Setting up the Dell™ DR Series System on Symantec™ NetBackup™

Dell Engineering
July 2015

A Dell Technical White Paper

Revisions

Date	Description
February 2014	Initial release
July 2015	Added content about creating and configuring NDMP target container(s) for NetBackup. Consolidated content for the various container types and updated cleaner recommendation.

This document 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.

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. Symantec™ and NetBackup™ are trademarks owned by Symantec Corporation or its affiliates in the U.S. 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

This paper provides information about how to set up the Dell DR Series system as:

- A CIFS or NFS backup target for Symantec NetBackup
- An OST backup target for Symantec NetBackup
- A VTL backup target for Symantec NetBackup

This document 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 Symantec NetBackup build versions and screenshots used for this paper may vary slightly, depending on the version of the system software you are using.

1 Installing and configuring the DR Series system for use with Symantec NetBackup

1.1 Symantec NetBackup prerequisites

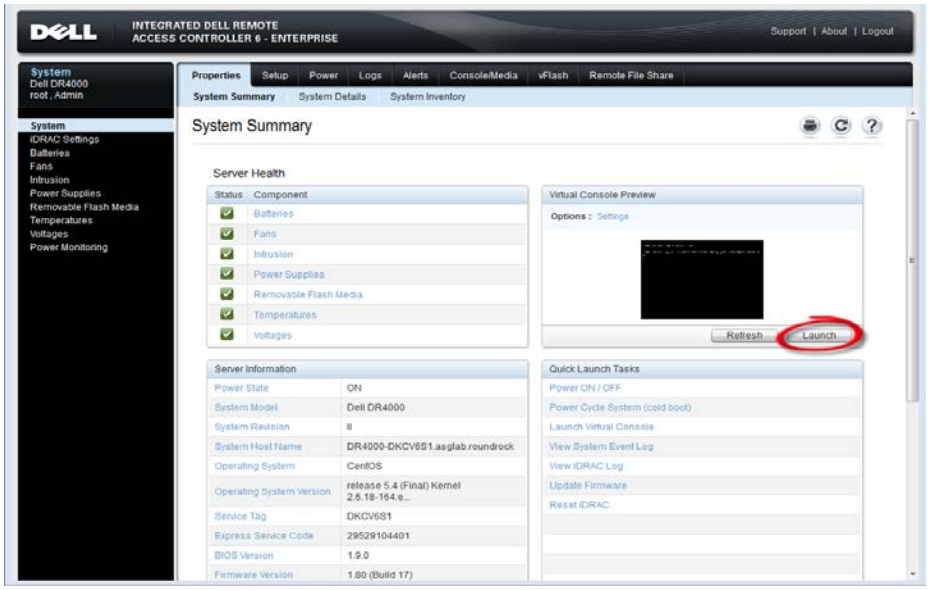
The instructions in this document apply to Symantec NetBackup version 8.1 and later.

1.2 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. In the *Dell DR Series System Administrator Guide*, refer to the following topics for more information about initializing the system: "iDRAC Connection," "Logging in and Initializing the DR Series System," and "Accessing iDRAC6/iDRAC7 Using RACADM".

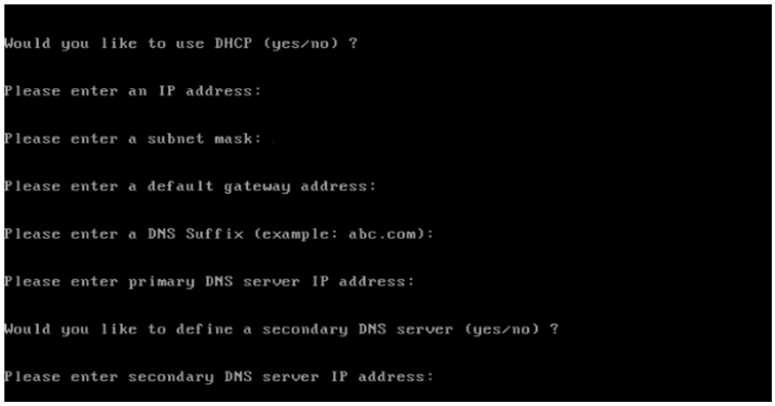
3. Log on to iDRAC with the default IP address **192.168.0.120**, or the IP address that is assigned to the iDRAC interface. Use the username and password: "**root/calvin**".



4. Launch the virtual console.

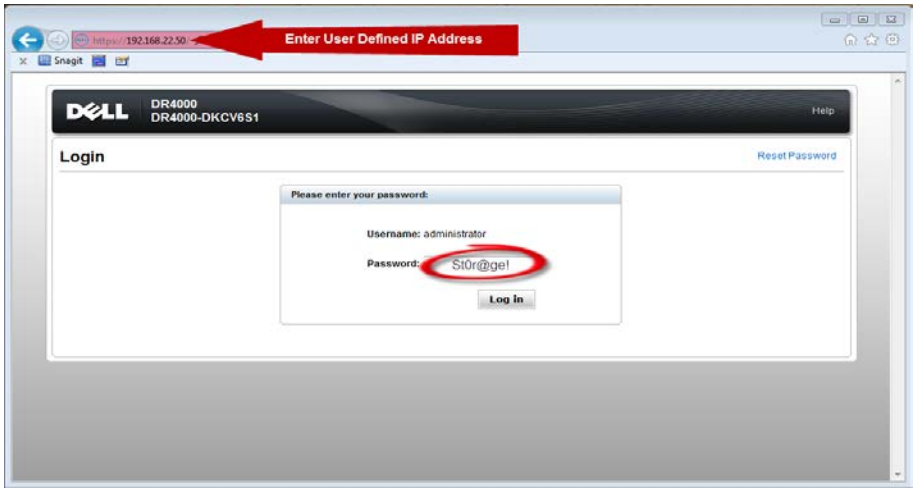
5. After the virtual console is open, log on to the system with the username **administrator** and password **St0r@ge!** (the "0" in the password is the numeral zero).

6. Set the user-defined networking preferences.



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

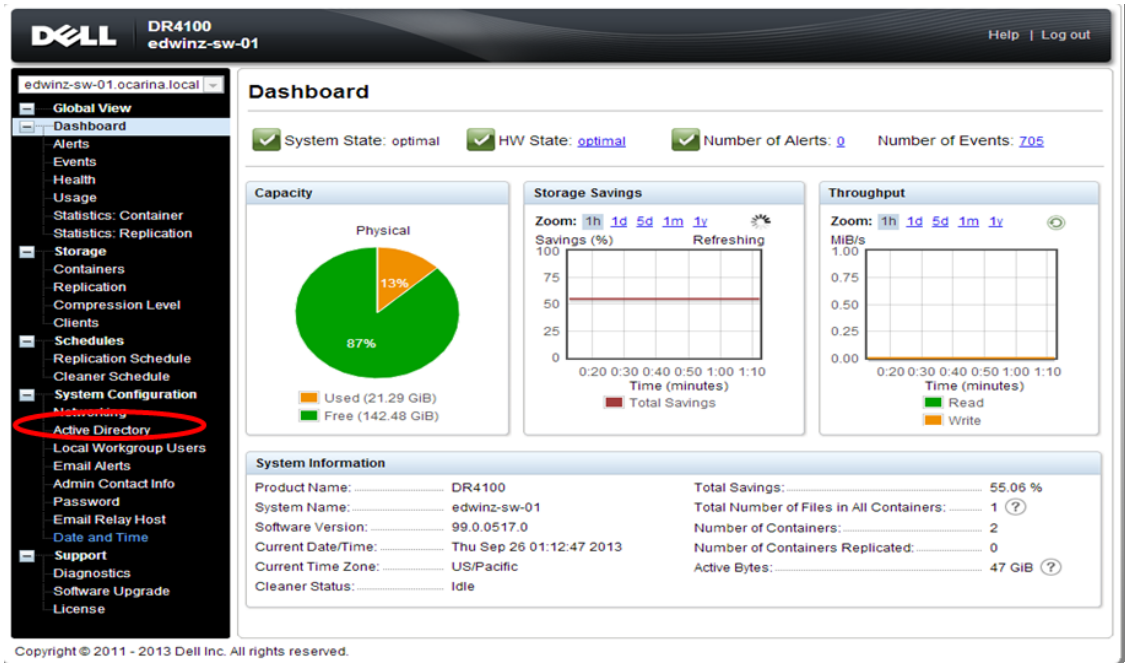
8. Log on to the DR Series system administrator console using the IP address you just provided for the DR Series system, the username **administrator,** and the password **St0r@ge!** (the "0" in the password is the numeral zero).



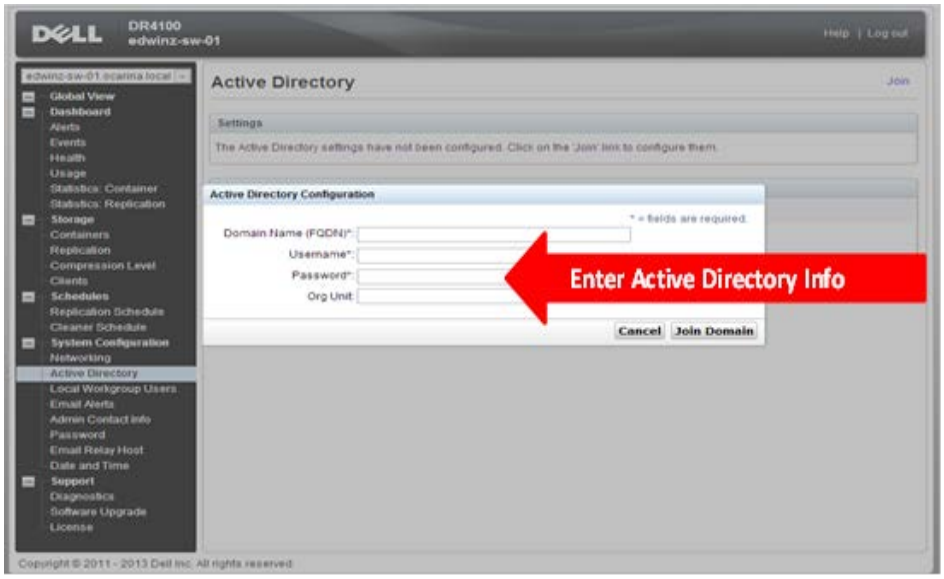
9. Join the DR Series system to Active Directory.

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 logon instructions.

a. Select **Active Directory** from left navigation area of the DR Series system GUI.

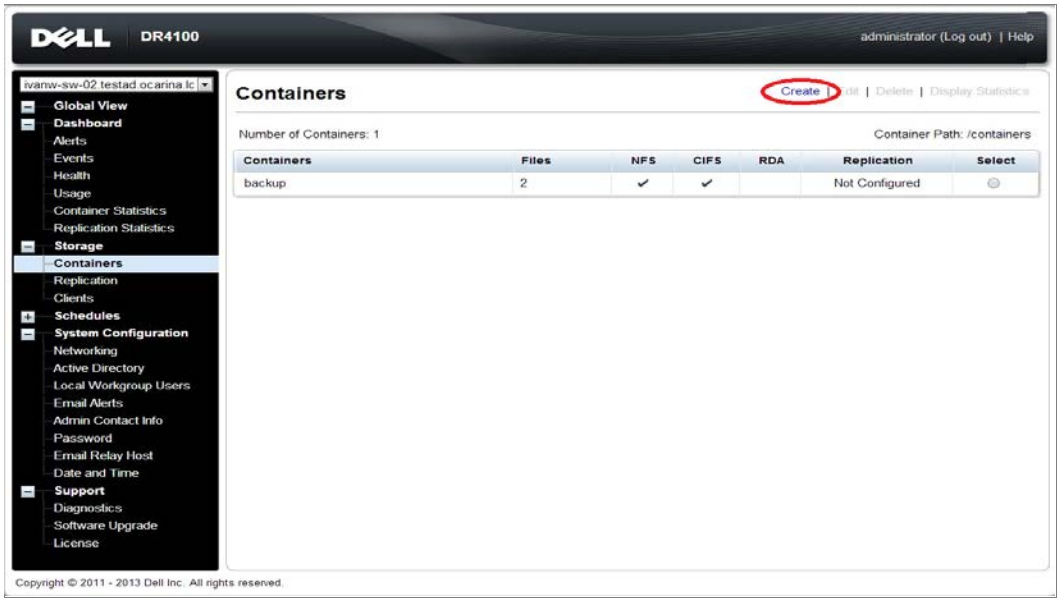


b. Enter your Active Directory credentials.



2 Configuring a CIFS or NFS target container

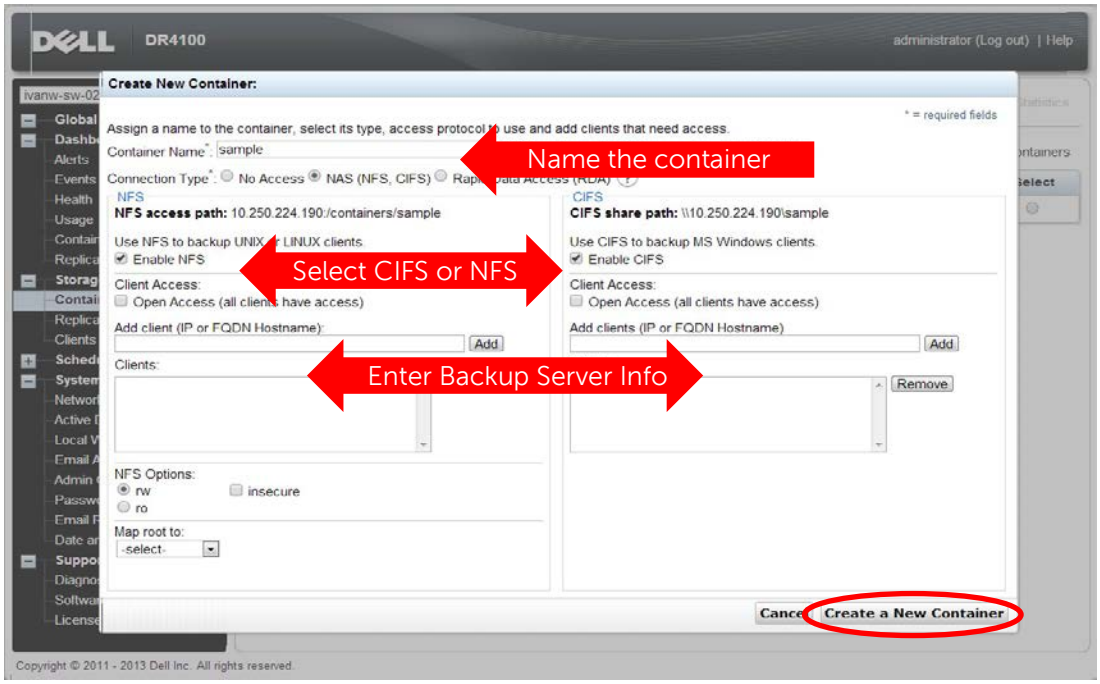
1. Create and mount a CIFS container by selecting **Containers** in left navigation area of the DR Series system GUI, and then clicking **Create** at the top of the page.



2. Enter a **Container Name**, select **Enable CIFS** or **Enable NFS** check box as needed.

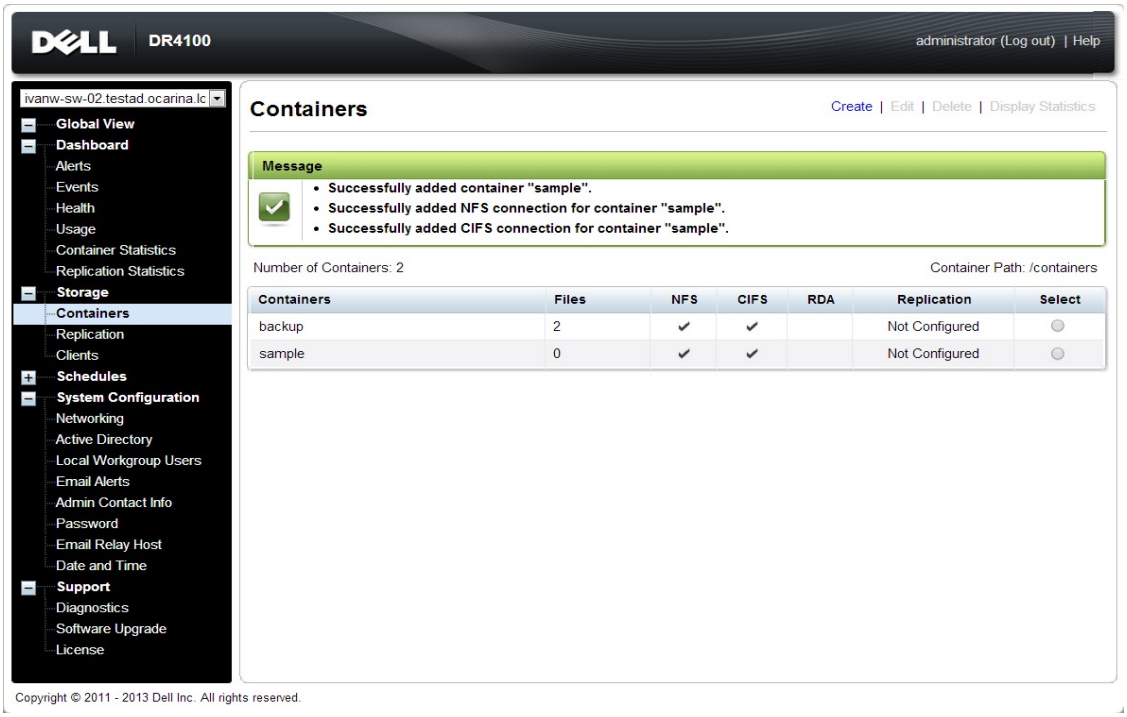
NOTE: Symantec NetBackup supports both CIFS and NFS protocols.

