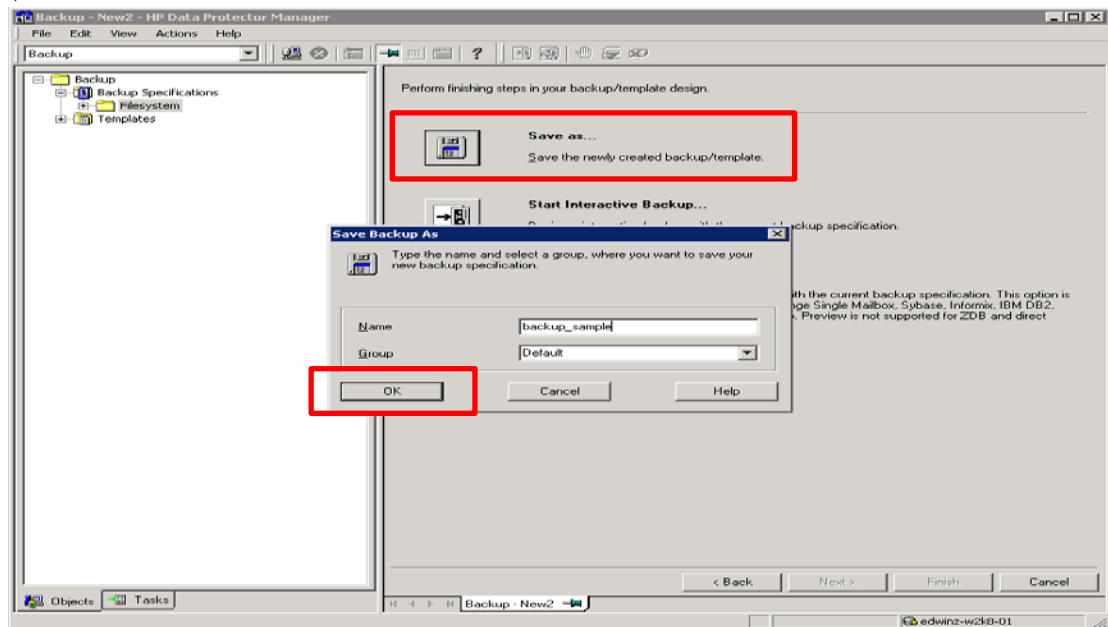
6. Define Backup Job Schedule options and click **Next**.



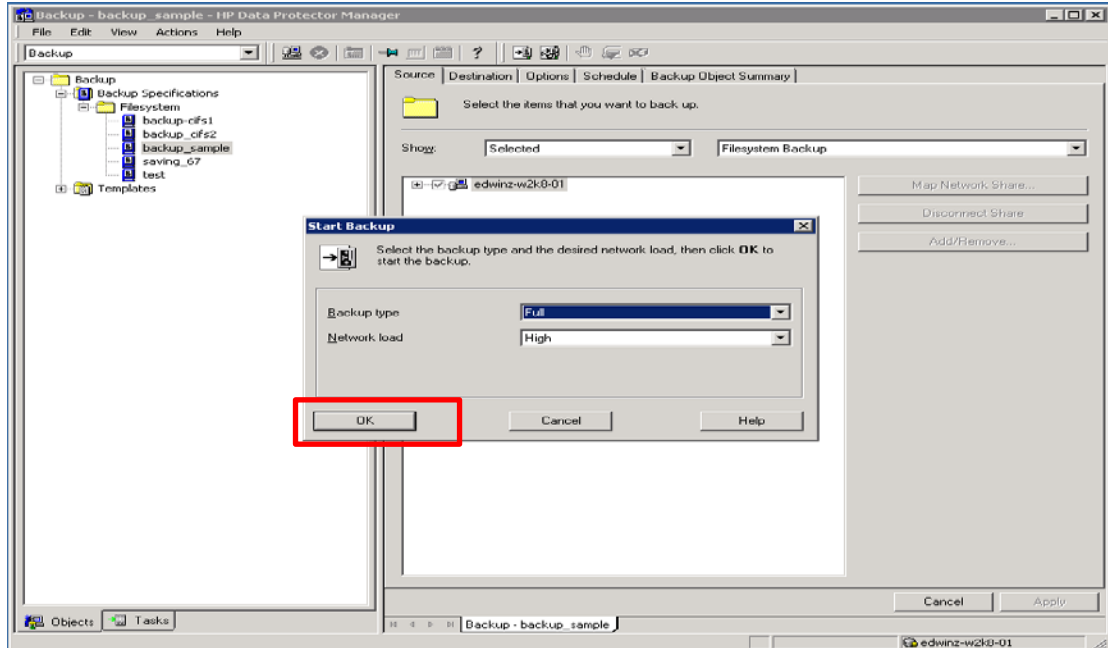
7. Review the Backup Job Summary. Click **Next**.



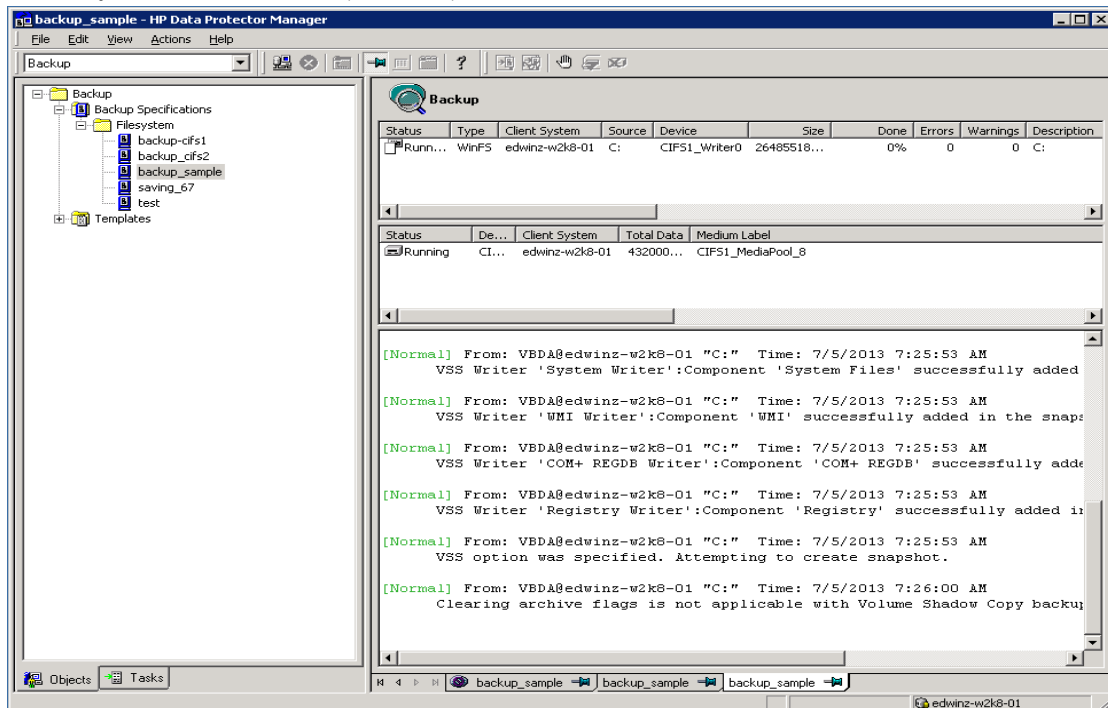
8. Specify a name for the Backup Job. Click **Save As** to save the newly configured backup specification.



- (This step and next are **Optional**: or wait for the scheduled backup run to complete.) Click **Start Backup** to run the backup. When the **Start Backup** window opens, click **OK** to start the backup.



- The **Backup** window displays the progress of the backup session. The Session Information window will tell you when the backup is completed.

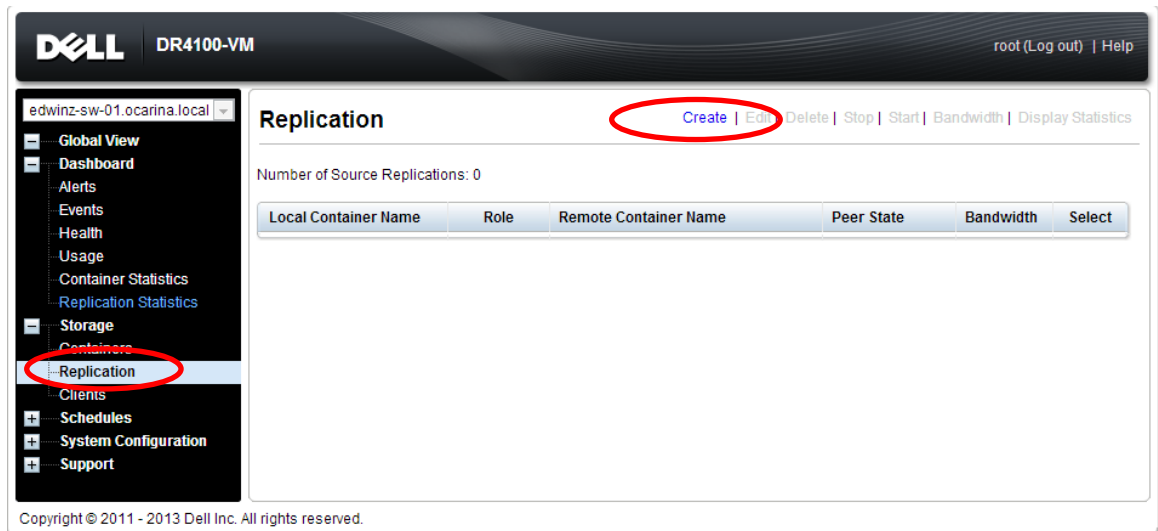


4 Set up DR Native Replication & Restore from Target Container

4.1 Build Replication Relationship between DRs

NOTE: The assumption is that on both the source and target DR, a container is already created for each of them. In this example it's called "backup". And the target container should not be used by anything else and is empty, with the same **Connection Type** as the source container.

11. On the source DR, select **Replication** from the menu panel on the left side of the management interface, click **Create**.



The screenshot shows the Dell DR4100-VM management interface. The top bar displays the Dell logo, the model name 'DR4100-VM', and user information 'root (Log out) | Help'. The left sidebar contains a navigation menu with items: Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Containers, Replication (circled in red), Clients, Schedules, System Configuration, and Support. The main content area is titled 'Replication' and includes a toolbar with buttons: Create (circled in red), Edit, Delete, Stop, Start, Bandwidth, and Display Statistics. Below the toolbar, it states 'Number of Source Replications: 0' and shows an empty table with columns: Local Container Name, Role, Remote Container Name, Peer State, Bandwidth, and Select. The footer contains the copyright notice: 'Copyright © 2011 - 2013 Dell Inc. All rights reserved.'

12. Select a local container as source container in **Step 1**, make appropriate selection in **Step 2** and **Step 3**. In **Step 4**, select **Map to container on remote system**, enter credential to authenticate to Target DR (default is "Administrator/St0r@ge!"), then click **Retrieve Containers**, select the target container on the list, click **Create Replication**.

13. Verify that the replication session is created. **Peer State** is **Online**. Monitor the replication progress under **Replication Statistics**, and make sure the replication **Status** is **INSYNC**.

DR4100-VM

edwinz-sw-01.ocarina.local

Global View | Dashboard | Alerts | Events | Health | Usage | Container Statistics | Replication Statistics | Storage | Containers | Replication | Clients | Schedules | Replication Schedule | Cleaner Schedule | System Configuration | Support

Replication

Create | Edit | Delete | Stop | Start | Bandwidth | Display Statistics

Message

- Successfully added replication for container 'backup'.

Number of Source Replications: 1

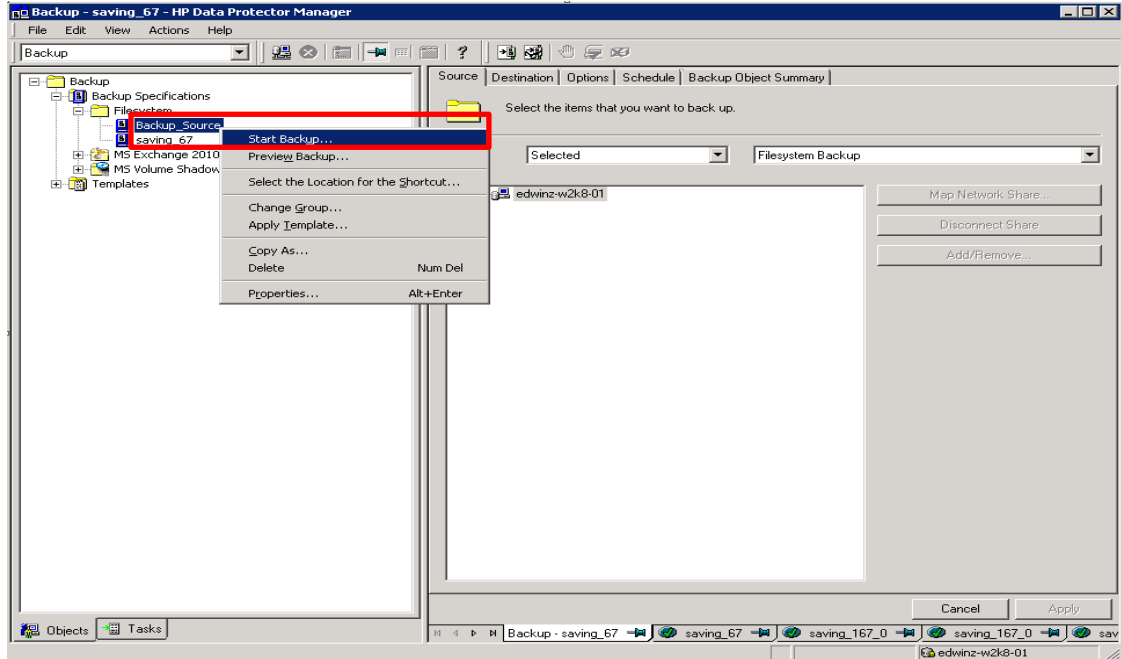
Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
backup	source	10.250.233.67 backup	Online	Default	<input type="radio"/>