3. Select the preferred client access credentials and then click **Create a New Container**.

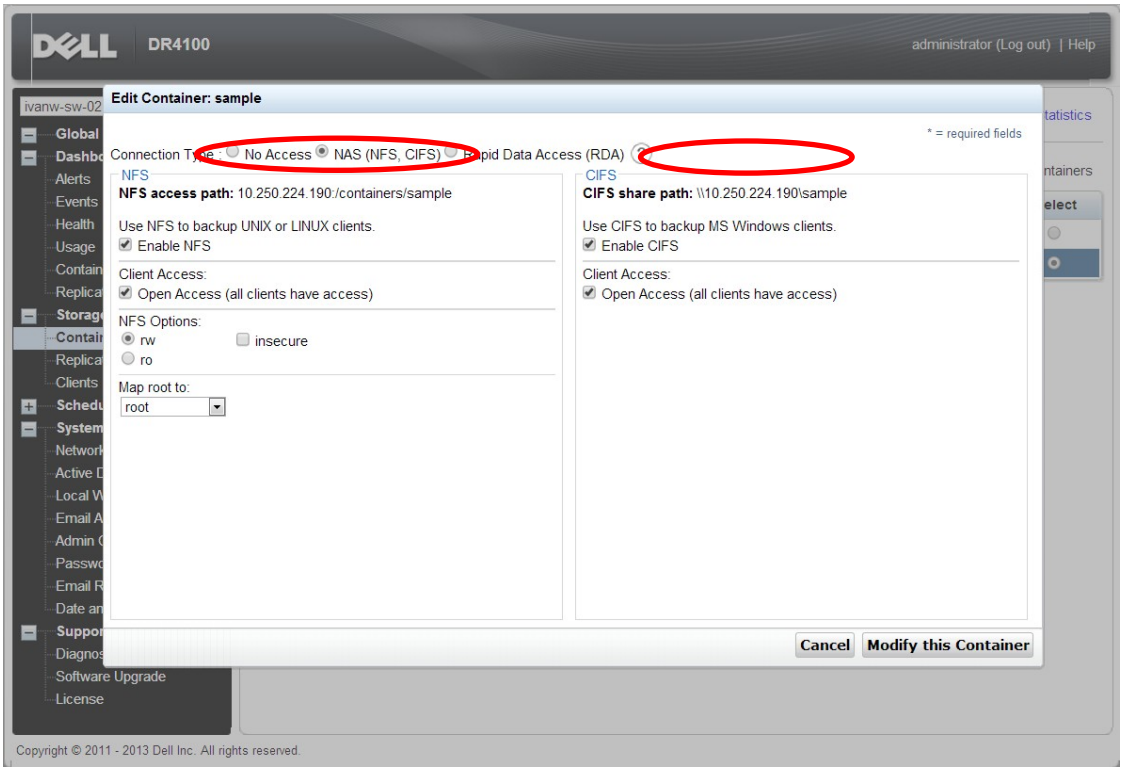


Note: For improved security, Dell recommends adding IP addresses for the following (Not all environments will have all components): Backup console (NetBackup Master Server, Media Server)

4. Confirm that the container is added.

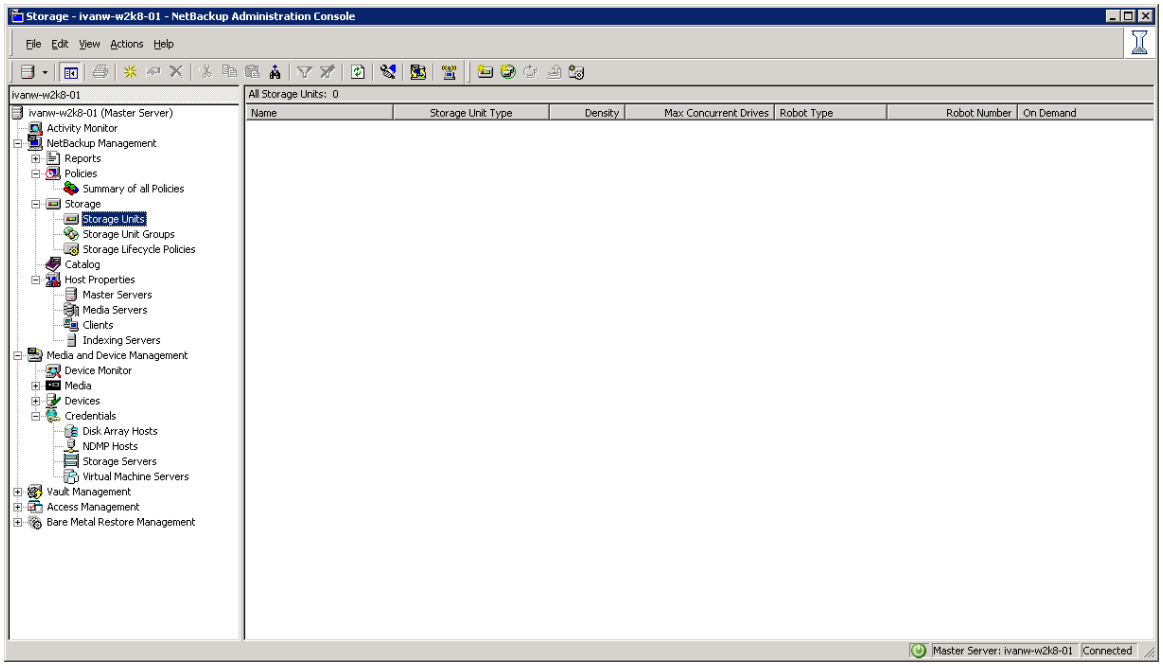


5. Click **Edit.** Note down the container share/export path, which you will use later to target the DR Series system.

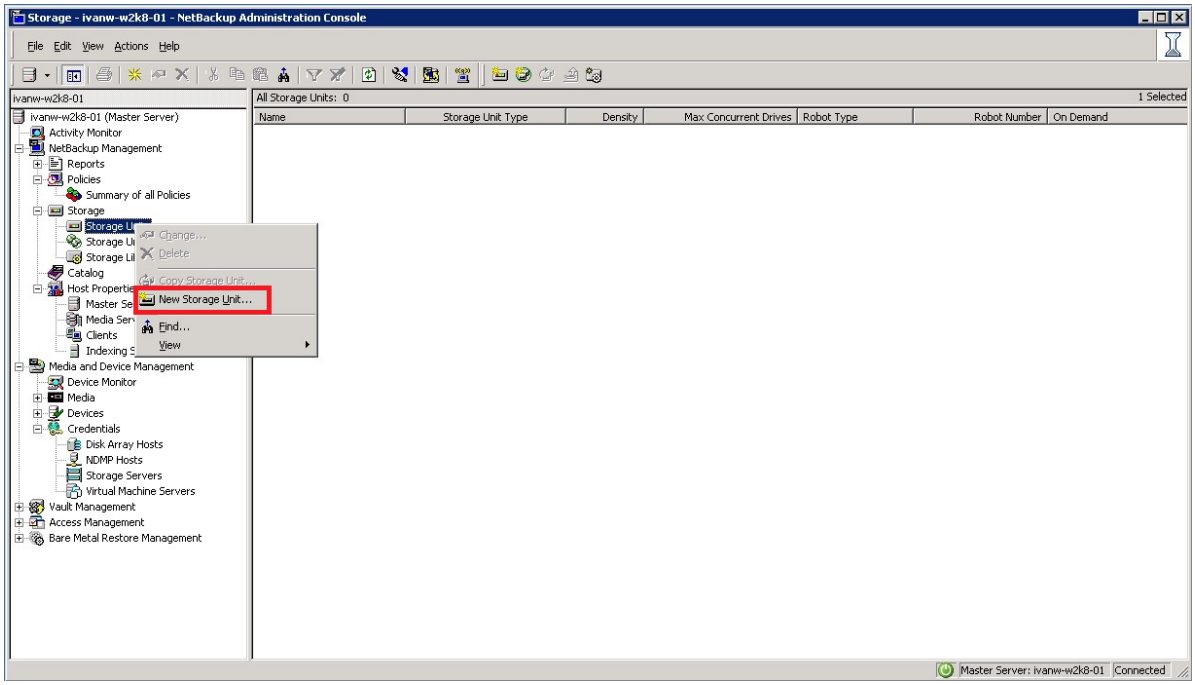


2.1 Setting up Symantec NetBackup storage units - Windows

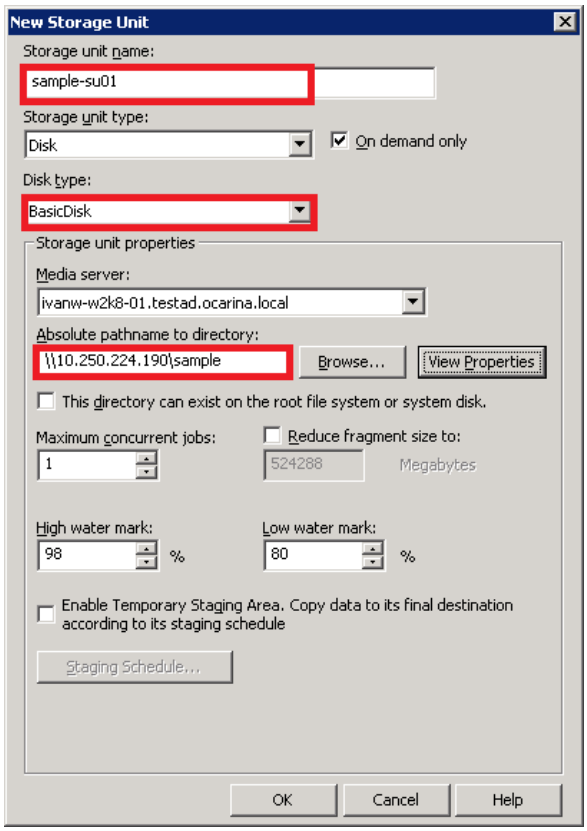
6. Open the NetBackup Administration Console, and then expand **Storage**, which displays the **Storage Units** section.



7. Right-click **Storage Units** and then click **New Storage Unit**.

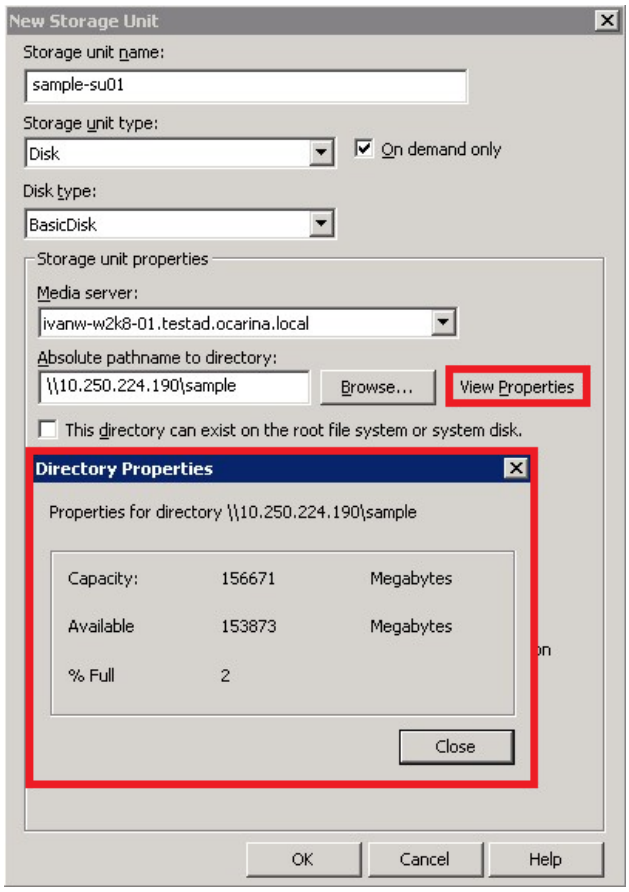


8. In the New Storage Unit window, enter the **Storage unit name** and select **BasicDisk** for the **Disk Type**.
9. Enter the **Absolute pathname to directory** (the UNC path to the DR Series system container share) and click **OK**.

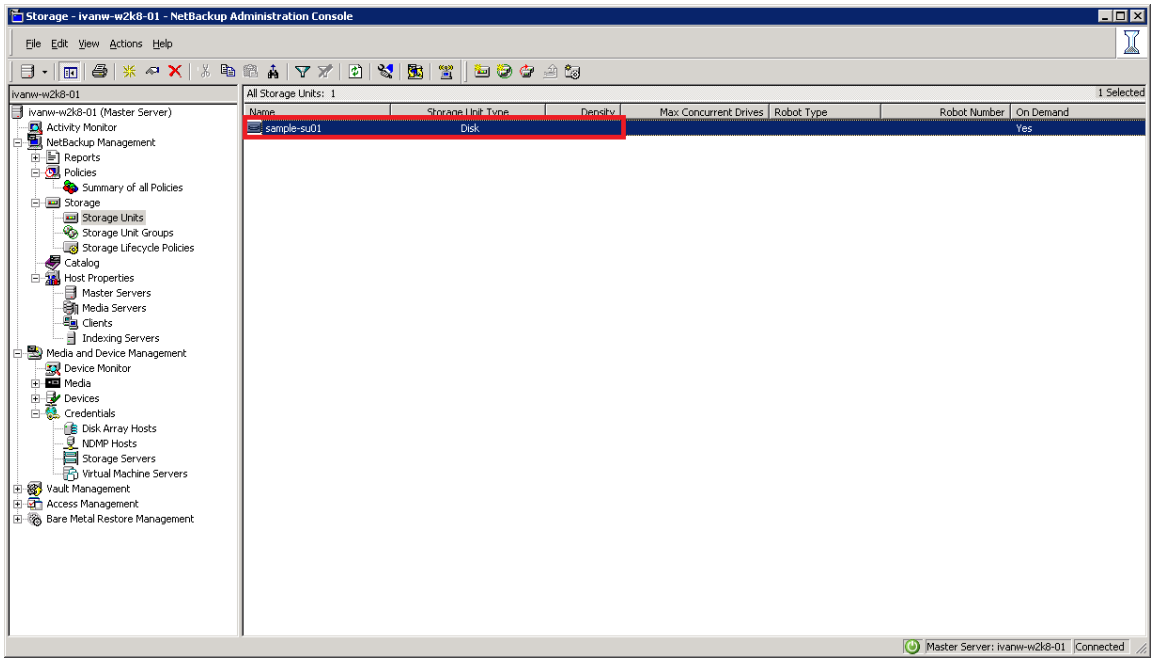


Note: The Windows service account for Symantec NetBackup requires appropriate permissions to the DR Series system CIFS Share for the step below to complete successfully. See **Appendix A** for information about setting up the Symantec NetBackup service account correctly. This should be done before the next step.

10. Click **View Properties** to view the **Directory Properties.**



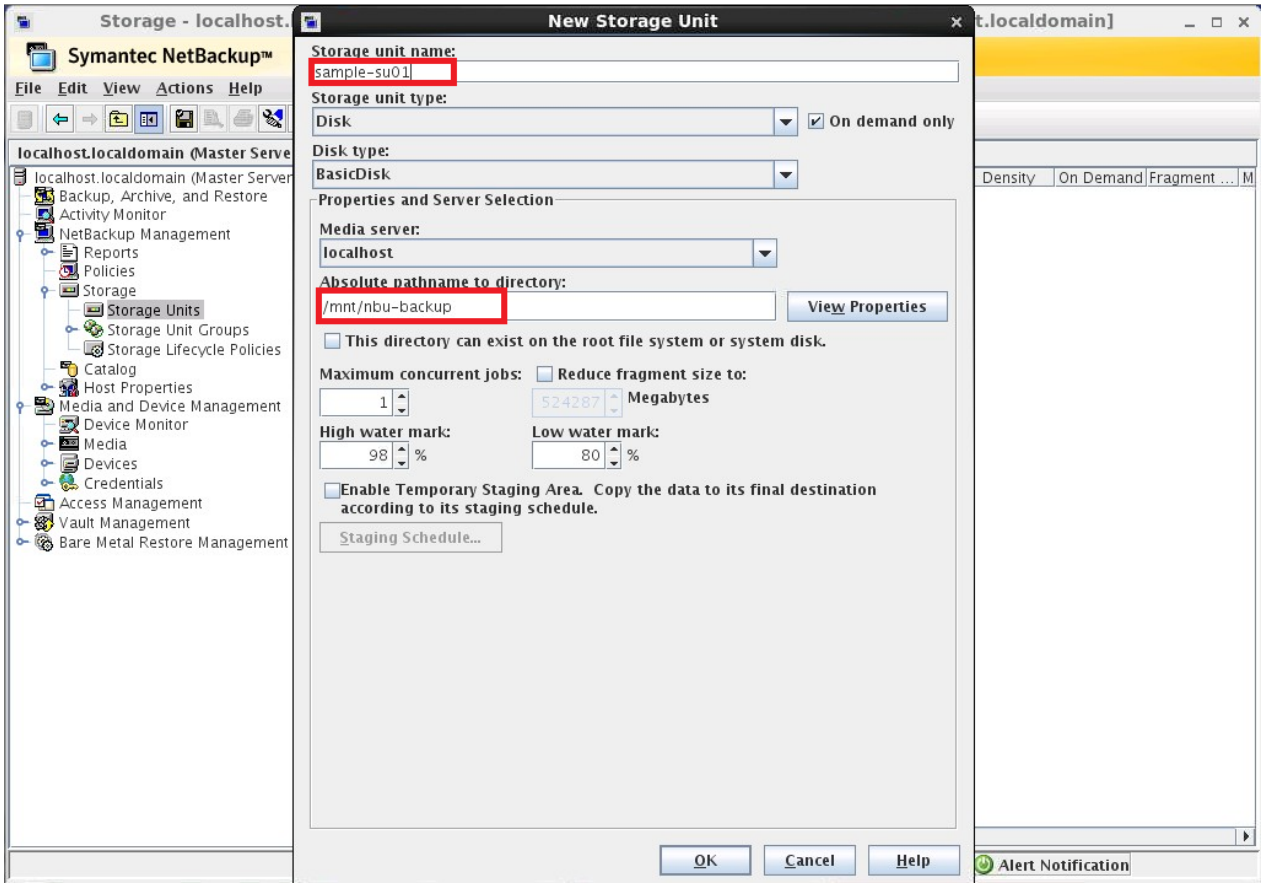
11. Close **Directory Properties**, and then click **OK**.



2.2 Setting up Symantec NetBackup storage units - Unix/Linux

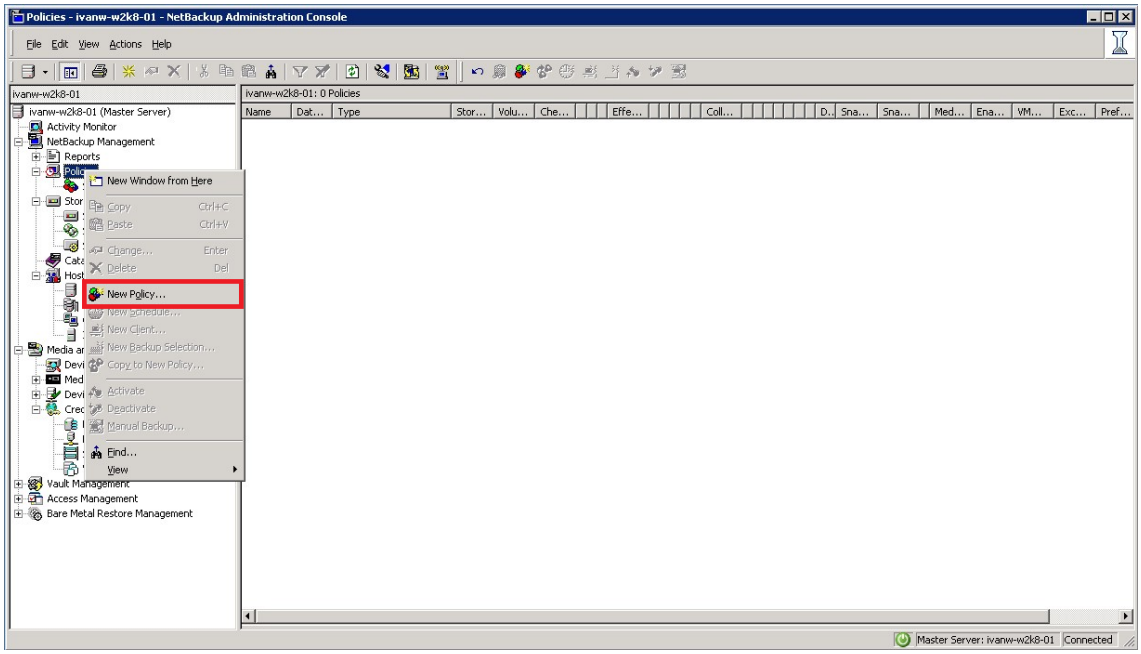
For this procedure, ensure that you can mount/verify the NFS share from the UNIX/Linux client system. See **Appendix B** for information about how to mount/verify the NFS share.

The procedure for the Unix/Linux Environment is similar to the procedure for the Windows Environment as described in the preceding section. The difference is that you must use UNIX path of the DR Series system container export instead of the UNC path, as shown in the screenshot below.