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

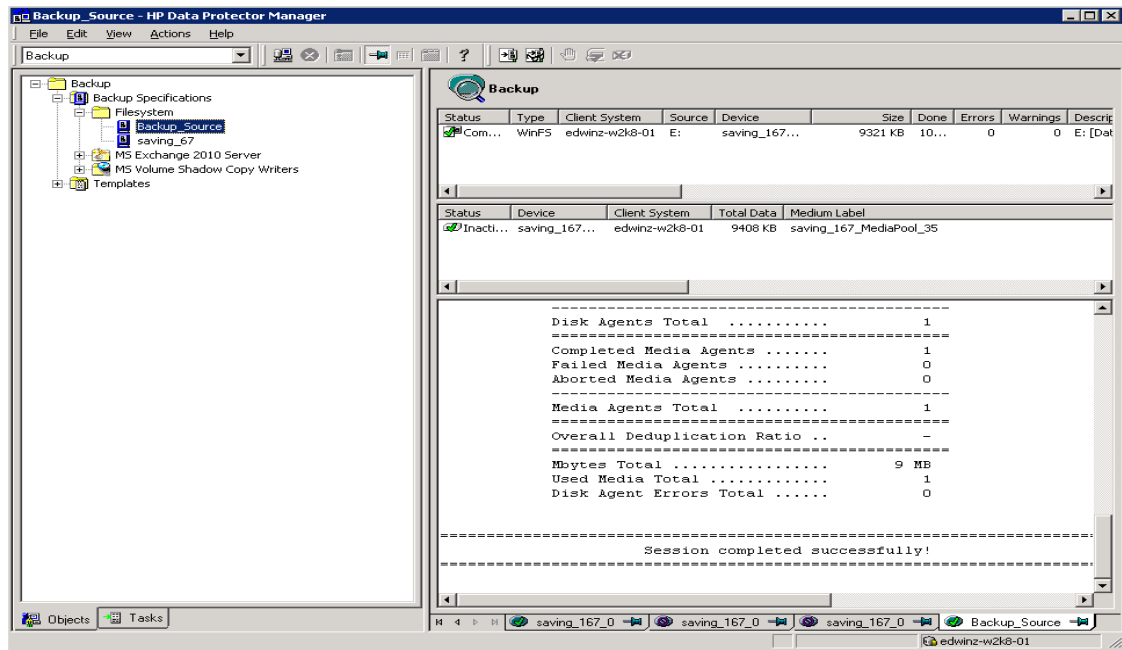


4.2 Run backup to source DR (Optional: only when there is no backup data on the source DR container)

1. Add both source DR and target DR as Devices on HP DP, create a New Backup Job with source DR as the Target.

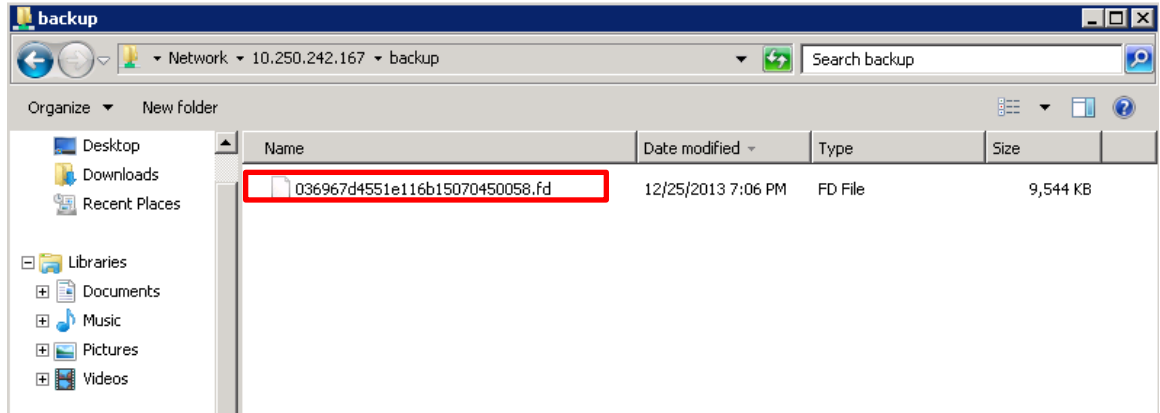


2. In **Start Backup** window, click **OK** to start the backup using the appropriate settings. Monitor job status.

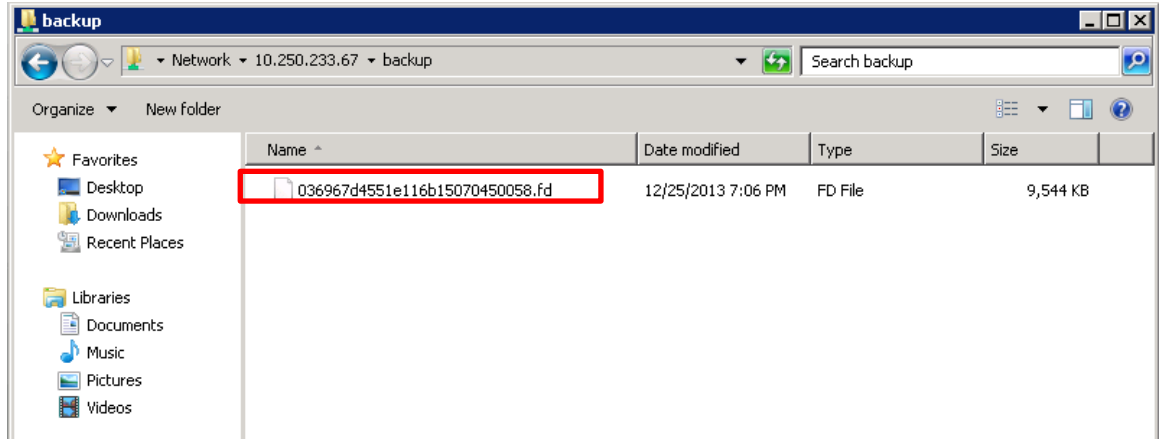


3. When backup job is completed, HP DP creates backup files using the suffix **'.fd'** on source DR , and the **'.fd'** files will be replicated to the target DR, as shown in screenshots.

- Source DR

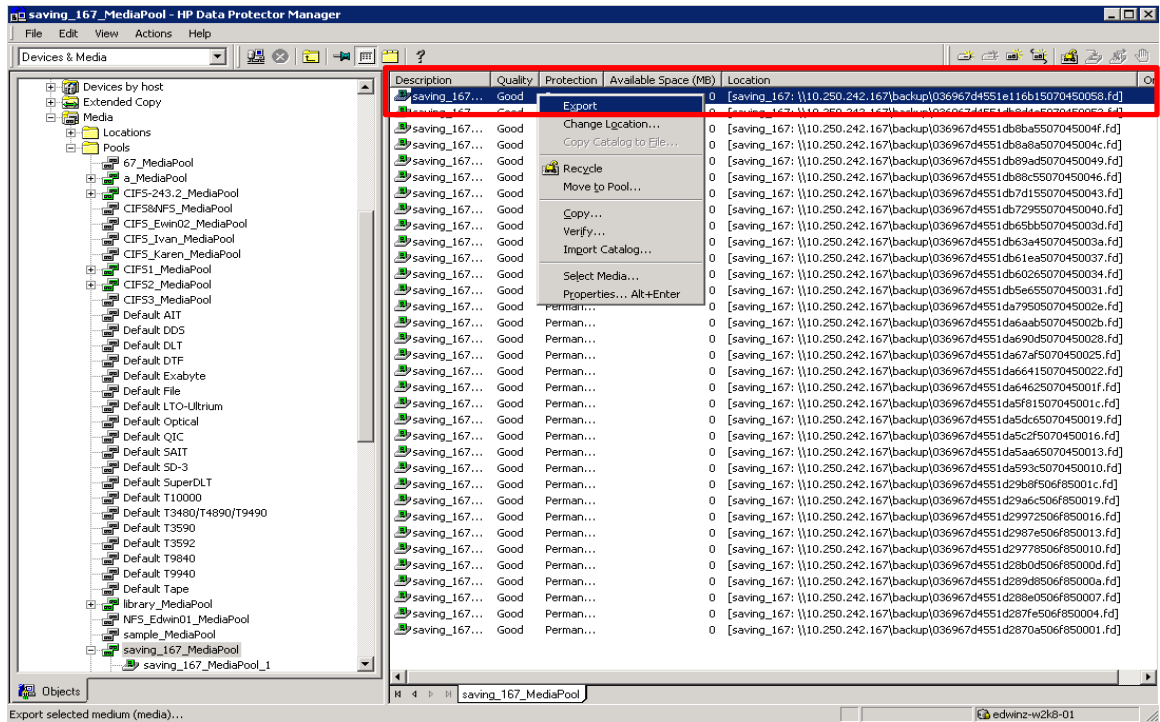


- Target DR



4.3 Prepare Replication Target for restore

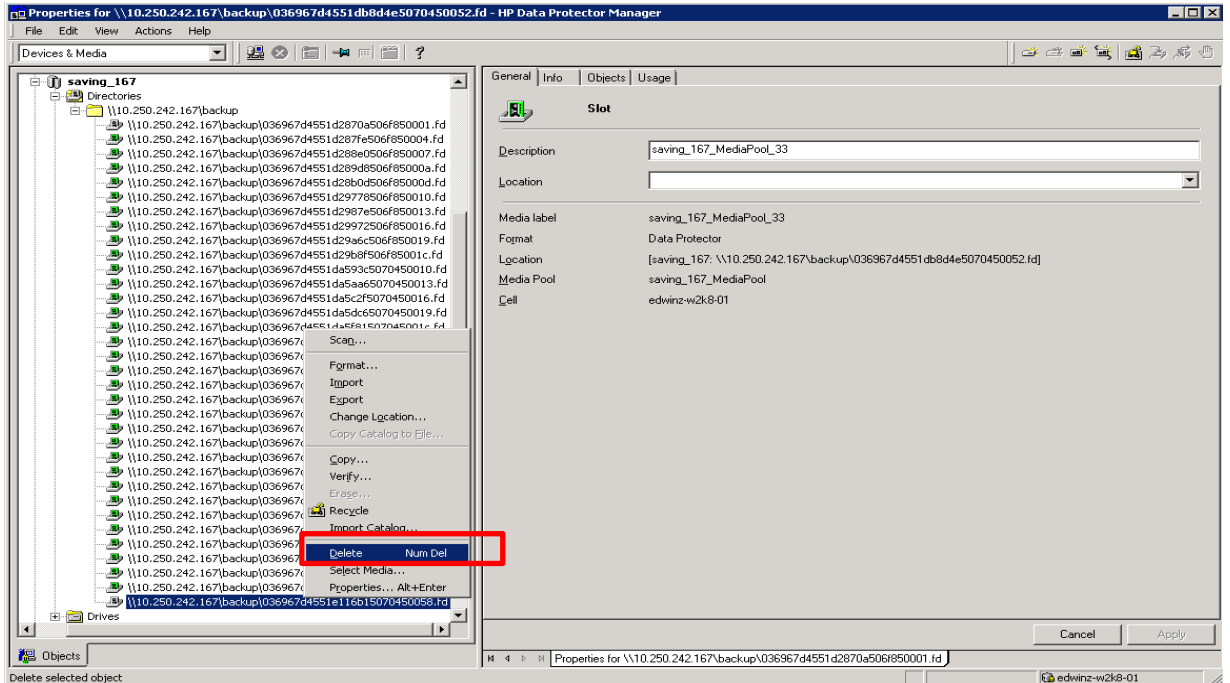
4. On HP DP, Go to **Devices & Media** -> **Media** -> **Pools**, right-click the Media Pool associated with the source container device and the backup set that needs to be restored, click **Export**.



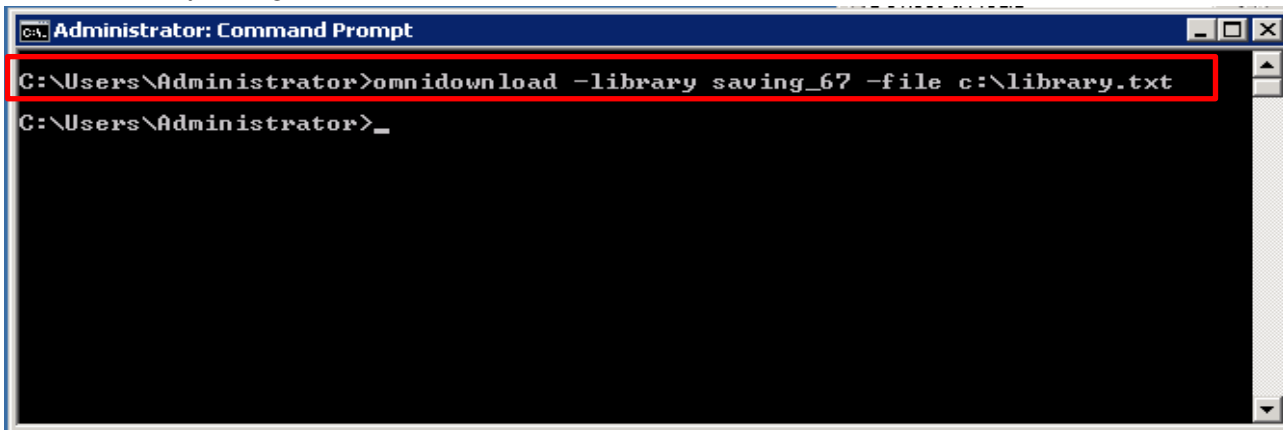
NOTE: If the media pool is protected and cannot be exported, you should perform **Recycle** before **Export**



- Under **Devices & Media** -> **Devices**, expand the source container device node, delete the device object that is associated with the backup set.



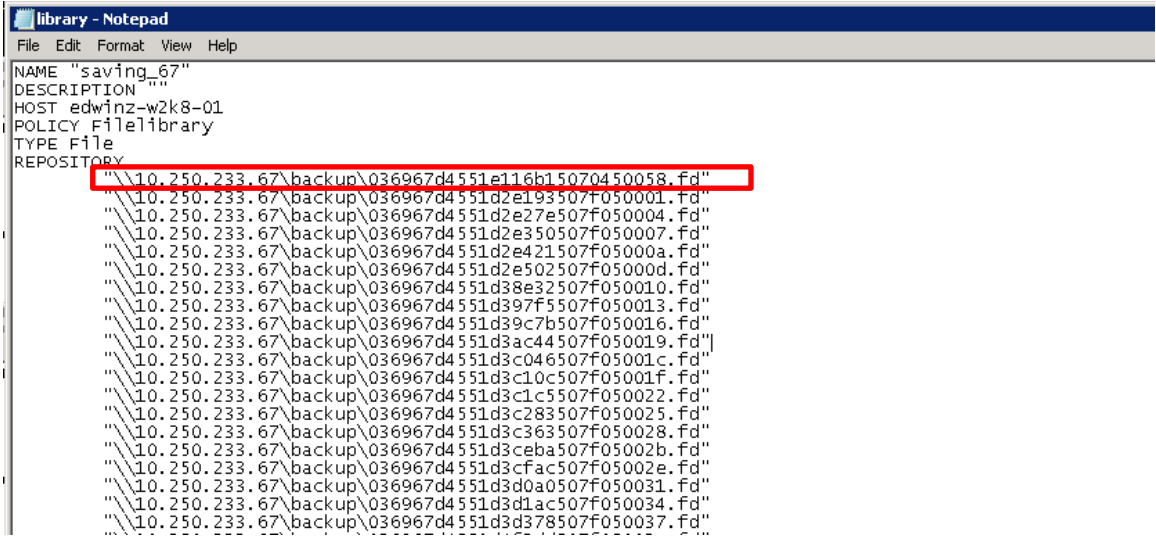
- Open HP DP CLI console, use command utility **"omnidownload"** to download the source container library configuration from IDB



NOTE: Please refer to Appendix C on how to use the command **"omnidownload"**.