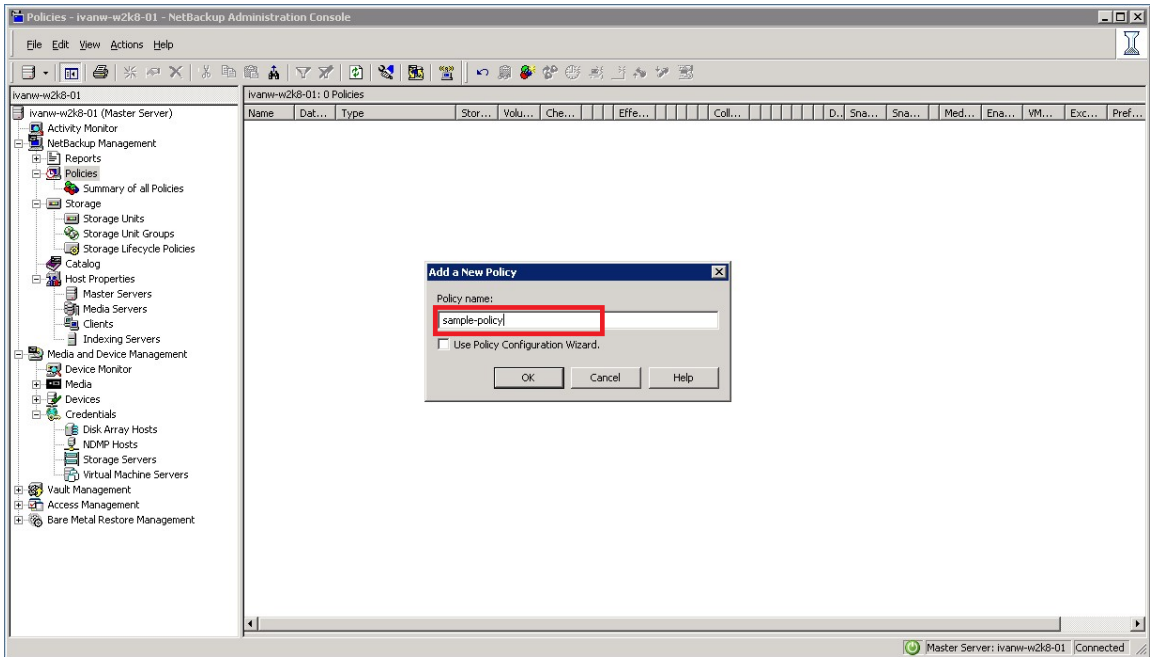


2.3 Creating a new backup job with the DR Series system as the target

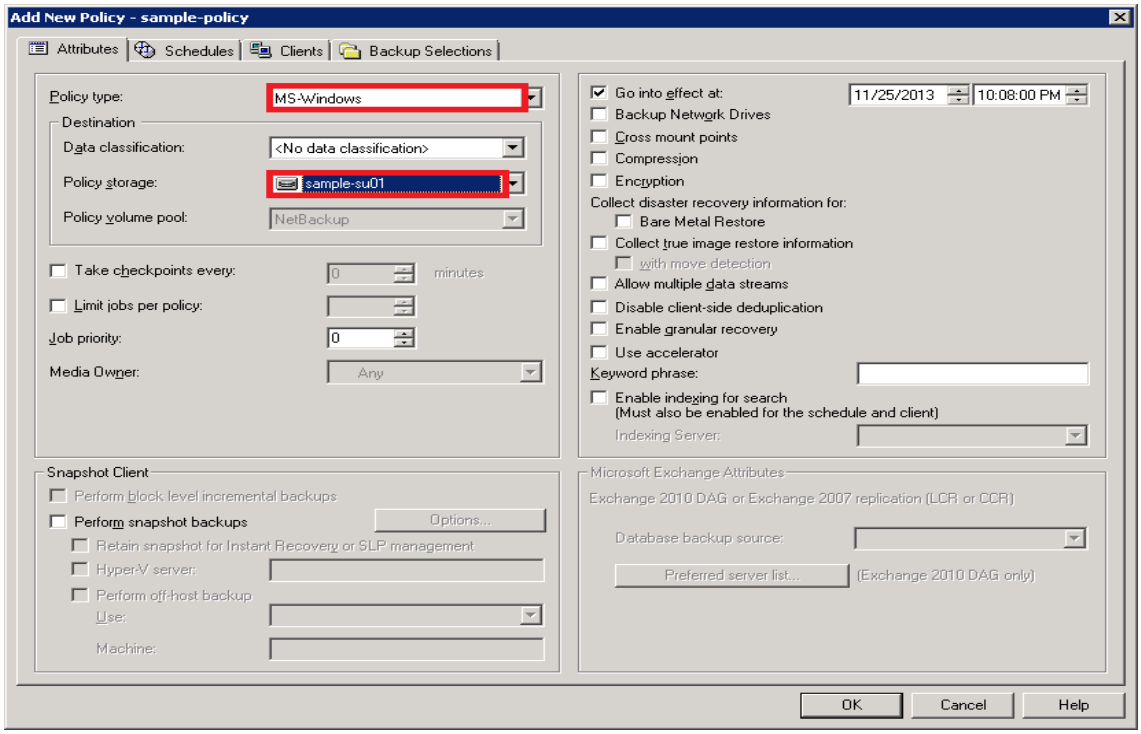
1. In the **NetBackup Administration Console**, right-click **Policies**, and then select **New Policy.**



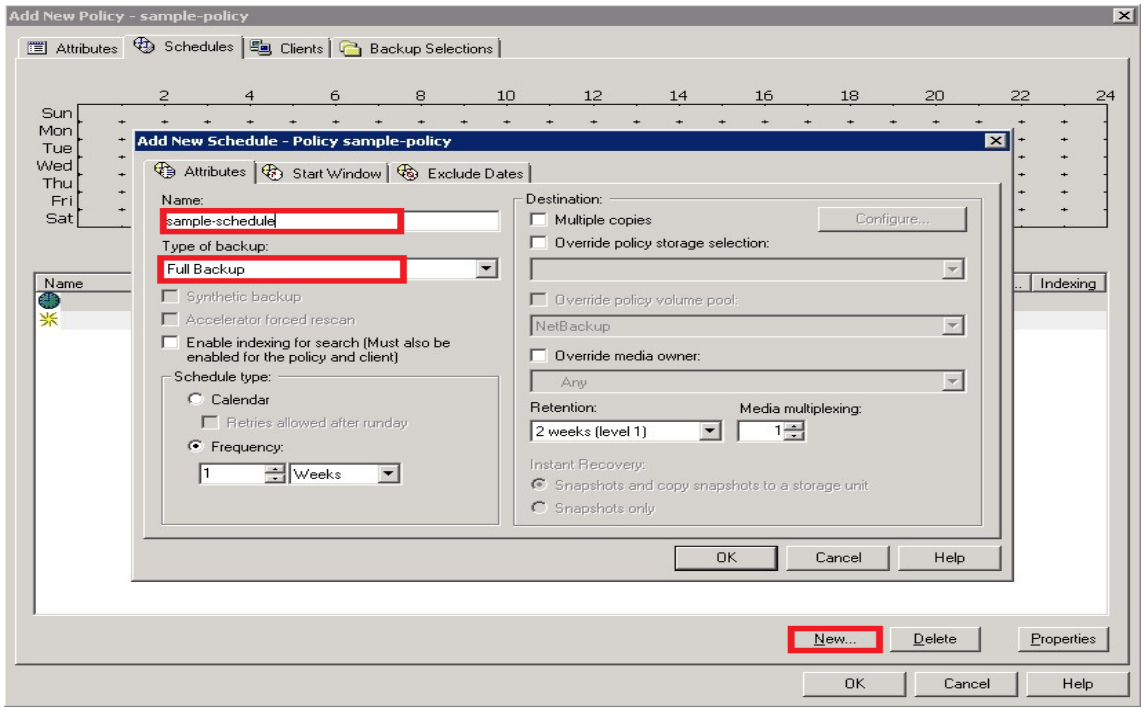
2. Enter a new policy name, and then click **OK**.



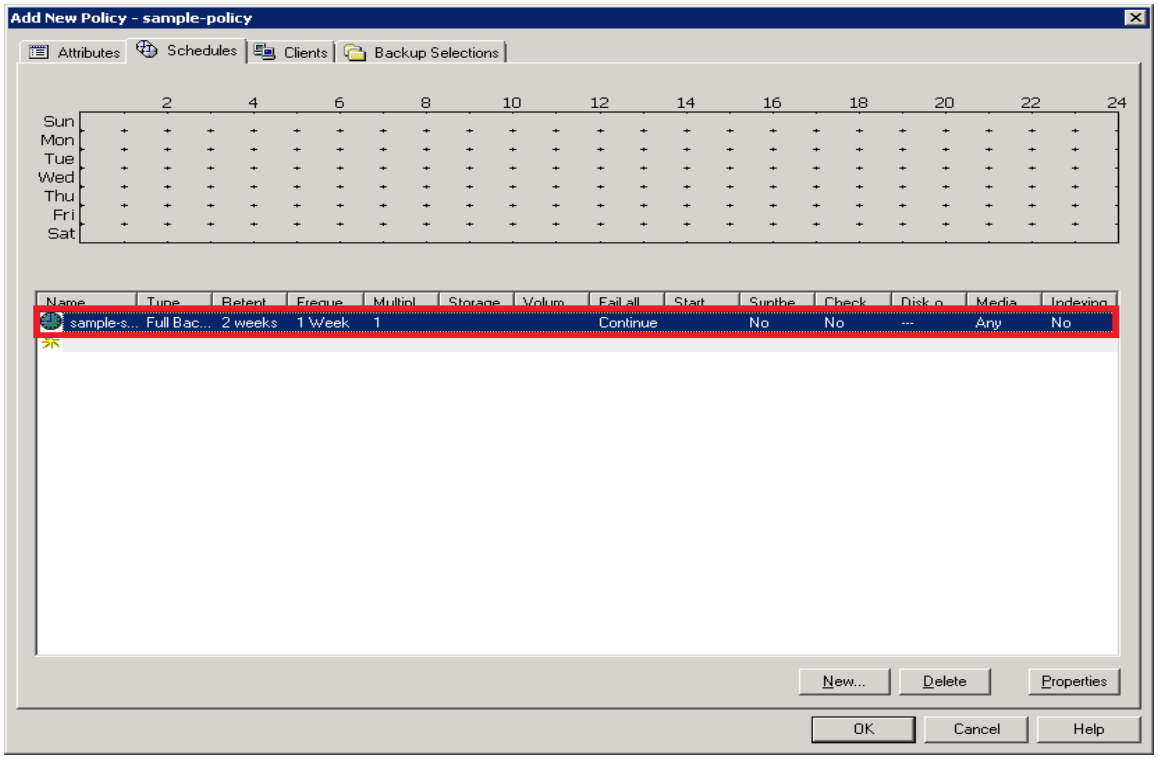
3. In the **Attributes** tab, select **Policy type** and **Policy storage**.



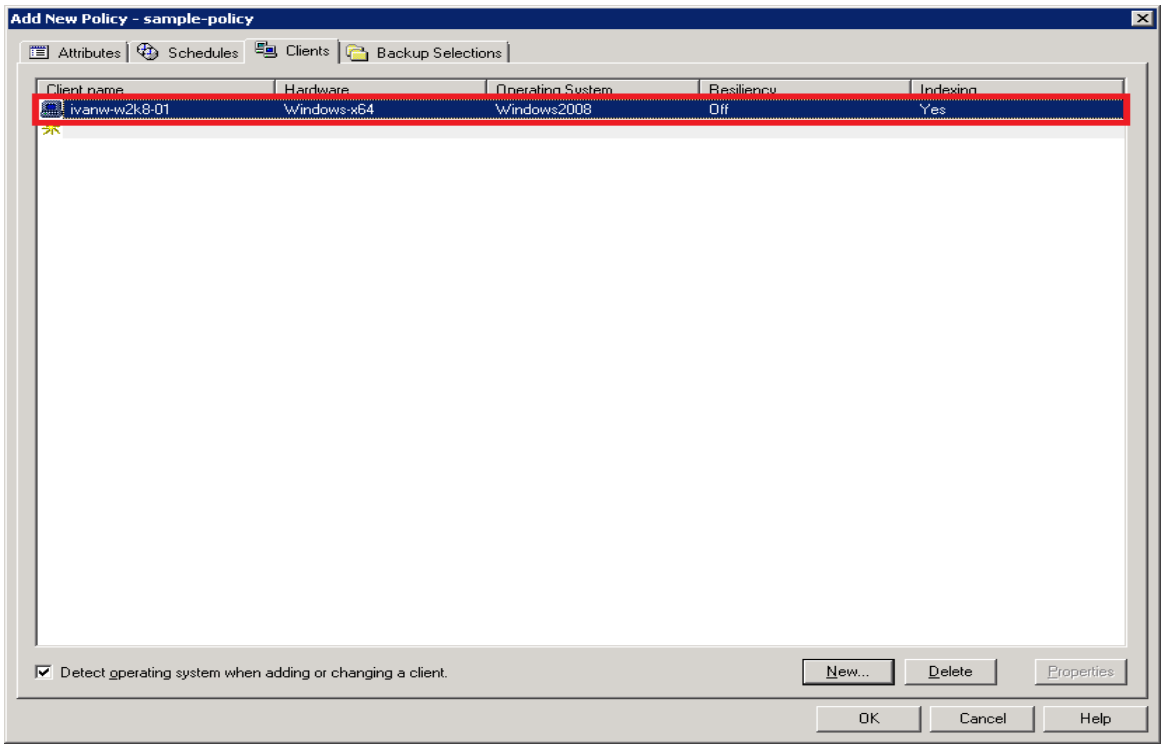
4. In the **Schedules** tab, click **New**, and then specify a schedule **Name**, and select **Type of backup.**



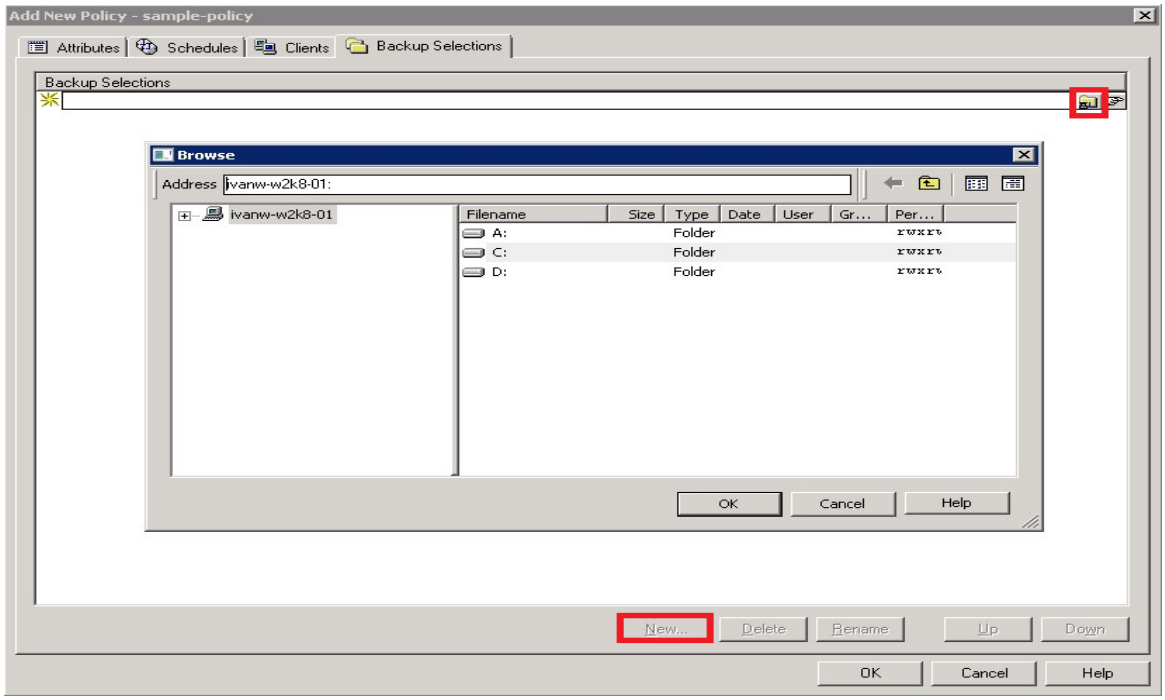
5. Click **OK** and verify that one full backup type schedule was added into the policy.



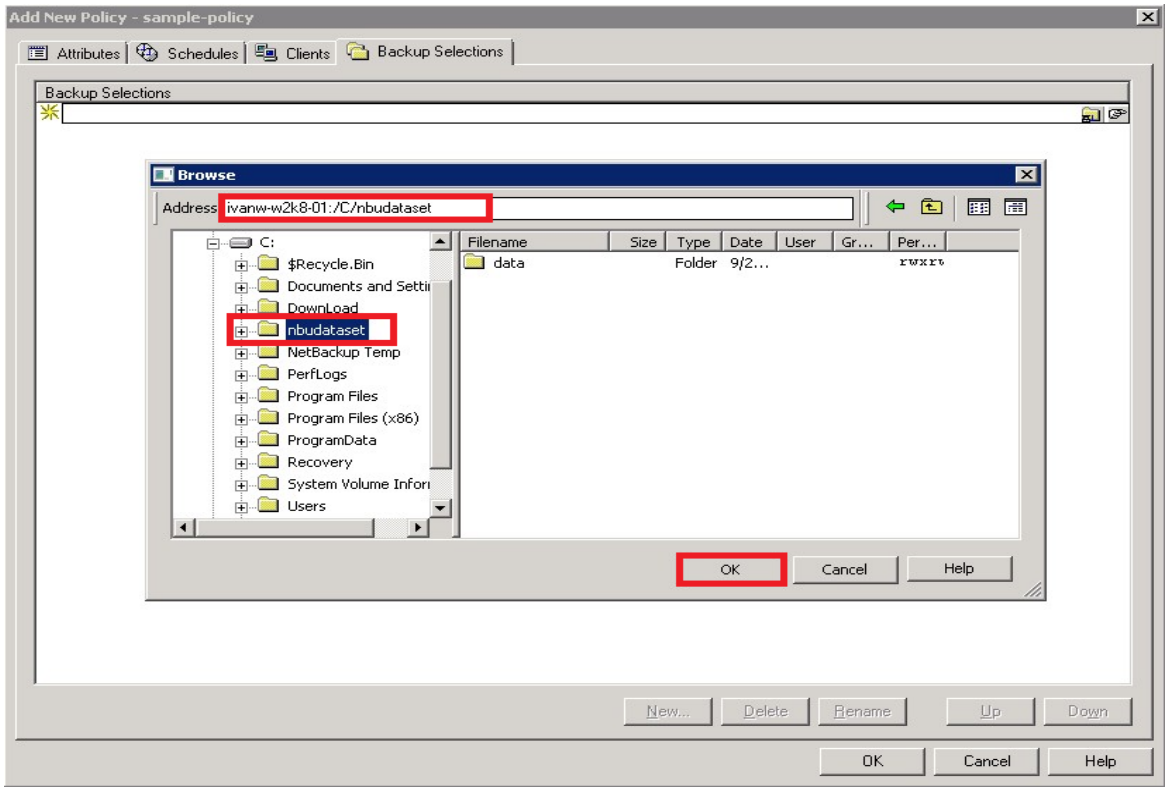
6. In the **Clients** tab, click **New**, enter the client name, and press **Enter**.



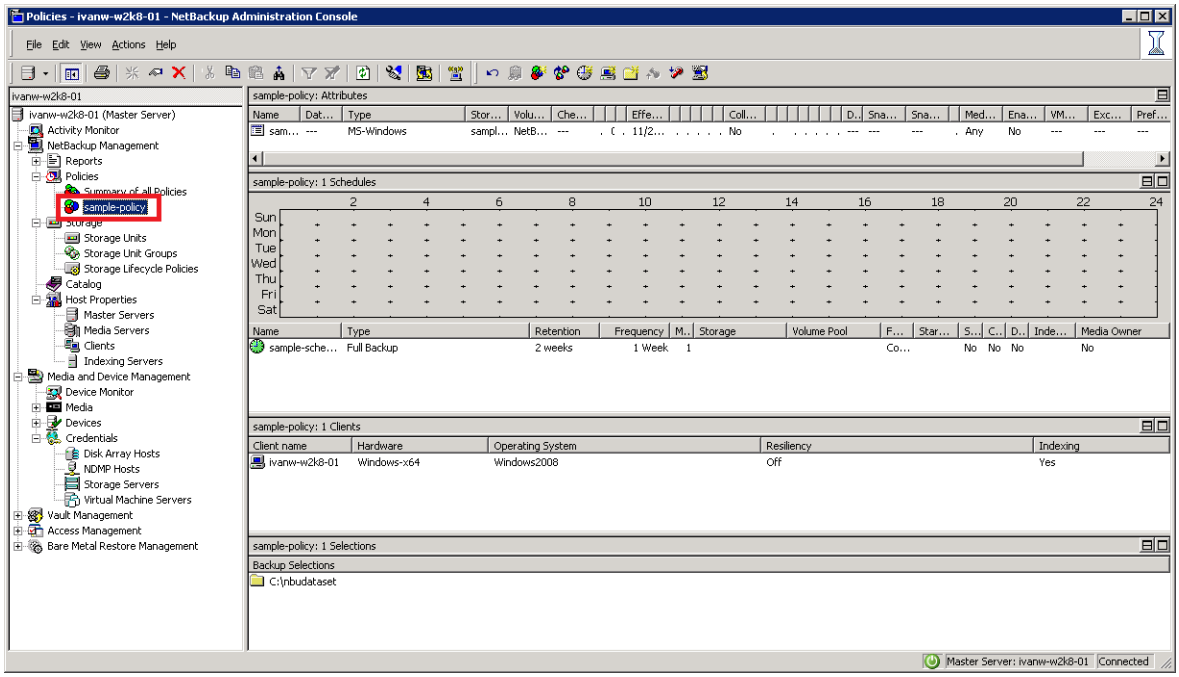
7. In the **Backup Selections** tab, click **New** and then click **Remote Folder**.