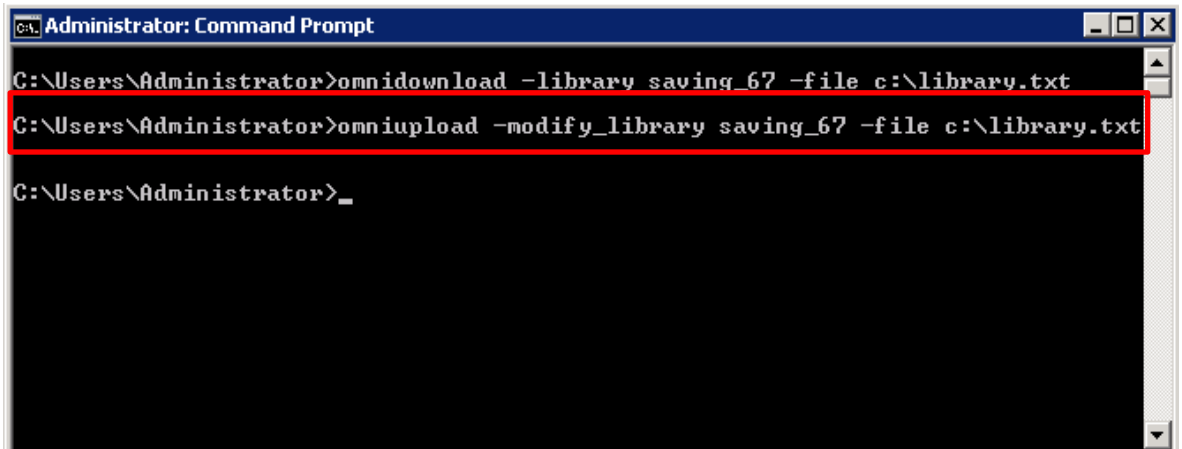


7. Edit the file, modify or add the object information to point to the target DR, save this file



```
library - Notepad
File Edit Format View Help
NAME "saving_67"
DESCRIPTION ""
HOST edwinz-w2k8-01
POLICY FileLibrary
TYPE File
REPOSITORY
""\\10.250.233.67\backup\036967d4551e116b15070450058.fd"
""\\10.250.233.67\backup\036967d4551d2e193507f050001.fd"
""\\10.250.233.67\backup\036967d4551d2e27e507f050004.fd"
""\\10.250.233.67\backup\036967d4551d2e350507f050007.fd"
""\\10.250.233.67\backup\036967d4551d2e421507f05000a.fd"
""\\10.250.233.67\backup\036967d4551d2e502507f05000d.fd"
""\\10.250.233.67\backup\036967d4551d38e32507f050010.fd"
""\\10.250.233.67\backup\036967d4551d397f5507f050013.fd"
""\\10.250.233.67\backup\036967d4551d39c7b507f050016.fd"
""\\10.250.233.67\backup\036967d4551d3ac44507f050019.fd"
""\\10.250.233.67\backup\036967d4551d3c046507f05001c.fd"
""\\10.250.233.67\backup\036967d4551d3c10c507f05001f.fd"
""\\10.250.233.67\backup\036967d4551d3c1c5507f050022.fd"
""\\10.250.233.67\backup\036967d4551d3c283507f050025.fd"
""\\10.250.233.67\backup\036967d4551d3c363507f050028.fd"
""\\10.250.233.67\backup\036967d4551d3ceba507f05002b.fd"
""\\10.250.233.67\backup\036967d4551d3cfac507f05002e.fd"
""\\10.250.233.67\backup\036967d4551d3d0a0507f050031.fd"
""\\10.250.233.67\backup\036967d4551d3d1ac507f050034.fd"
""\\10.250.233.67\backup\036967d4551d3d378507f050037.fd"
```

8. Upload this modified configuration file to IDB using the command "omniupload".

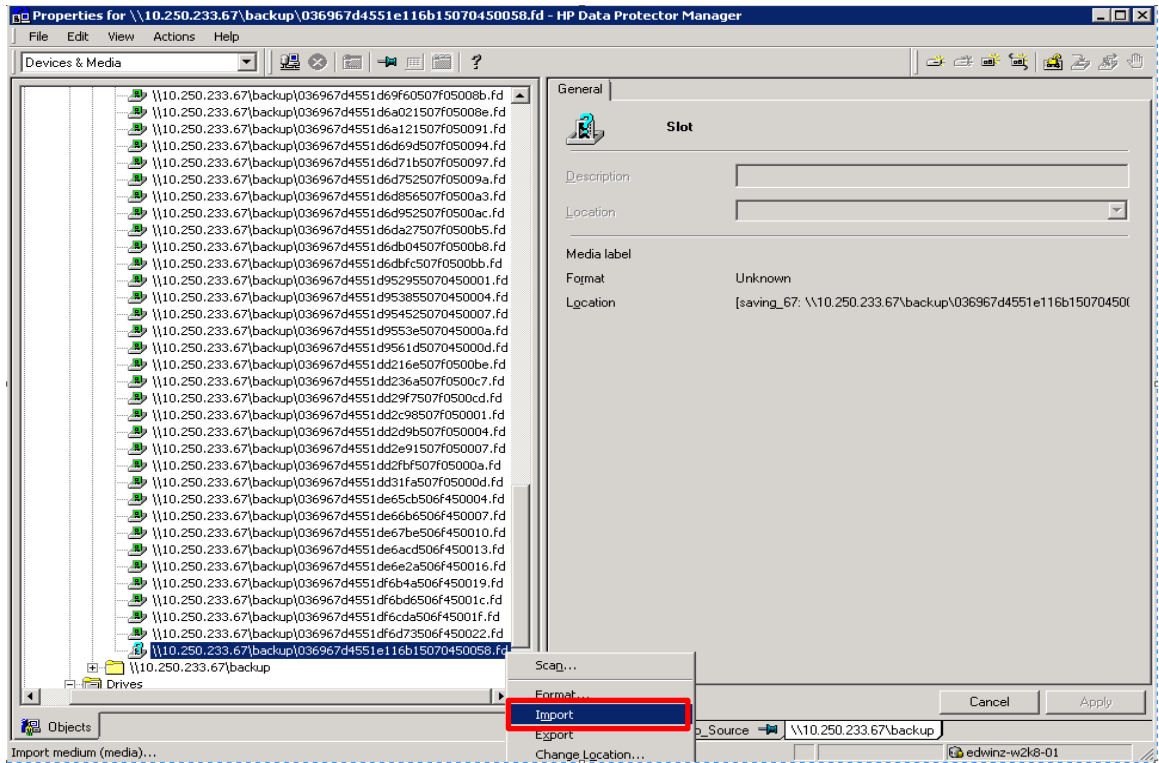


```
Administrator: Command Prompt
C:\Users\Administrator>omnidownload -library saving_67 -file c:\library.txt
C:\Users\Administrator>omniupload -modify_library saving_67 -file c:\library.txt
C:\Users\Administrator>_
```

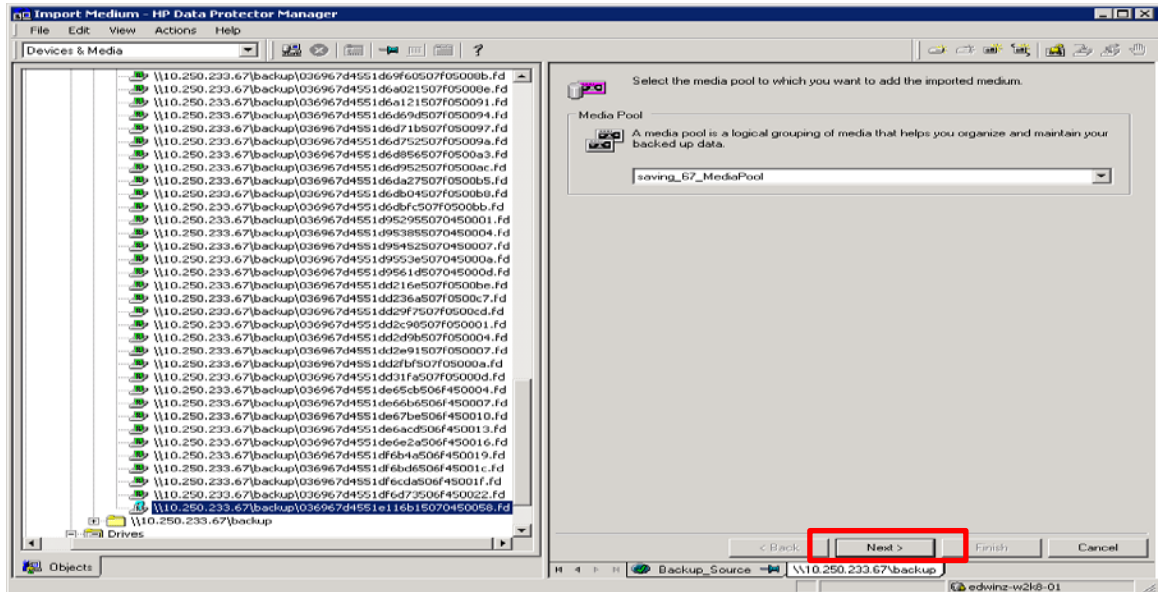
NOTE: Please refer to Appendix C on how to use the command "omniupload"



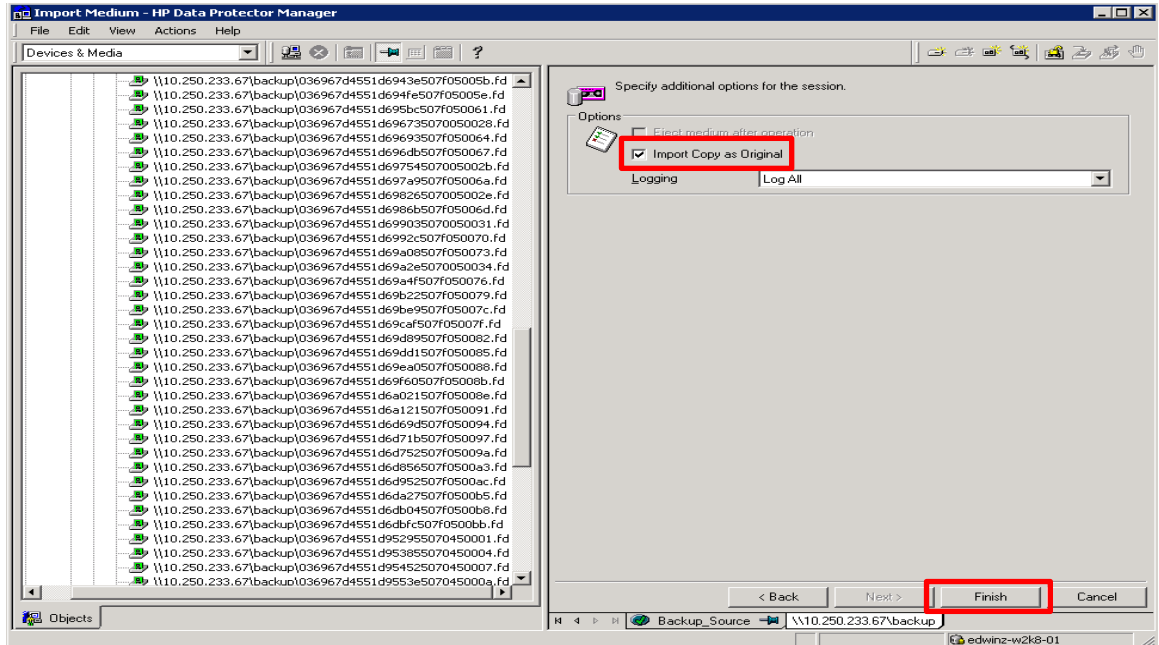
9. Expand the device node, **Import** the device object from target device



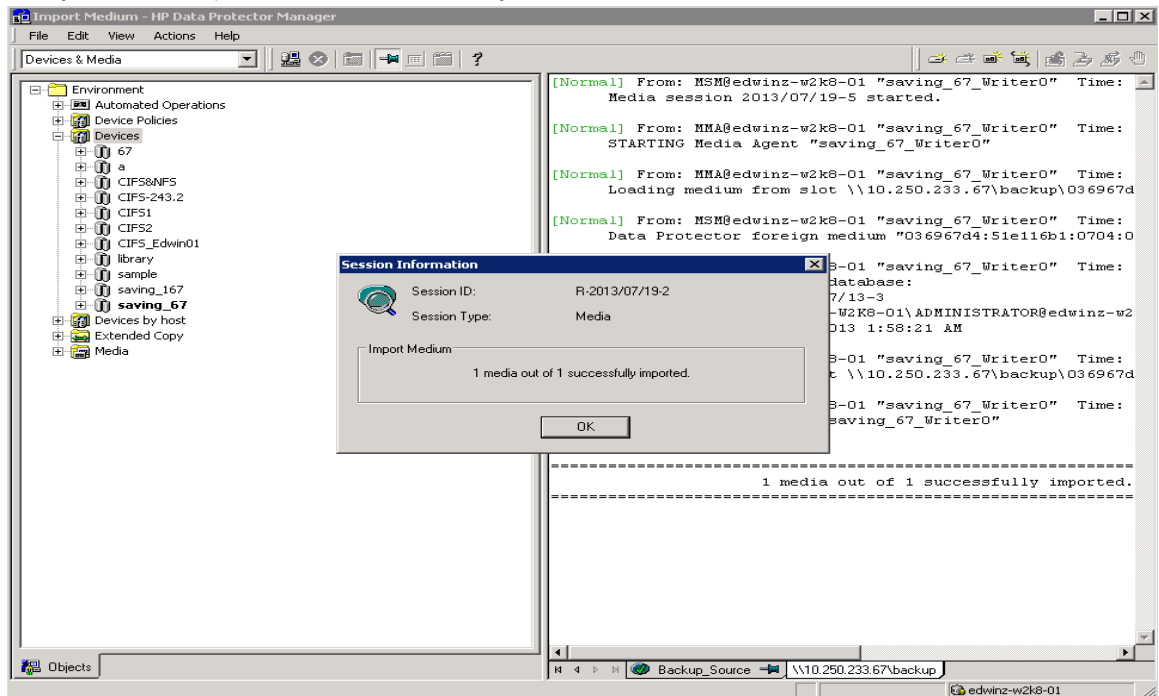
10. Click **Next**.