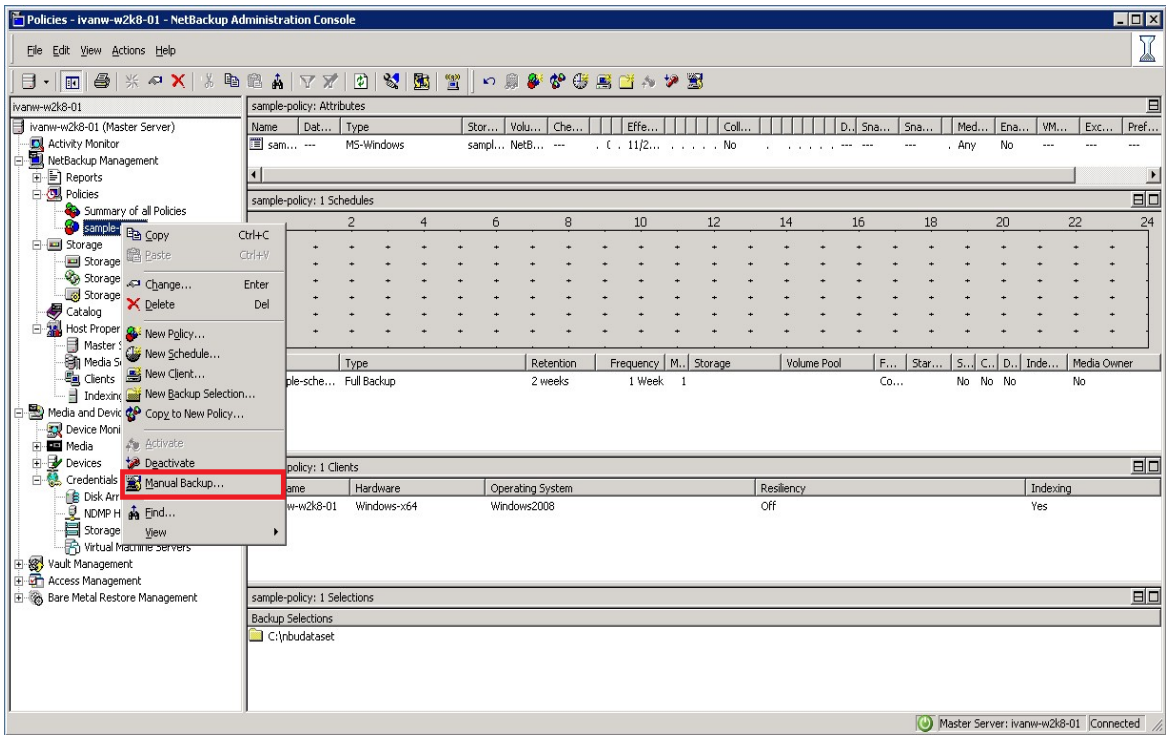
8. Select a backup path, and then click **OK**.



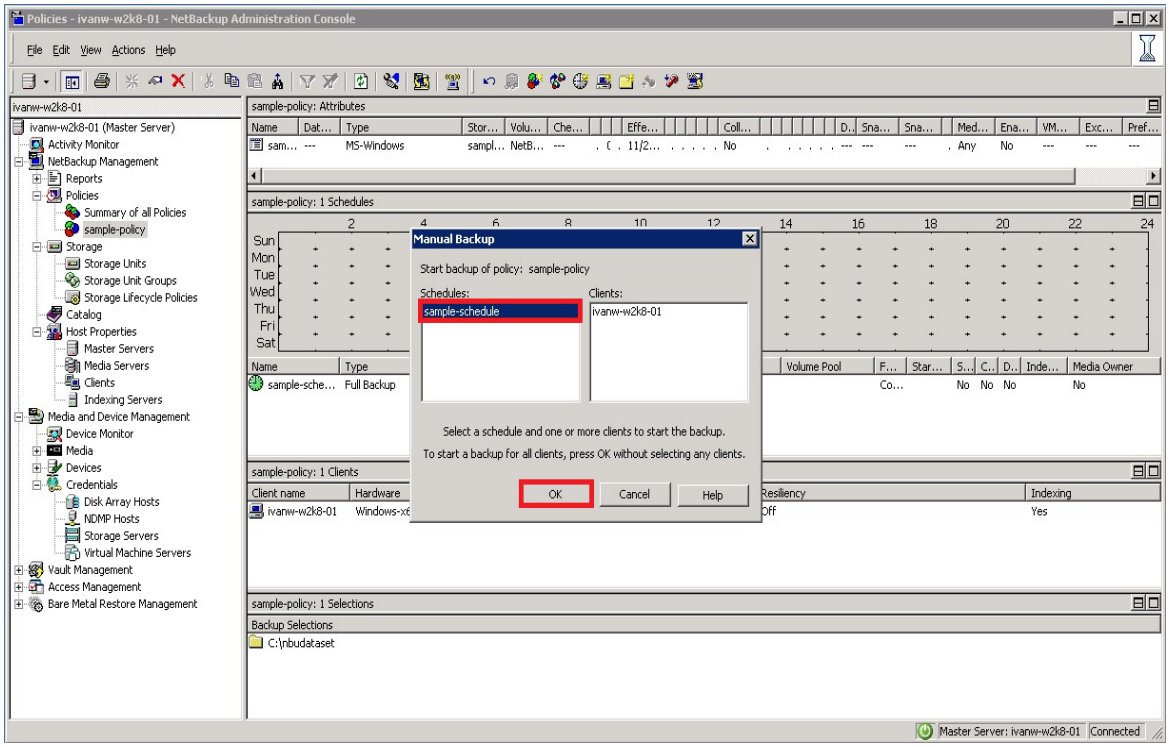
9. Click **OK.** A new policy is added.



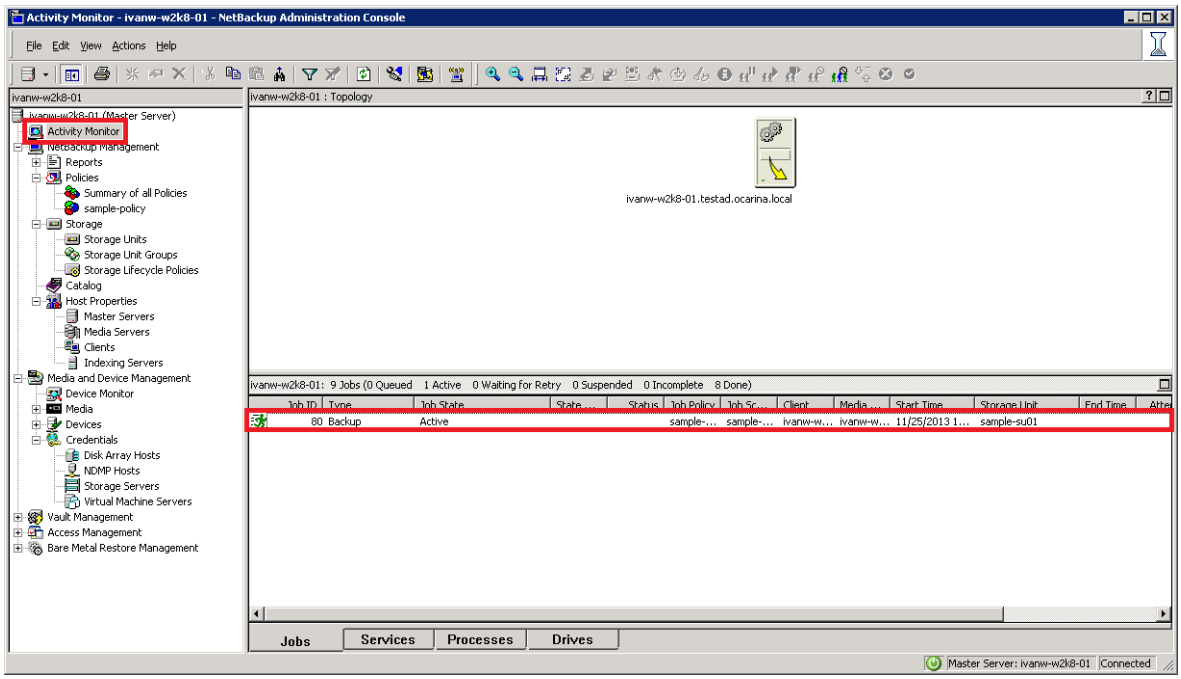
10. To run a manual backup right away and monitor the status, right-click the new policy, and select **Manual Backup**.



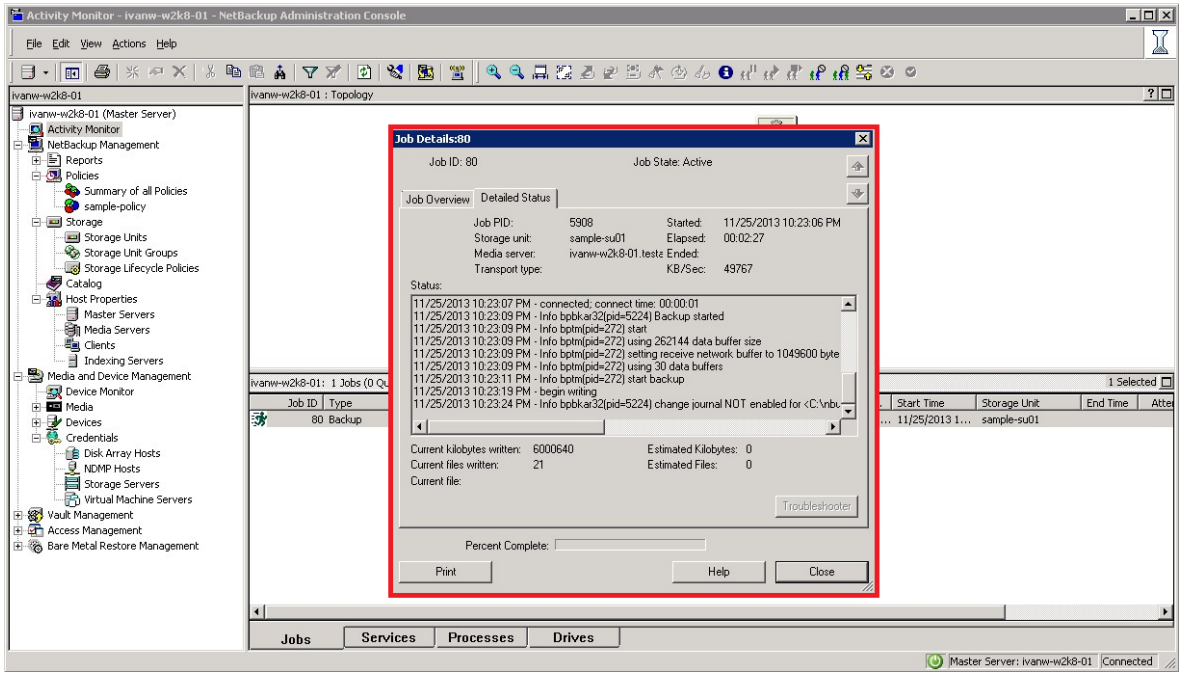
11. Select the new schedule, and then click **OK**.



12. Click **Activity Monitor** to monitor the job status.



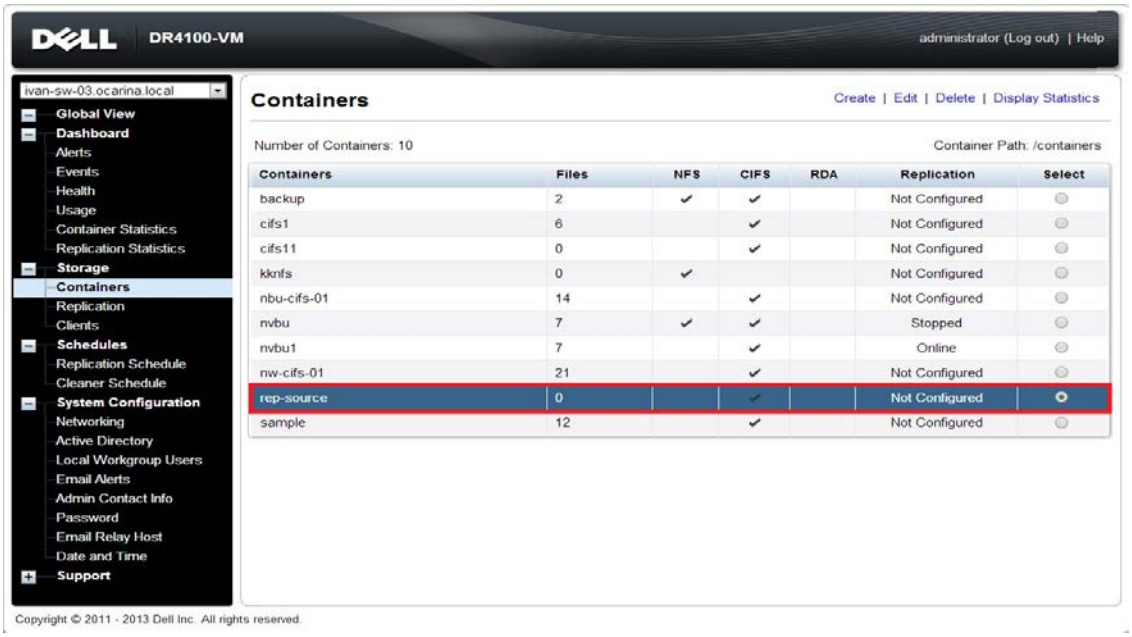
13. Double-click the job to view job details.



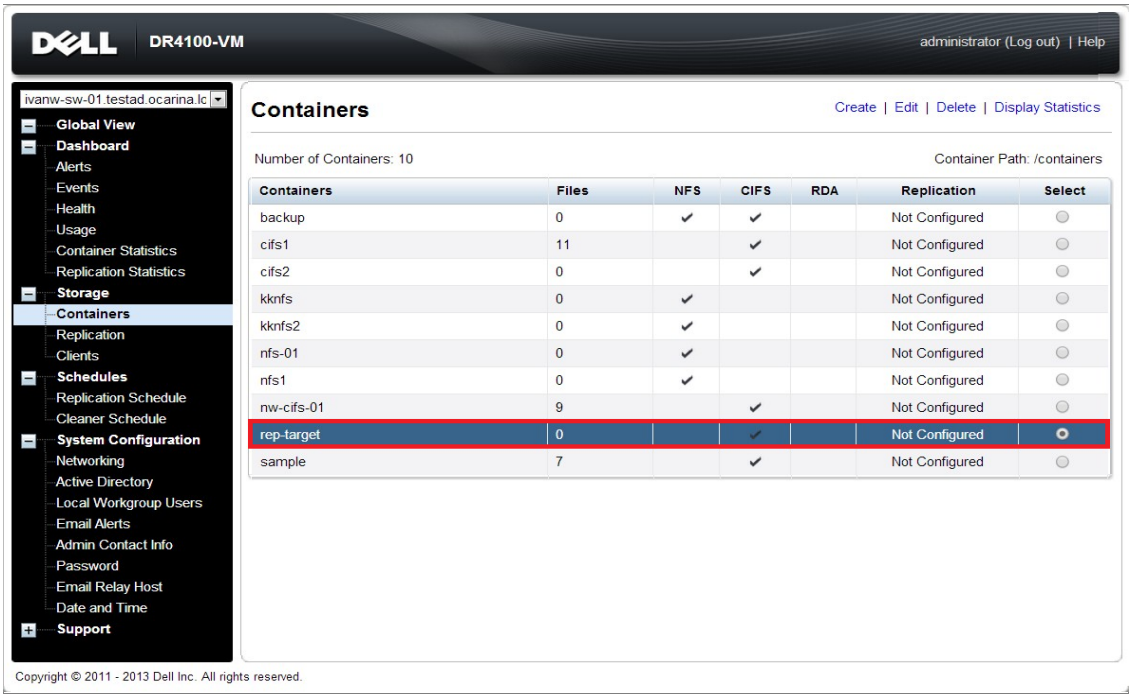
2.4 Setting up native replication & restore from the target container

2.4.1 Building the replication relationship between two DR Series systems

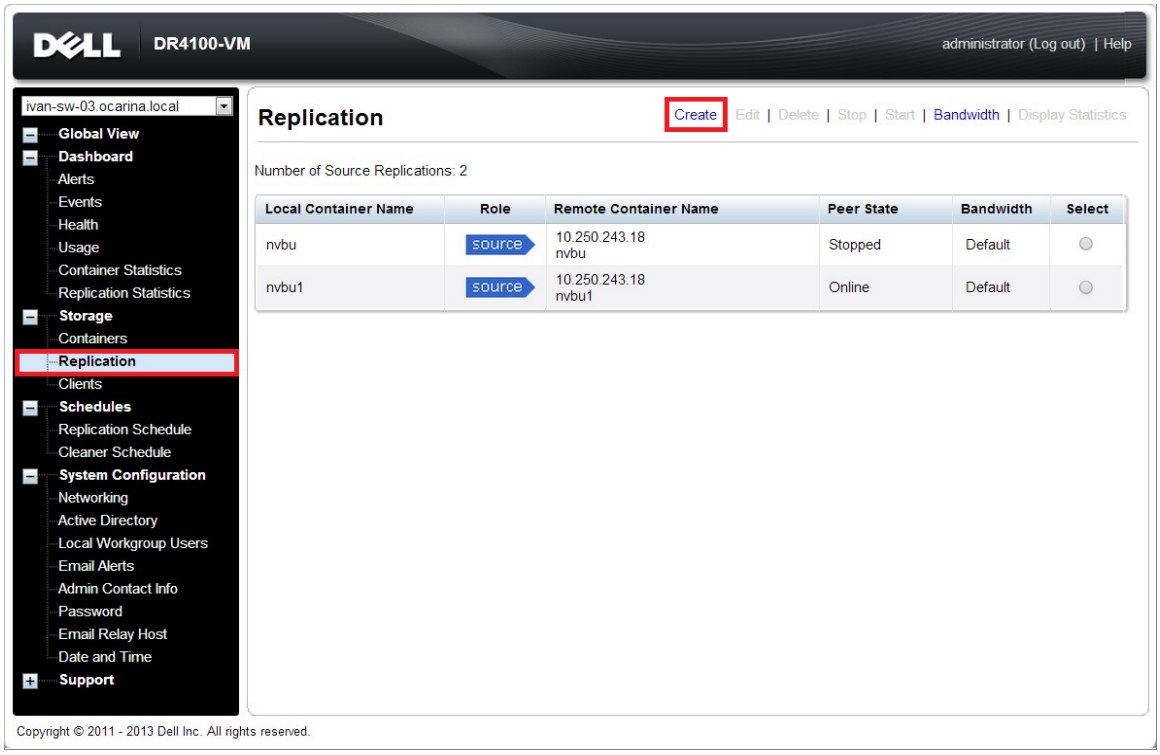
1. Create a source container on the first DR Series system.



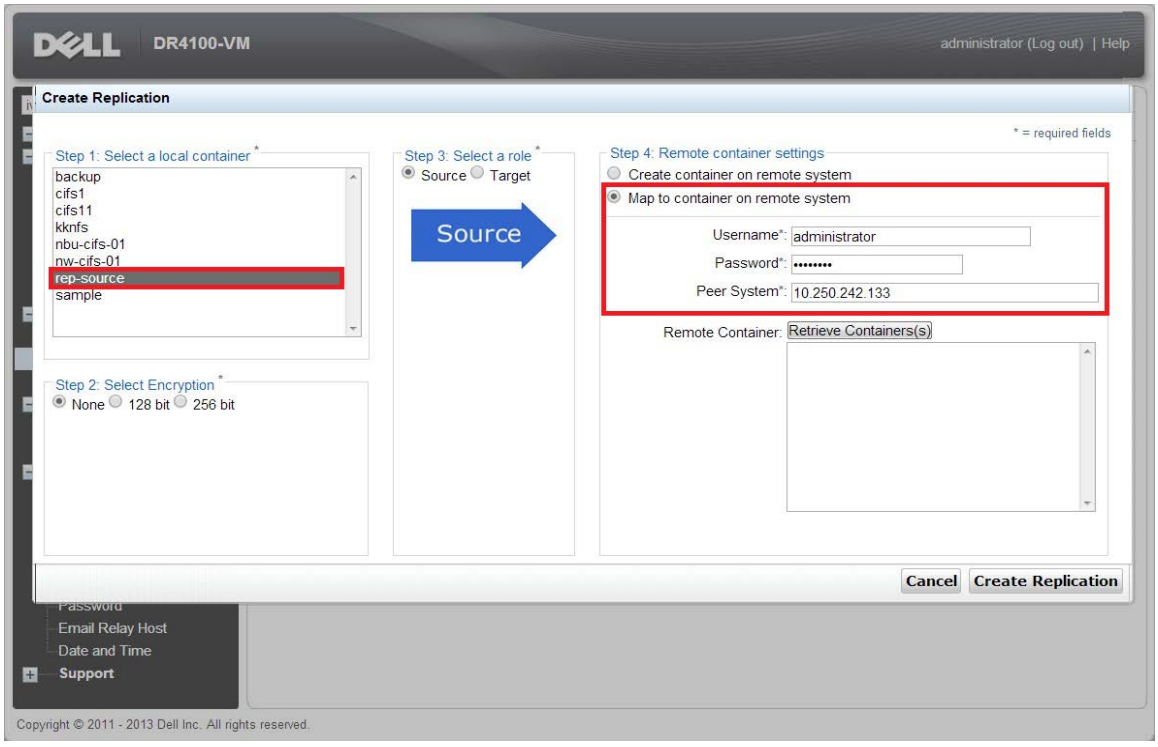
2. Create a target container on the second DR Series system.



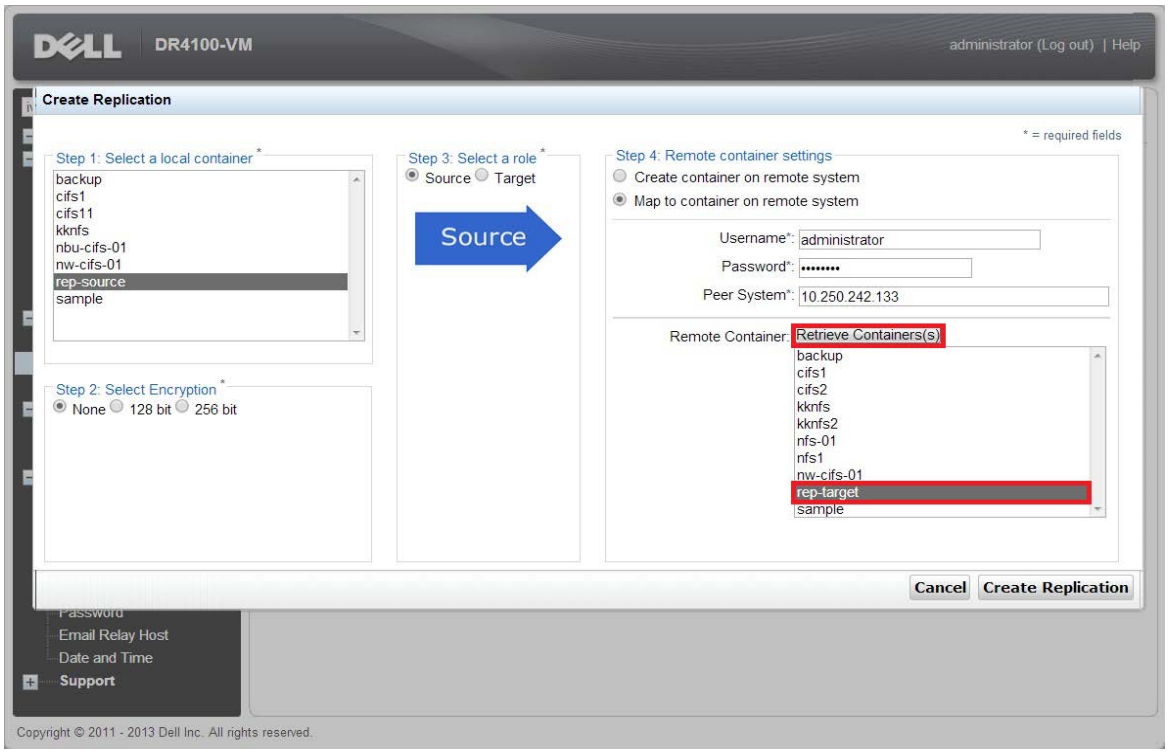
3. On the first DR Series system, go to the **Replication** page, and then click **Create**.



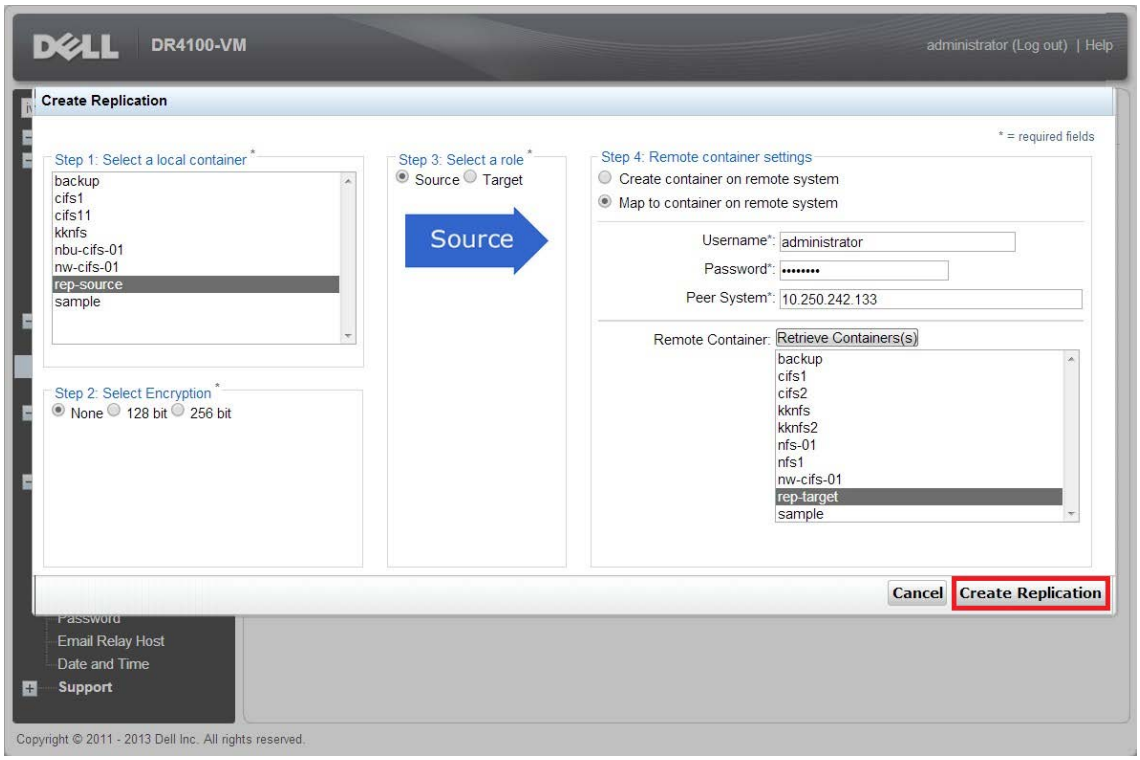
4. Select a local container as the source container, and then enter the information for the second DR Series system.



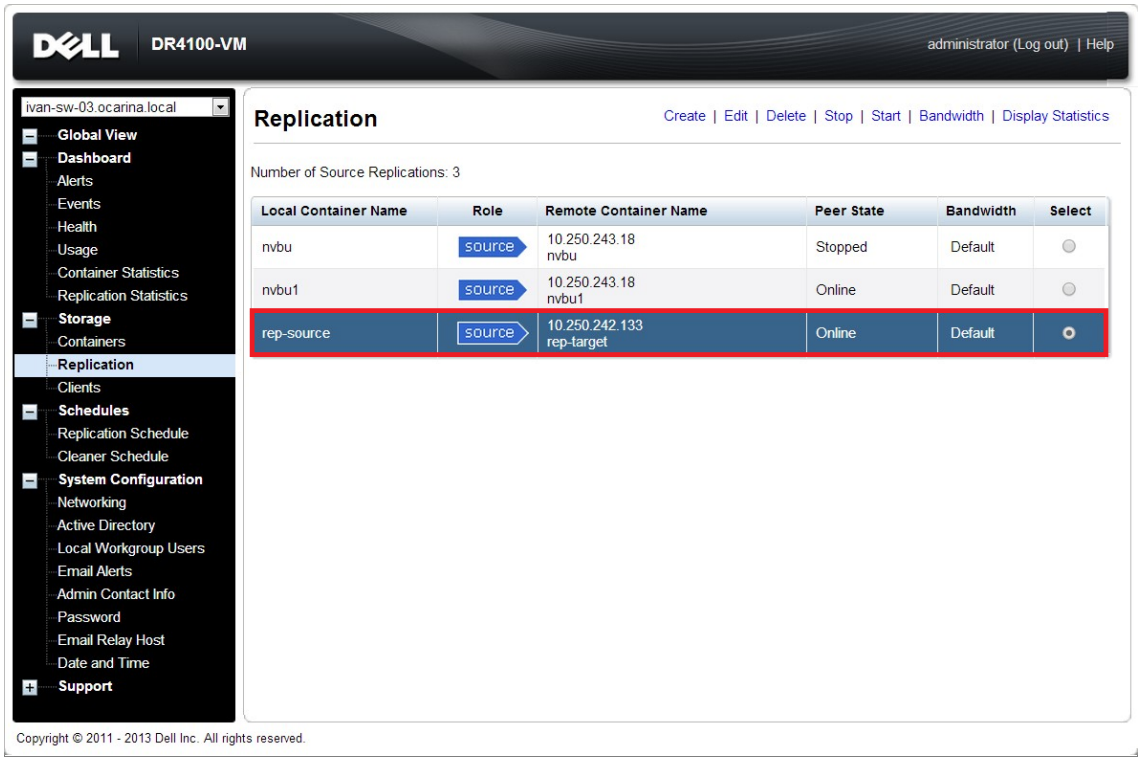
5. Click **Retrieve Containers**, and then select the target container on the list.



6. Click **Create Replication**



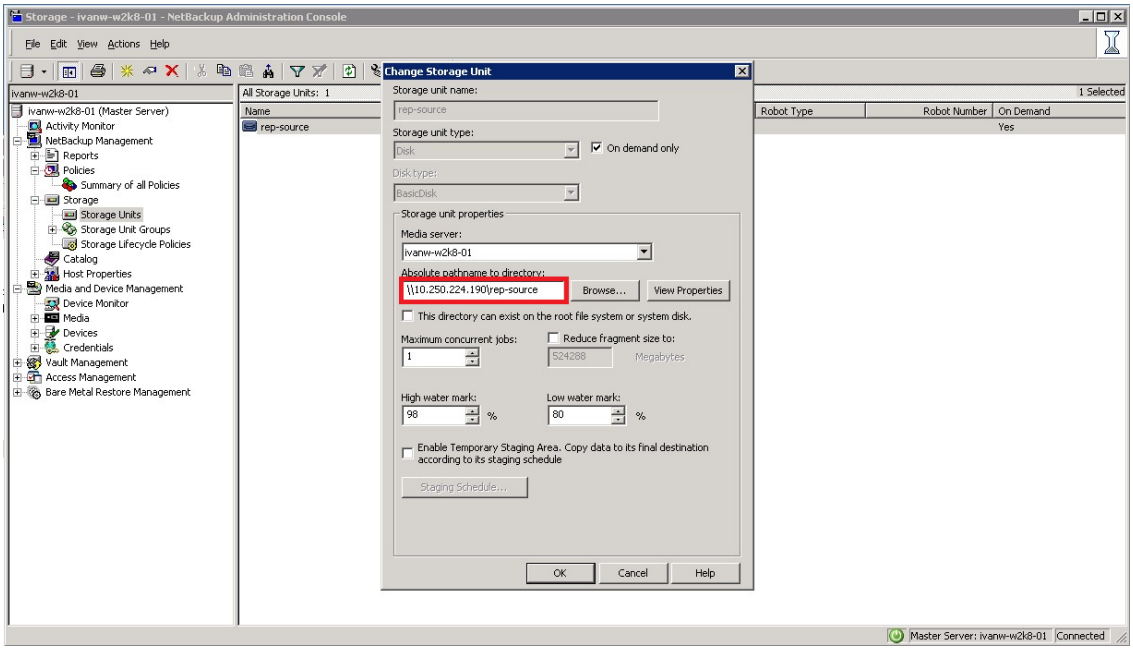
7. Verify that the replication relationship between the DR Series systems is created.



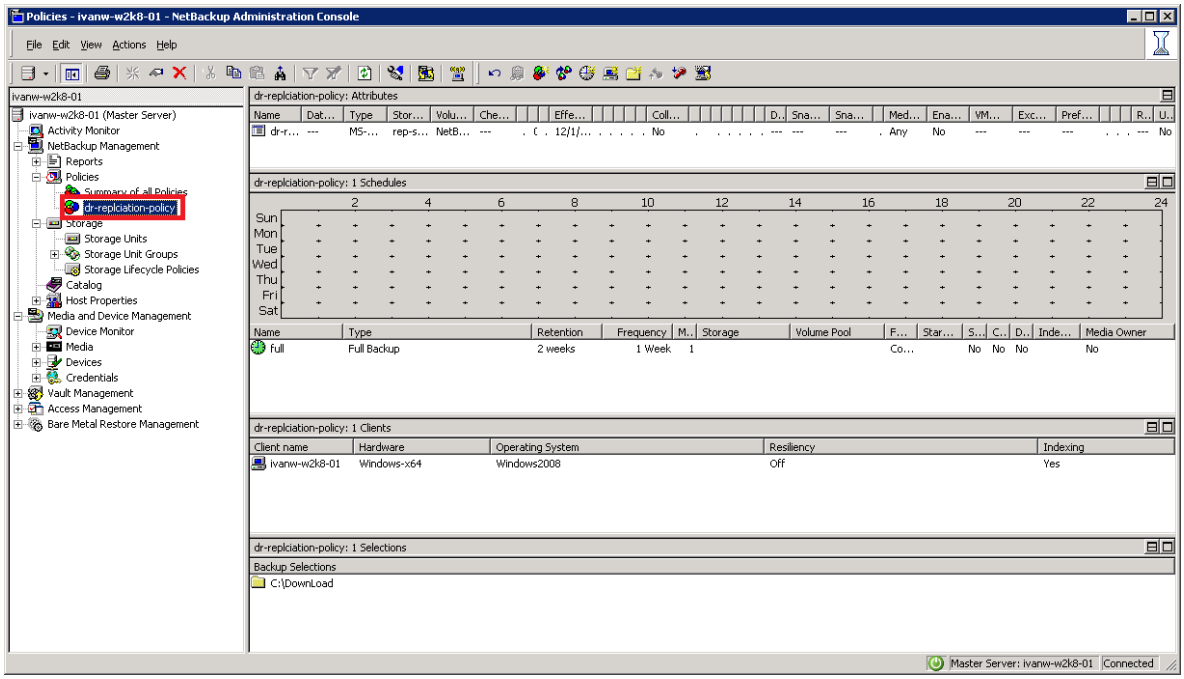
2.4.2 Backing up the image to the source DR Series system

This procedure is optional – if the source DR Series system container is newly created without having data backed up.

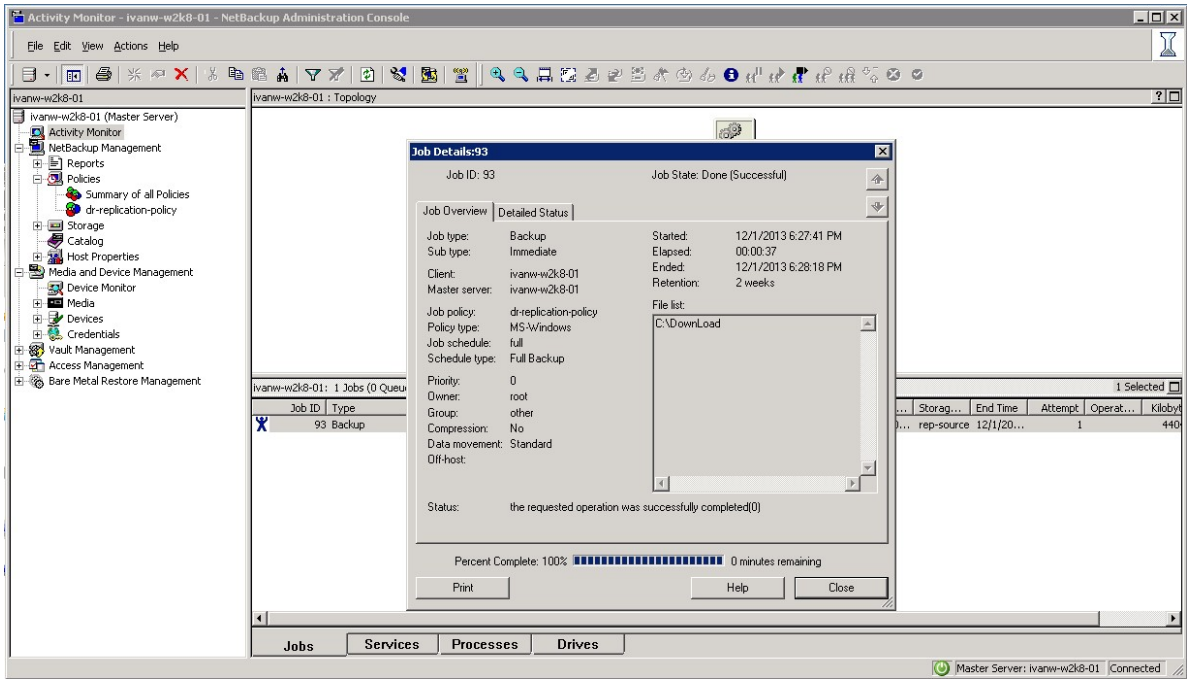
1. Add the source container to NetBackup.



2. Create a new backup policy.



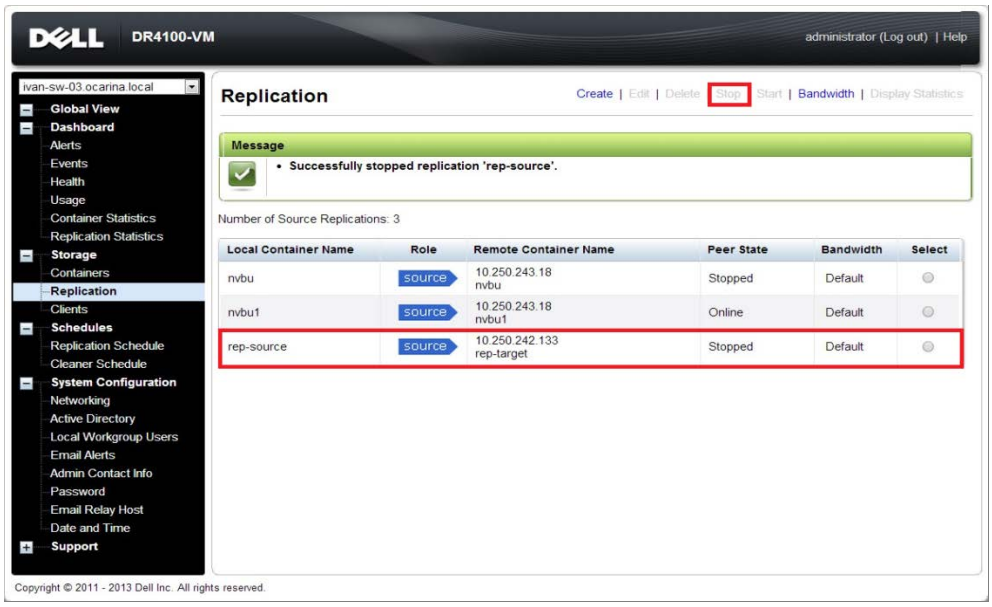
3. Run the backup job.



2.4.3 Cleaning up the image from NetBackup

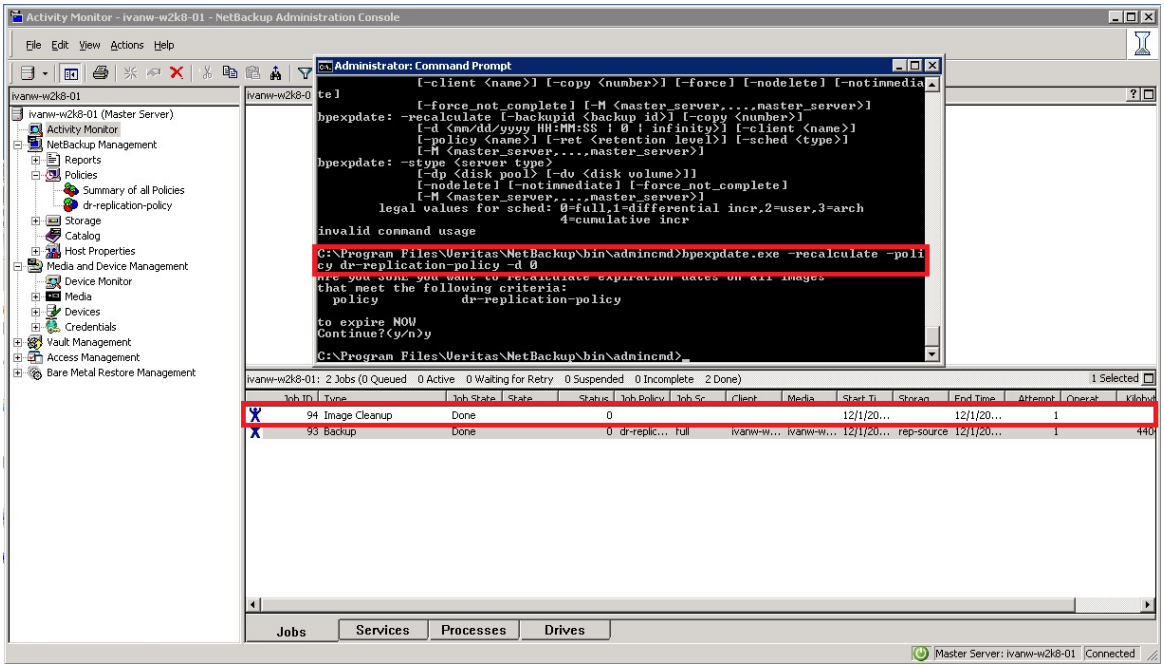
This procedure is optional and is only required when importing of images reports a failure (The image import procedure is described in later in this document). The purpose of this procedure is to clean up residual images that could have conflicts with imported images.