11. Check **Import Copy as Original**, click **Finish**.

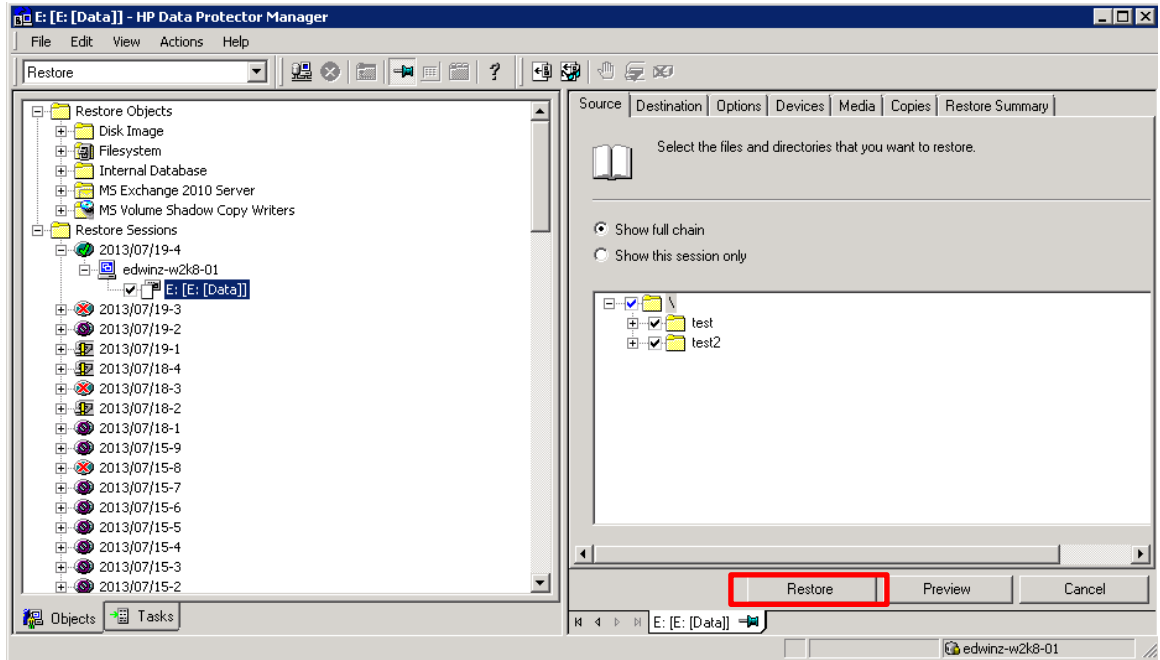


12. Verify that the import is done successfully.

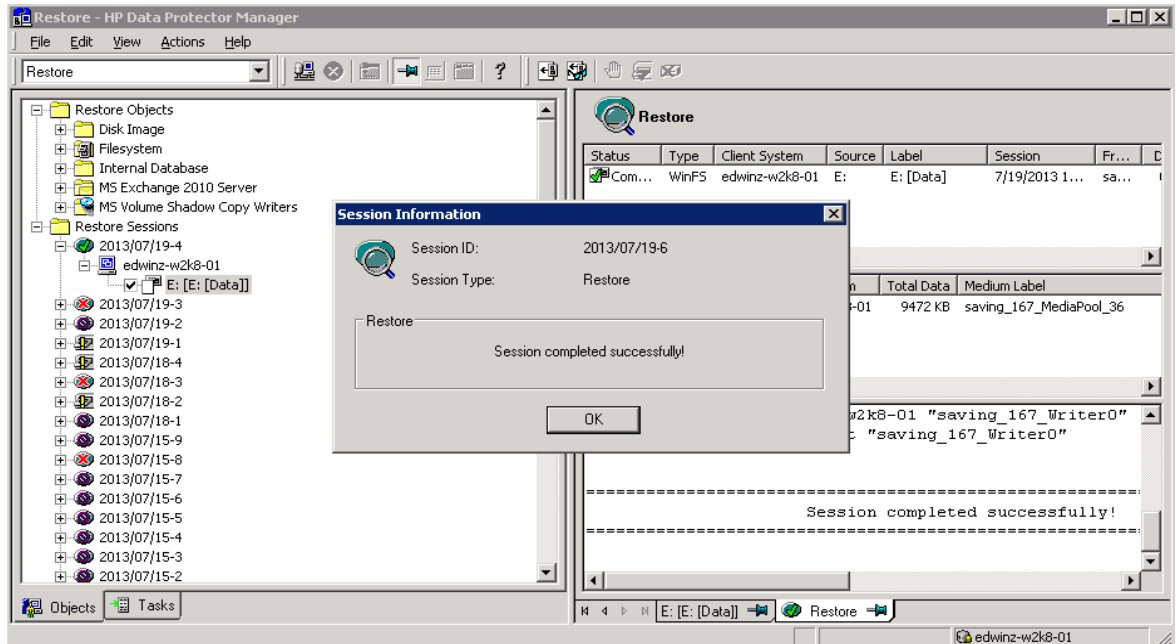


4.4 Restore from target DR

13. In **Context List** drop-down menu, choose **Restore**. Run the restore session that is associated to the backup set, click **Restore**.



14. Verify that the restore is done successfully.



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 DR4100 web interface. The header includes the Dell logo, system ID 'DR4100 EdwinZ-SW-01', and 'Help | Log out' links. The left navigation menu has 'Cleaner Schedule' highlighted. The main content area is titled 'Cleaner Schedule' and 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 shows a schedule for Sunday through Saturday, with all start and stop times currently set to '--'. A red arrow points to the 'Edit Schedule' button in the top right corner.