1. Stop replication between the DR Series systems.



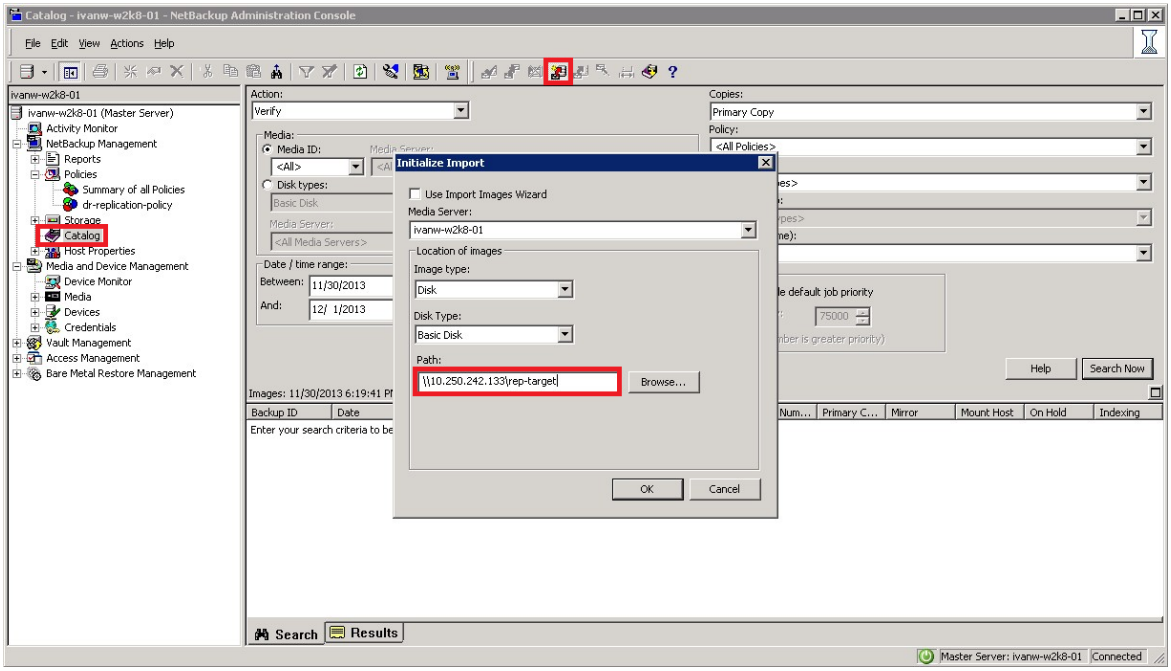
Note: Before cleaning up the image from NetBackup, you should stop/delete replication first. If you do not, the backup image on the target DR Series system will be cleaned up.

2. Clean up the image, and from the command line, run the following command. NetBackup will automatically run the cleanup job.

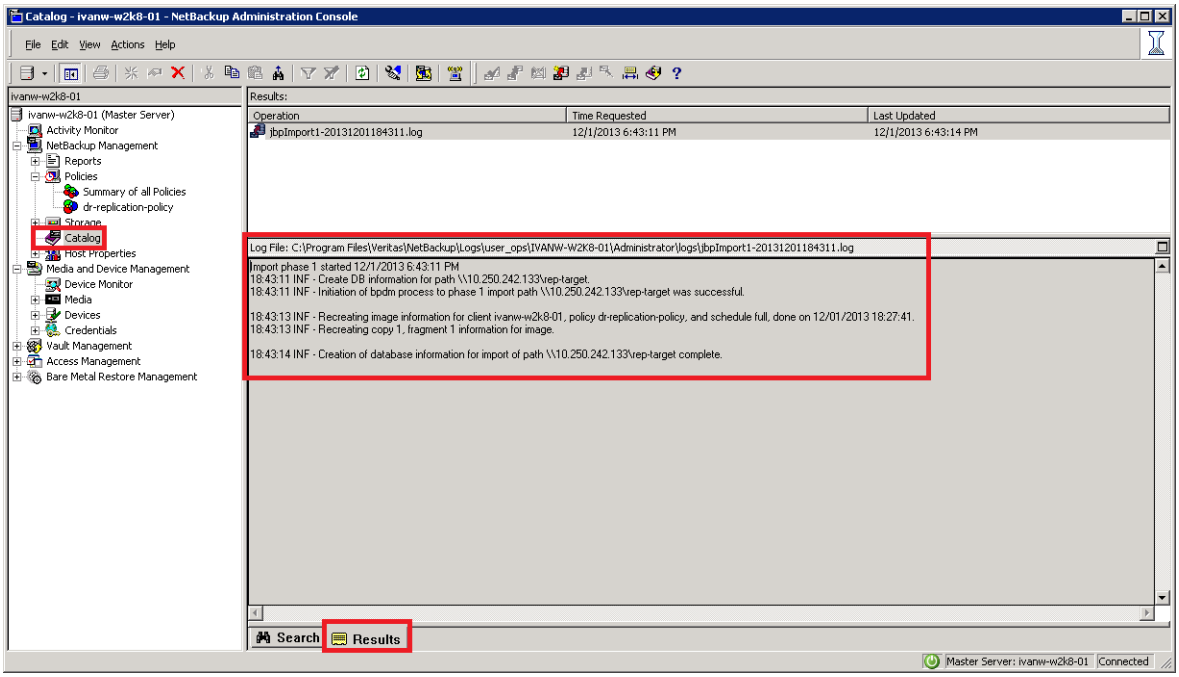


2.4.4 Importing the image from the target DR Series system

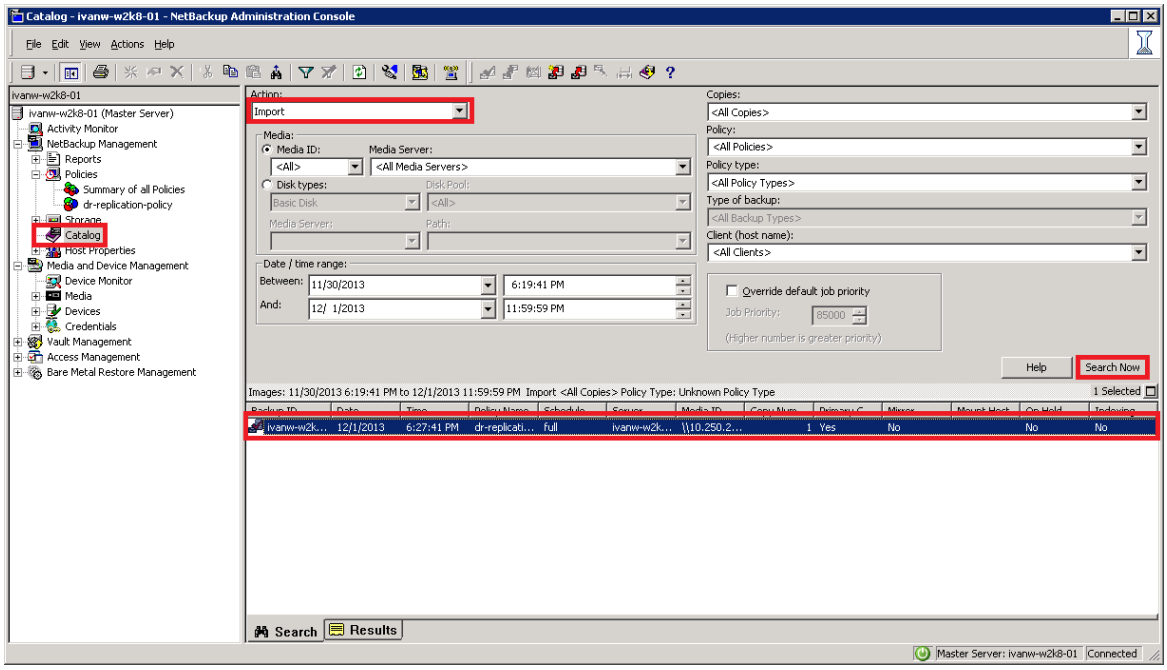
1. Go to **Catalog**, and then click **Initiate Import**. Enter the target container path, and then click **OK**.



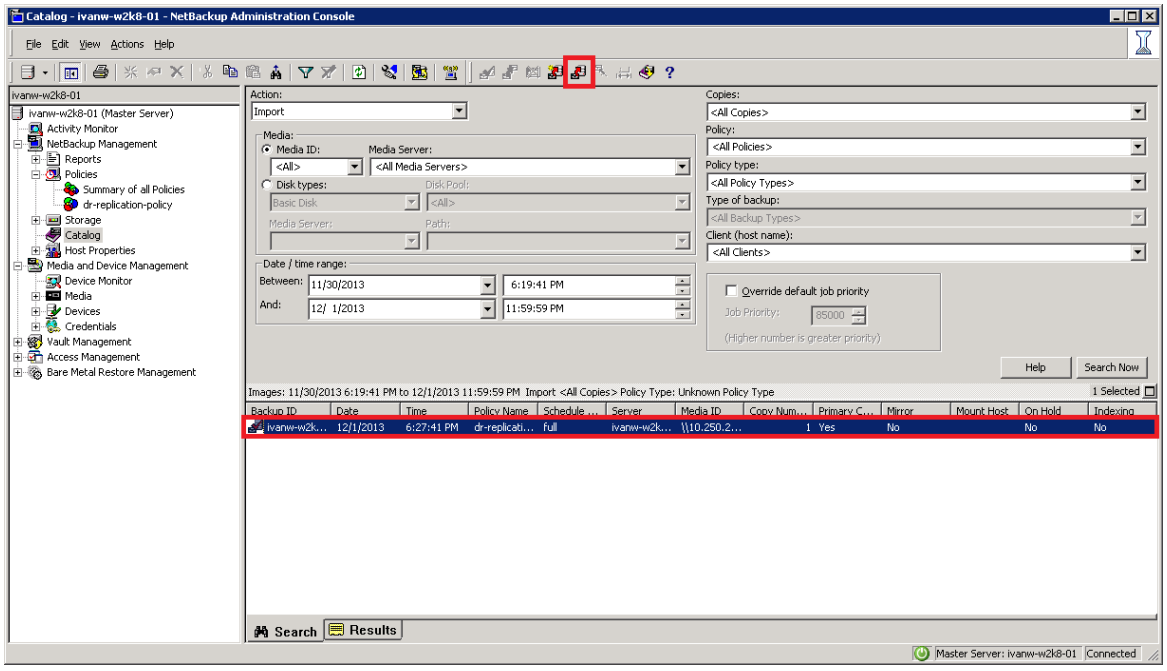
2. Click the **Results** tab, and check the import results.



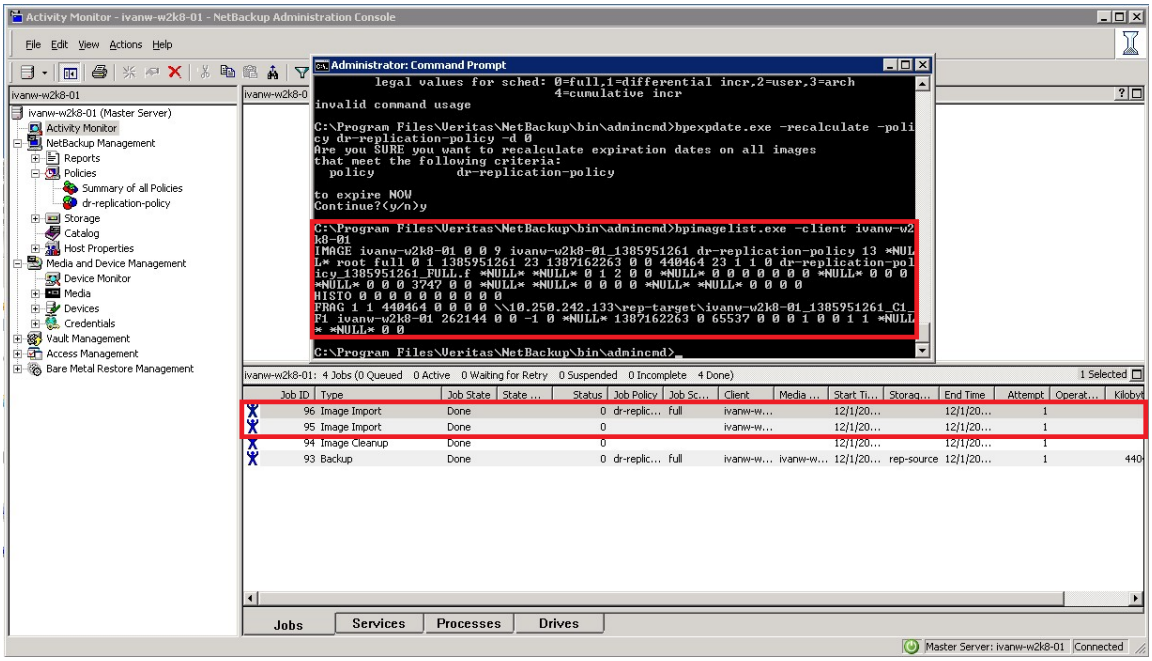
3. Go back to the **Search** tab, select **Import**, and then click **Search Now**.



4. Select the import image, and then click **Import**.

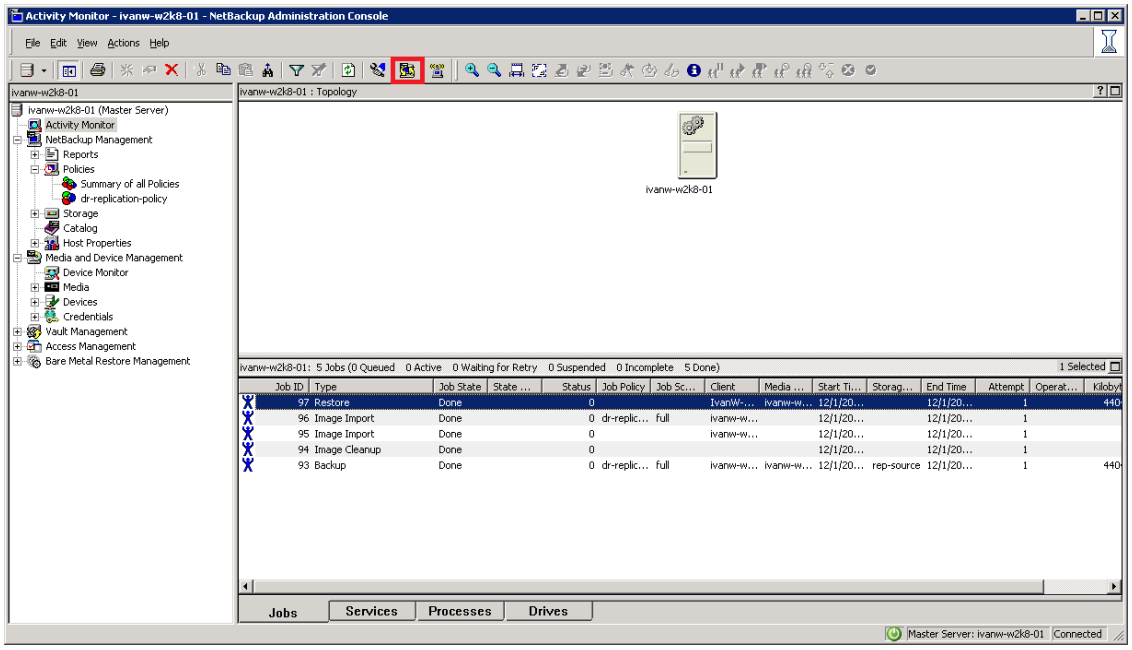


5. Go to the **Activity Monitor** or run the **bpimagelist** command, and check the image import status.

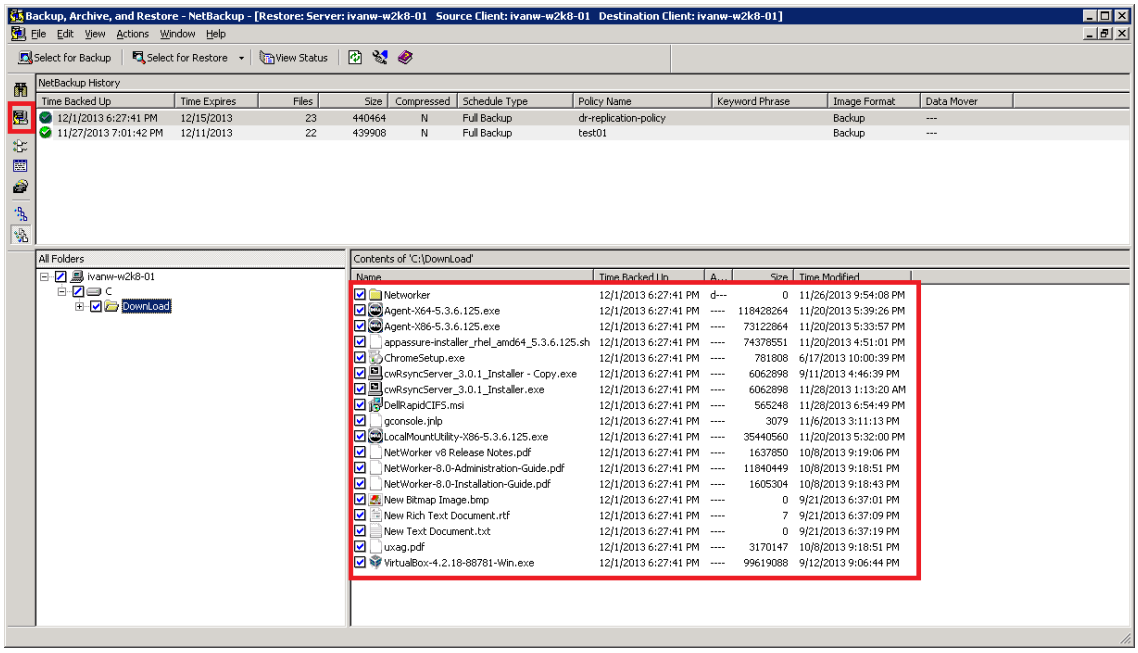


2.5 Restoring the image from the target DR Series system

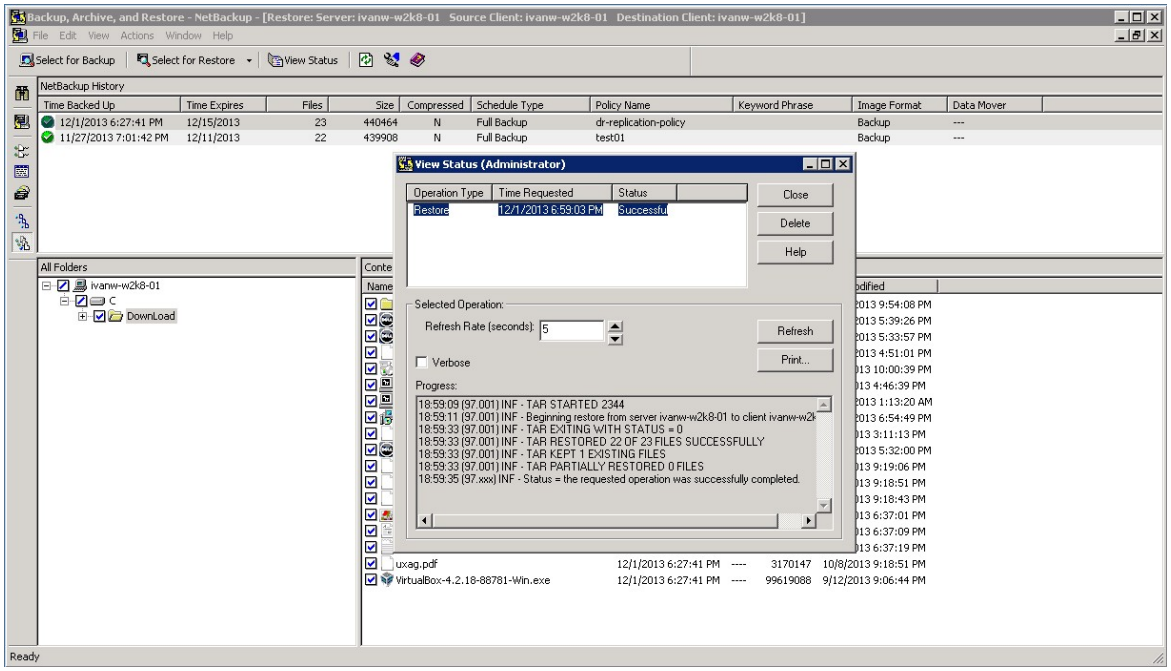
1. Click the NetBackup Administrator Console.