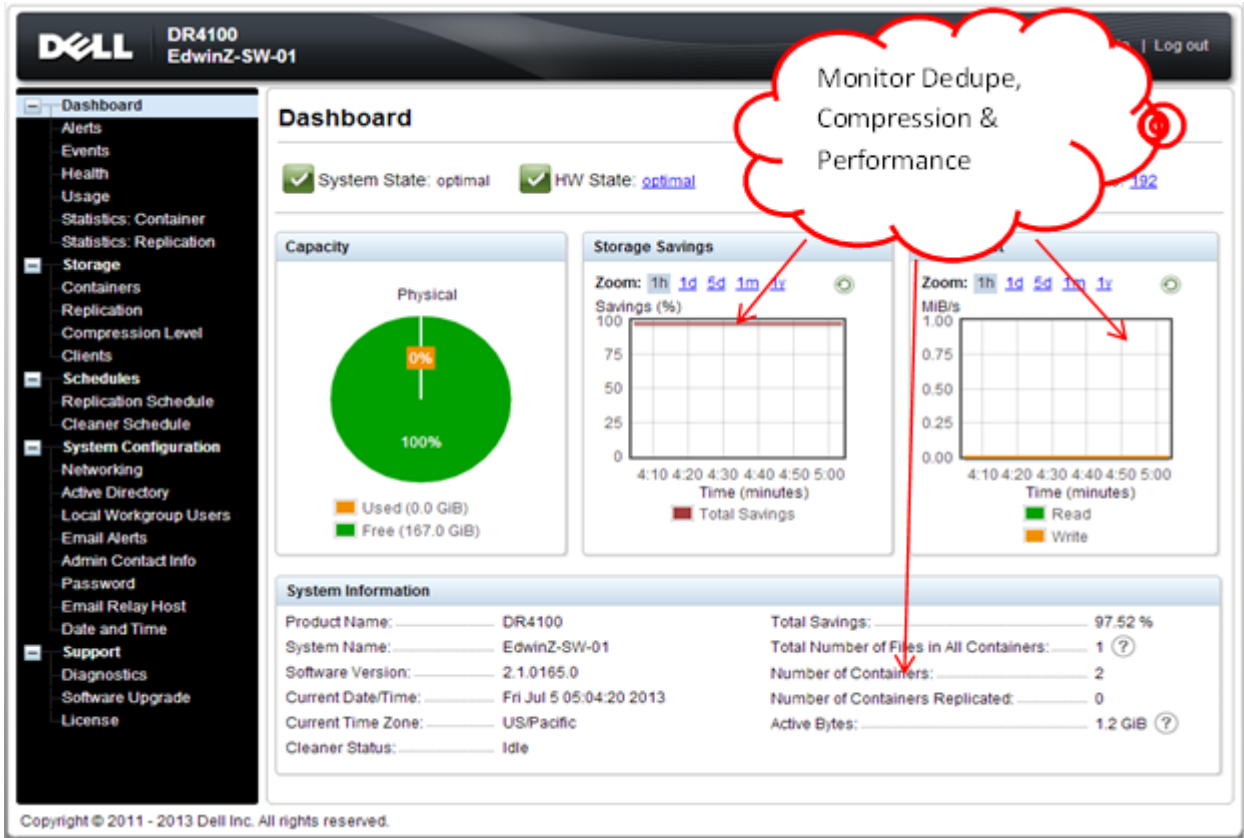
Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--



6 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.



7 Appendix

7.1 Create a Storage Device for CIFS

There are two options for HP Data Protector to authenticate to DR Series Deduplication Appliance through CIFS.

1. **DR joined into domain:** Integrate HP Data Protector 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 HP Data Protector service to run with this AD user <Domain\User>

2. **DR is standalone CIFS server:** Make sure HP Data Protector Inet service and CRS service use the same Log On user. DR Series Deduplication Appliance also has the same username and password defined in Local Workgroup Users.

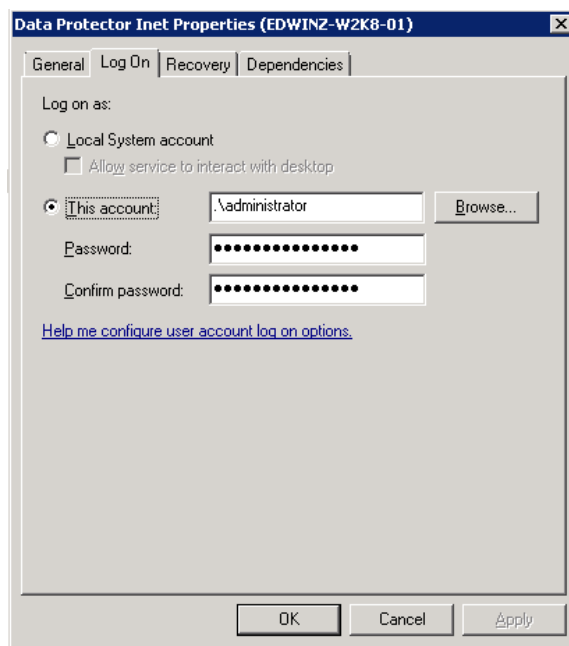
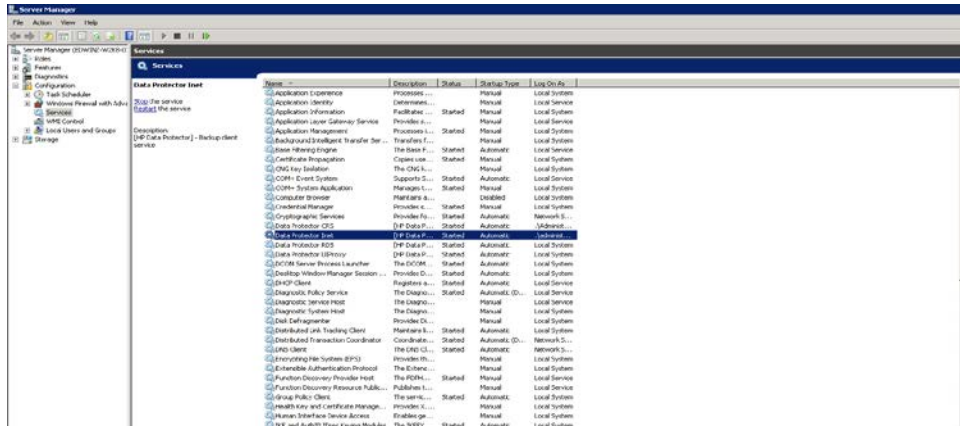
Also make sure this CIFS user has appropriate access permission to the DR Series Deduplication Appliance container share. HP Data Protector services will use this user to authenticate to DR Series Deduplication Appliance share in Workgroup mode.

 - 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 HP Data Protector service account to use the CIFS administrator account.

- b. Launch Microsoft Services Snap-in by clicking **Start > Run > Services.msc > Enter**.
- c. Locate the Data Protector Inet and Data Protector CRS Service. 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 synced accounts rather than the AD account, make sure that there is a "." in front of the user name. [move this before the step – that's when the user needs this info]

- d. Click **OK**.
- e. After changing both services for HP Data Protector, choose **Stop/Start** to restart the two services.



7.2 Create a Storage Device for NFS

For NFS backup using the HP Data Protector, a target folder needs to be created as NFS share directory. This is the location to which backup objects will be written. This is not required while adding CIFS share.

1. Mount the DR Series Deduplication Appliance NFS share onto the NFS share directory which backup objects will be written in the HP Data Protector environment.
2. Verify the NFS share. One way is to try using the Linux command "cat /proc/mounts". The rsize and wsize of the nfs mount should be 512K.

7.3 User commands

1. Omnidownload

- Downloads information about a backup device and a library from the Data Protector internal Database (IDB).
- This command is available on systems with the Data Protector User Interface component installed.

Examples:

To review the information about a virtual tape library named "VTL" in ASCII format that will be saved as the file "libVTL.txt" to the directory "C:\Temp", run:

```
omnidownload -library VTL -file C:\Temp\libVTL.txt
```

2. Omniupload

- Uploads information about a backup device from an ASCII file to the Data Protector internal database(IDB).
- This command is available on systems with the Data Protector User Interface component installed.

Examples

To modify library"Exabyte1" using the information in the file "/tmp/EXA", run:

```
omniupload -modify_library Exabyte1 -file /tmp/EXA
```