2. Select the files that you want to restore, and then click **Start Restore of Marked Files**.

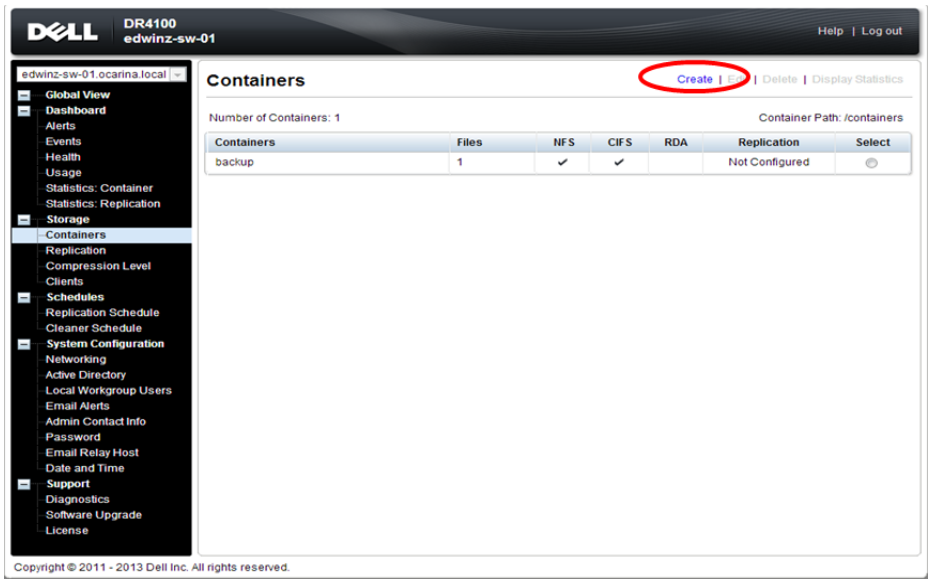


3. Run the restore job.

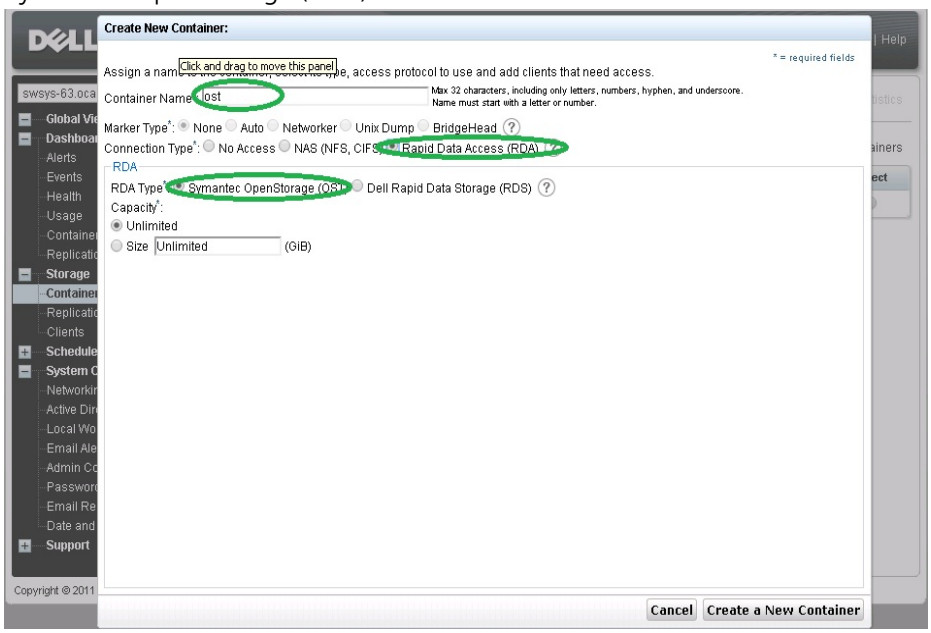


3 Creating and configuring OST target container(s) for NetBackup

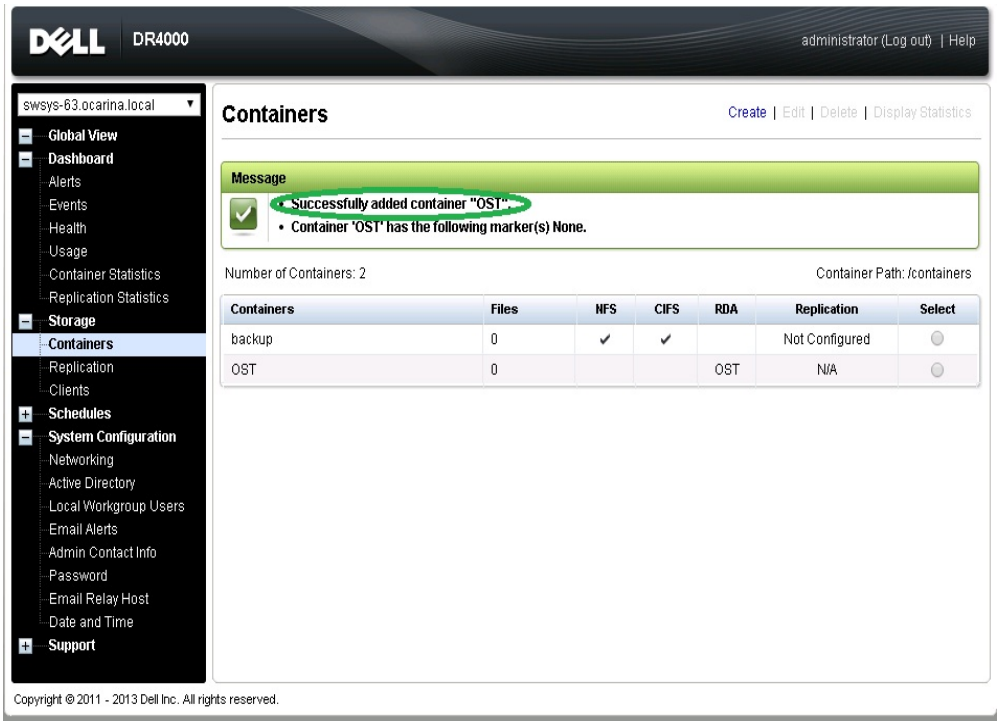
1. Create an **OST** container in the DR Series system GUI by selecting **Containers** in the left navigation area and then clicking **Create** at the top of the page.



2. Enter a container name and select the connection type as RDA. Then select the RDA type as Symantec OpenStorage (OST).



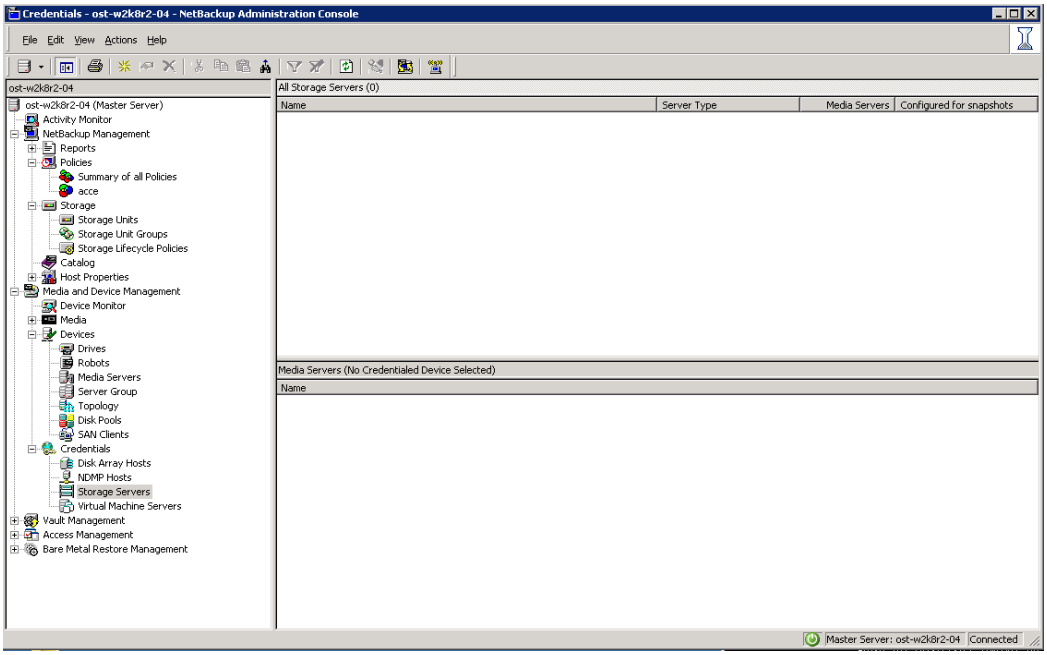
3. Click **Create a New Container** and confirm that the container was added.



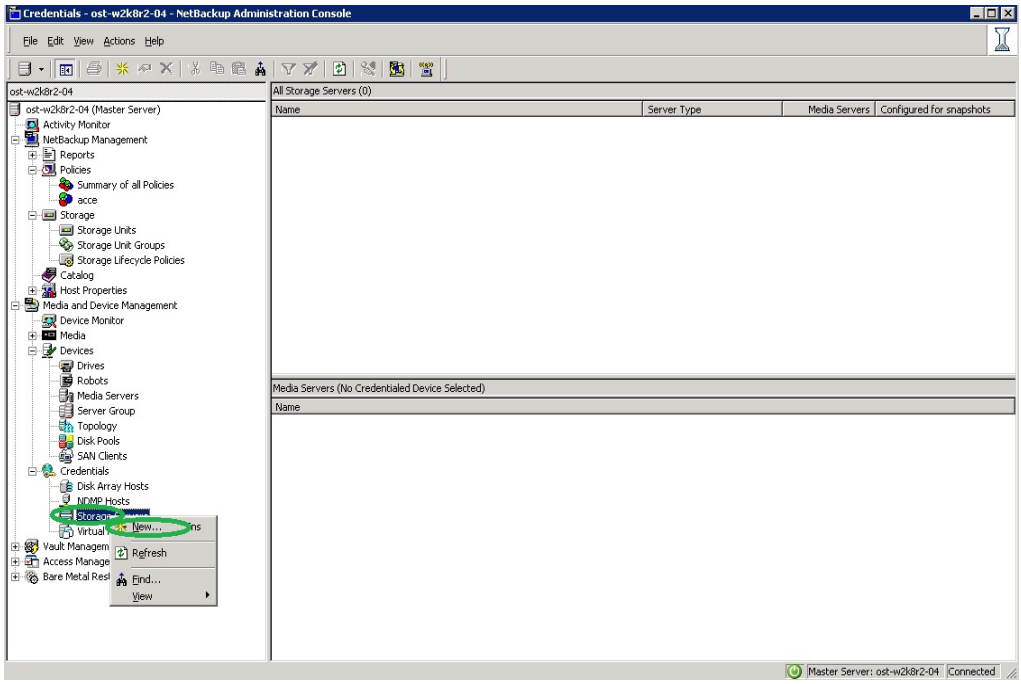
3.1.1 Setting up NetBackup for virtual synthetic backup on a Windows or Linux client

Note: Make sure that the Dell OST plugin is installed on the DMA client that is used for NetBackup.

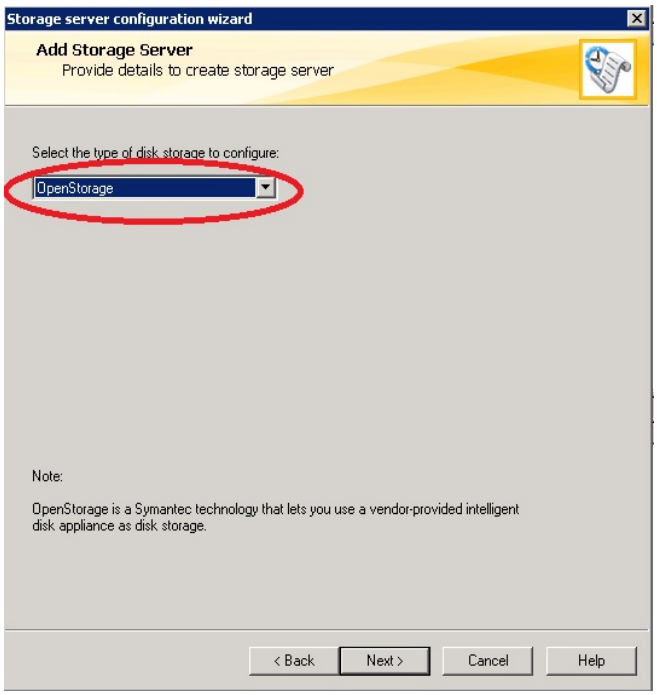
1. Launch the NetBackup Console.



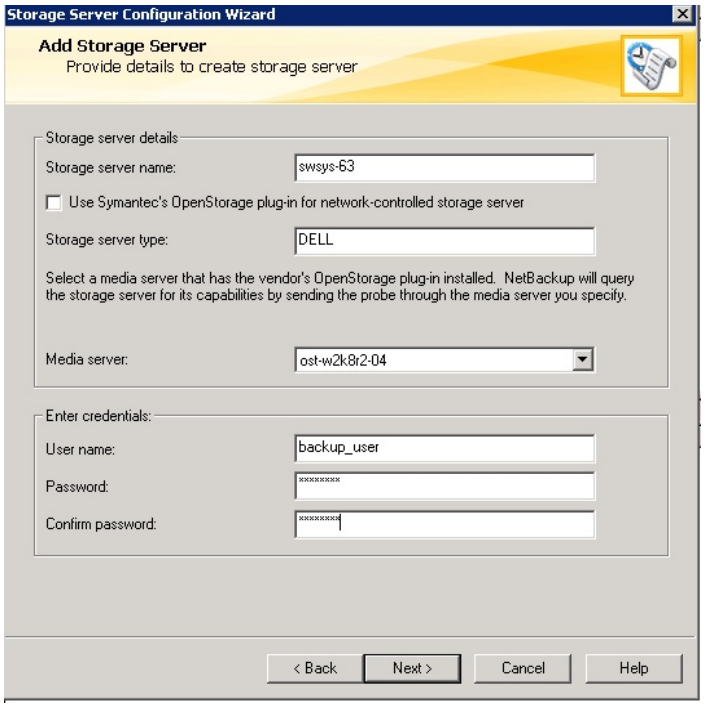
2. Right-click **Media and Device Management** and select **Credentials** > **Storage Server**, and then click **New**.



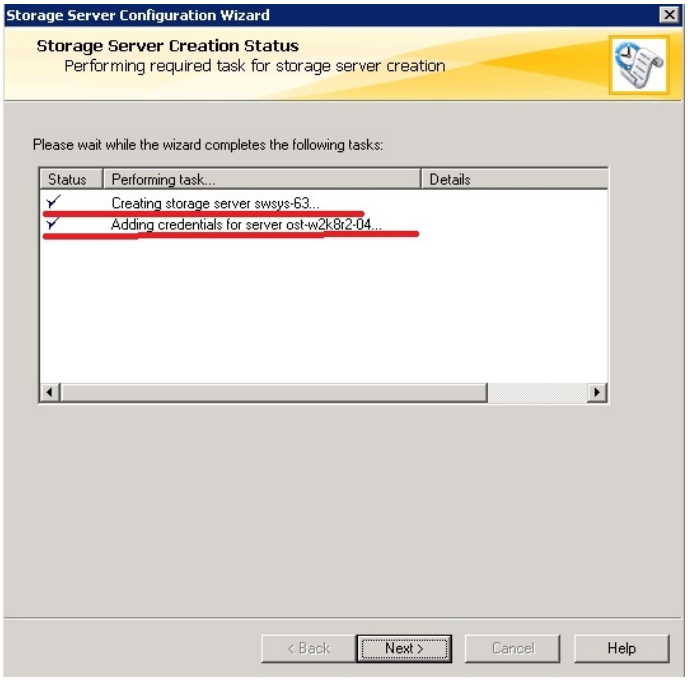
3. In the **Storage server configuration wizard** dialog box, select **OpenStorage** from the list and click **Next**.



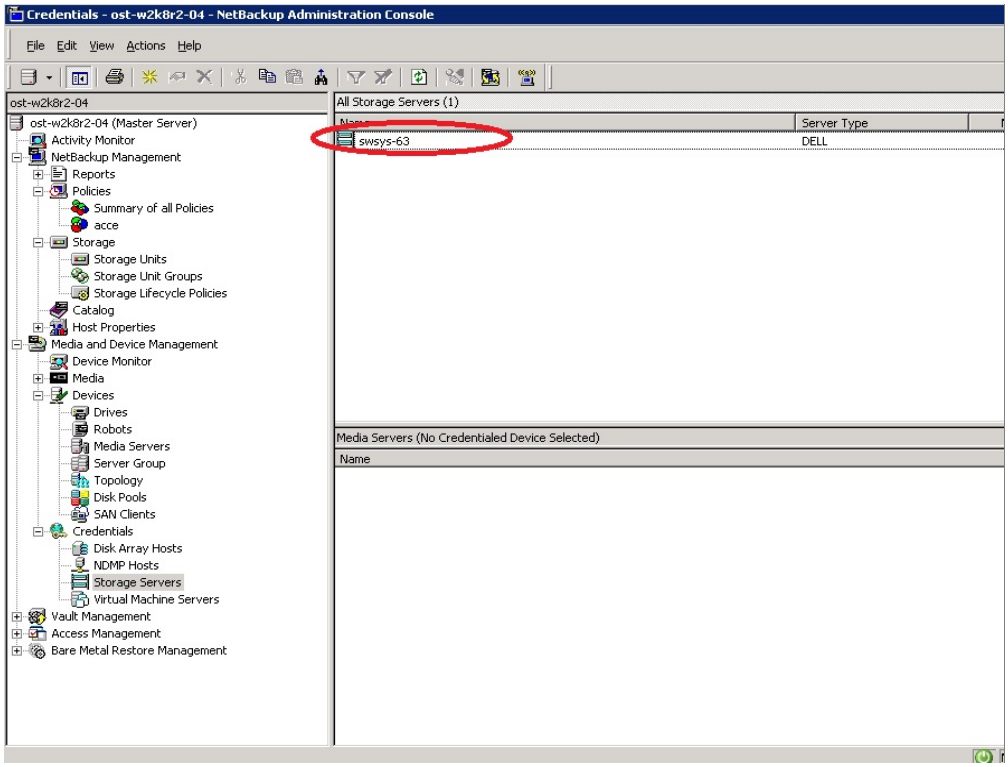
4. Under **Storage server name**, enter the DR Series system IP address or hostname, and under **Storage server type**, enter **DELL.**
5. In the **Media server** list, select the media server and enter the user name: **backup_user**, password: **St0r@ge!**



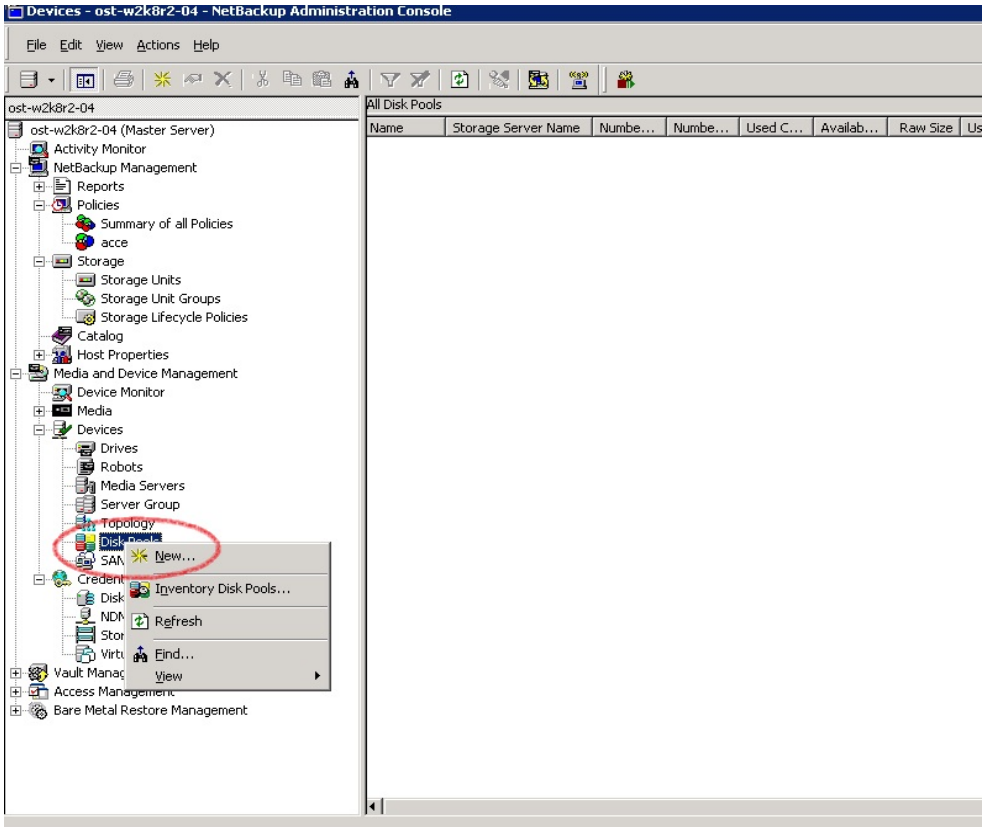
6. Make sure the storage server creation is successful and that authentication is working.



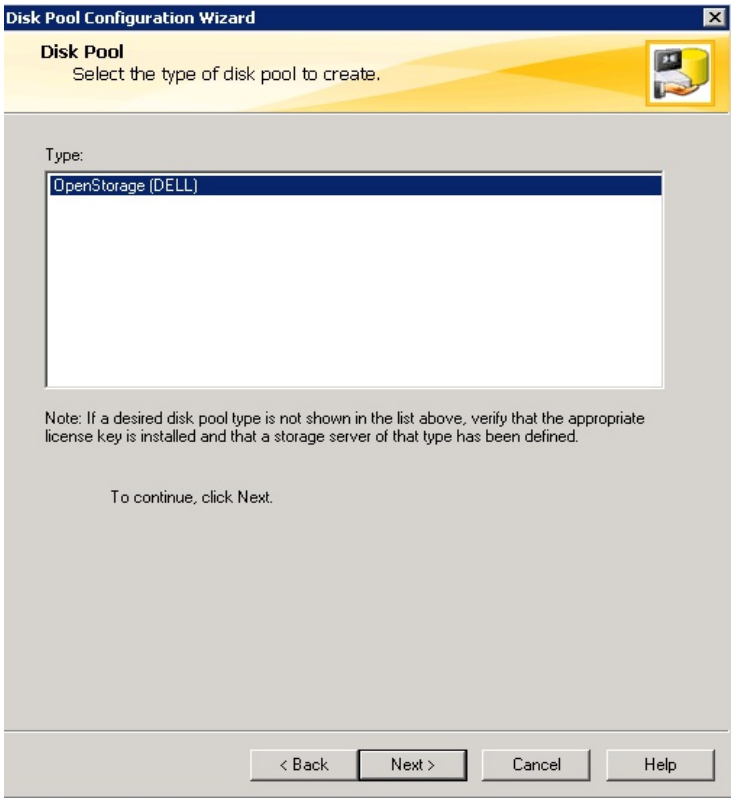
The created storage server should now be listed.



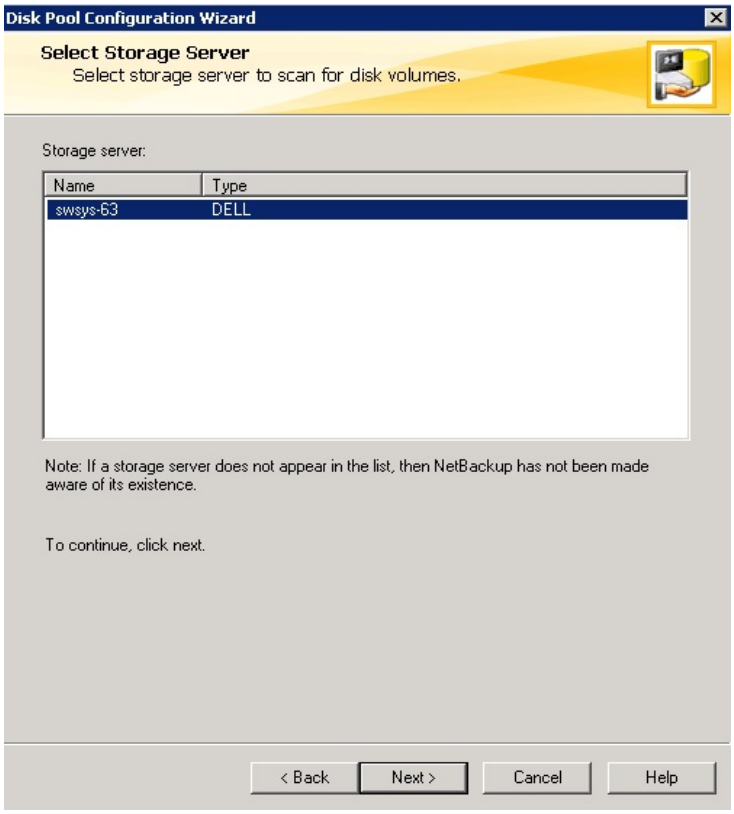
7. Right-click **Media and Device Management** and select **Devices -> Disk Pool**, and then click **New**.



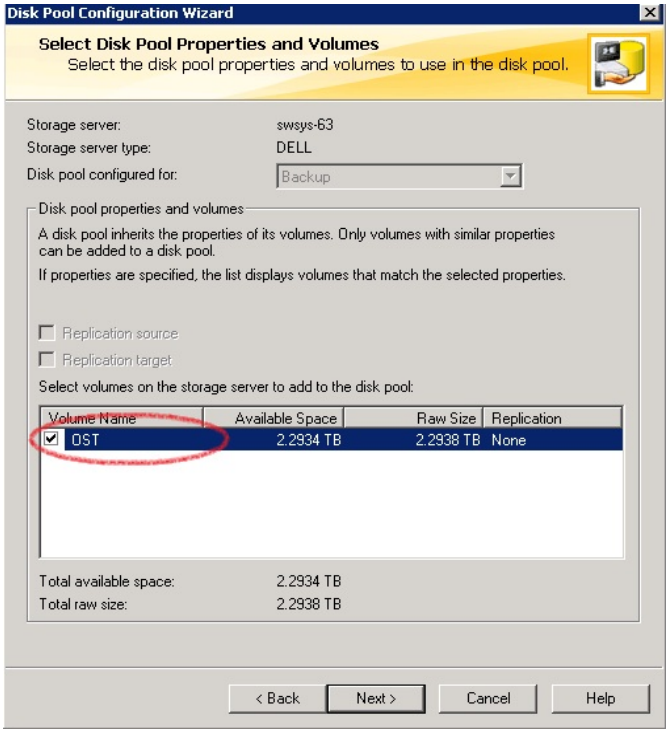
8. In the **Disk Pool Configuration Wizard** dialog box, select **OpenStorage (DELL)** for **Type**.



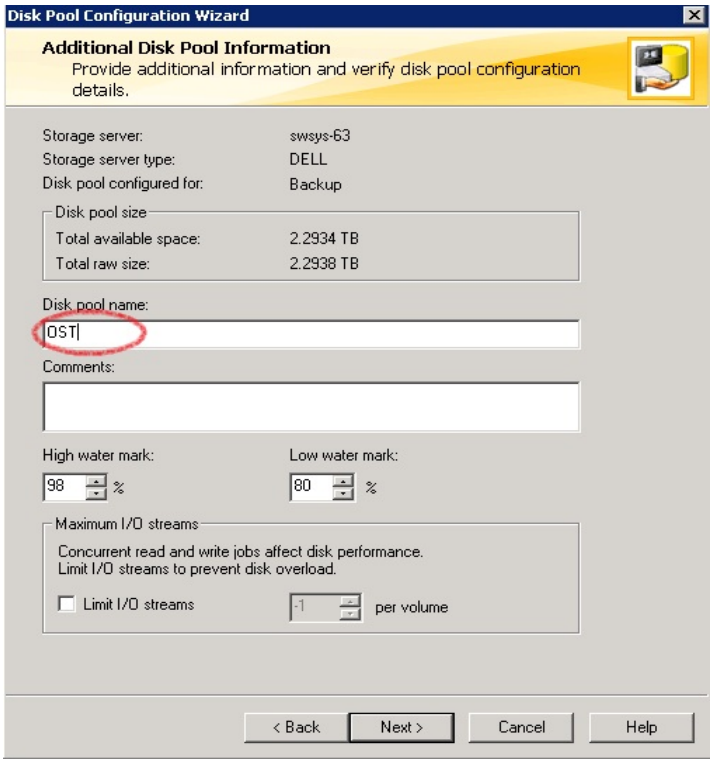
9. In the **Storage server** list, select the DR storage server created previously.



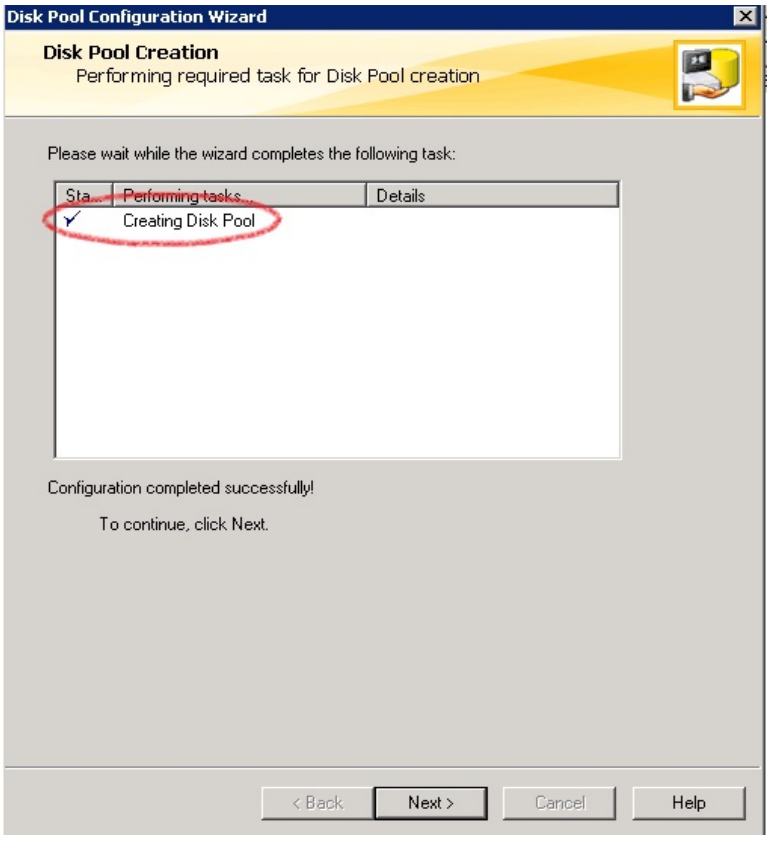
10. Select the **OST** container created previously, which will be used for backup.



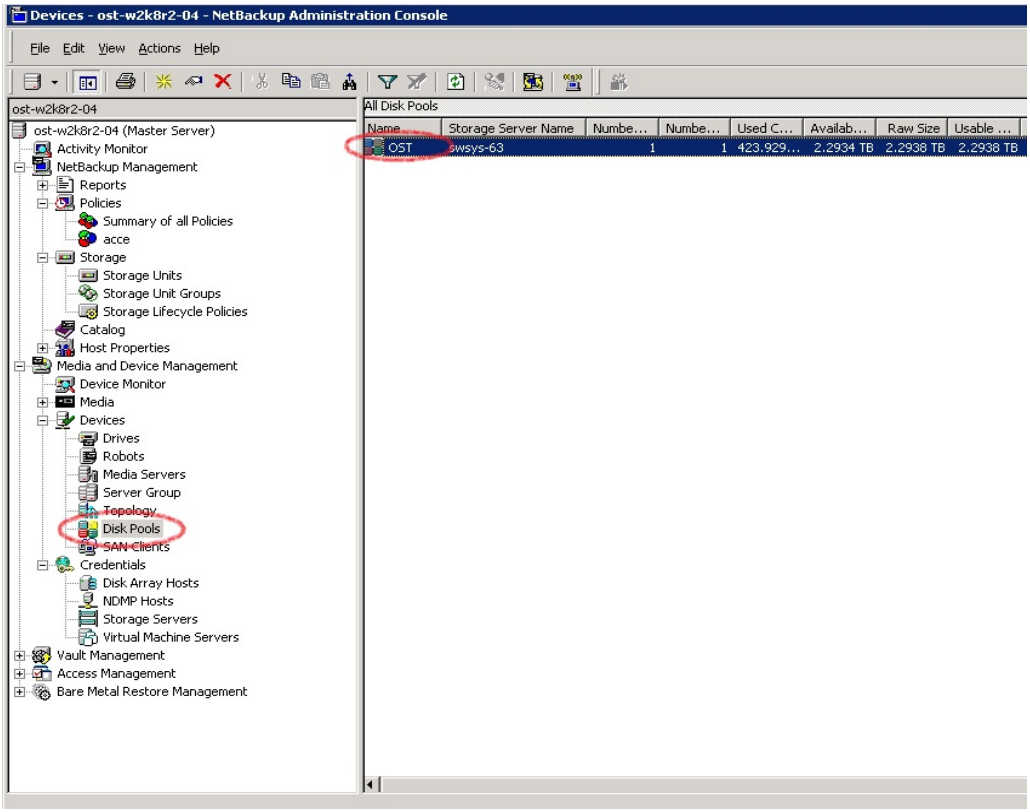
11. Enter the **Disk pool name**.



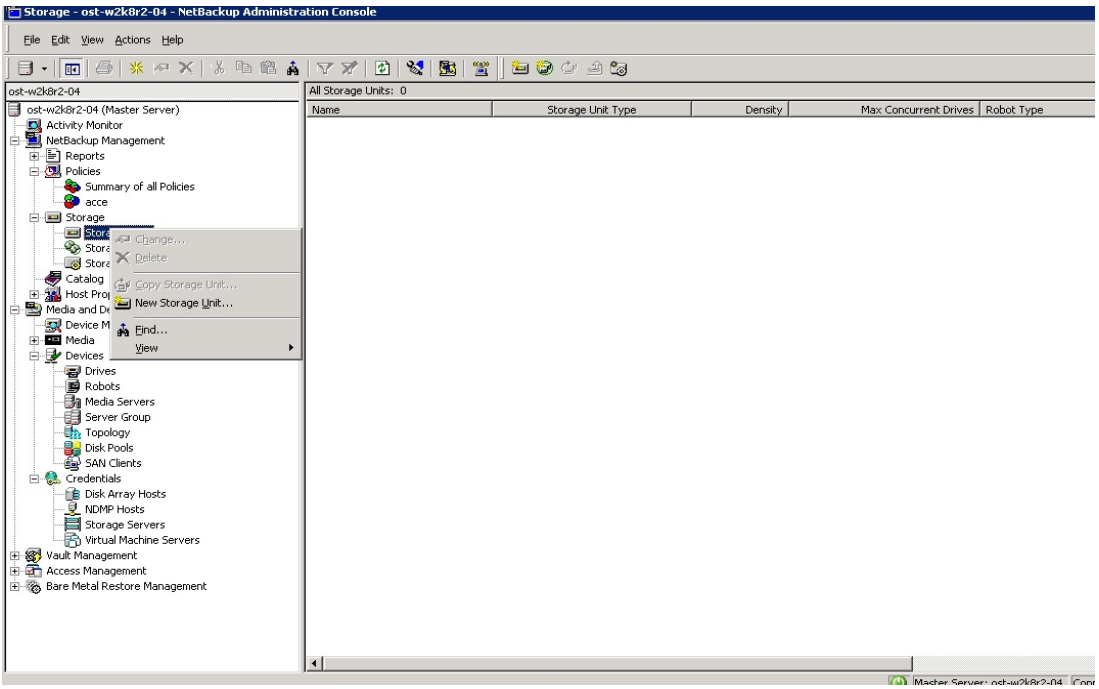
12. Confirm that disk pool creation is successful.



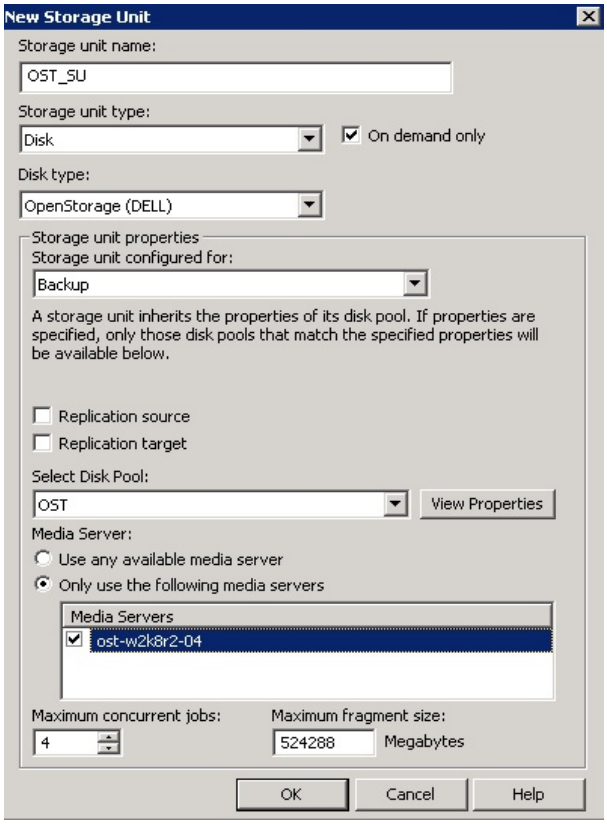
13. Make sure the disk pool is listed.



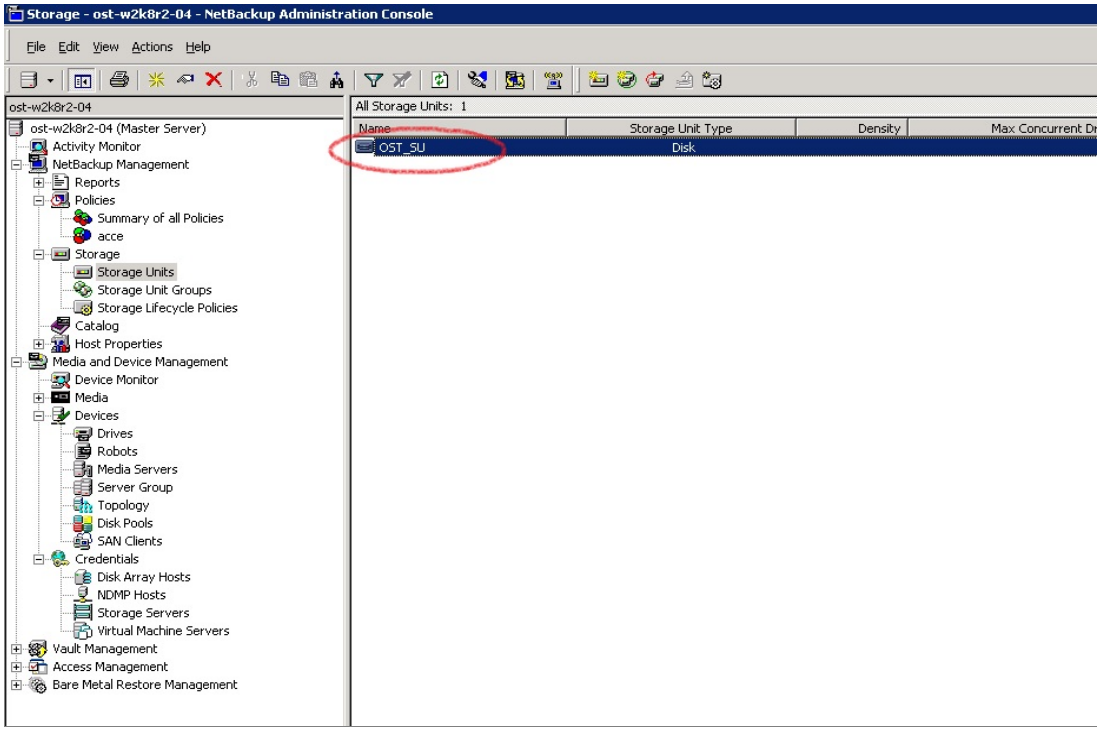
14. Right-click **NetBackup Management** and select **Storage** > **Storage Unit**, and then click **New Storage Unit**.



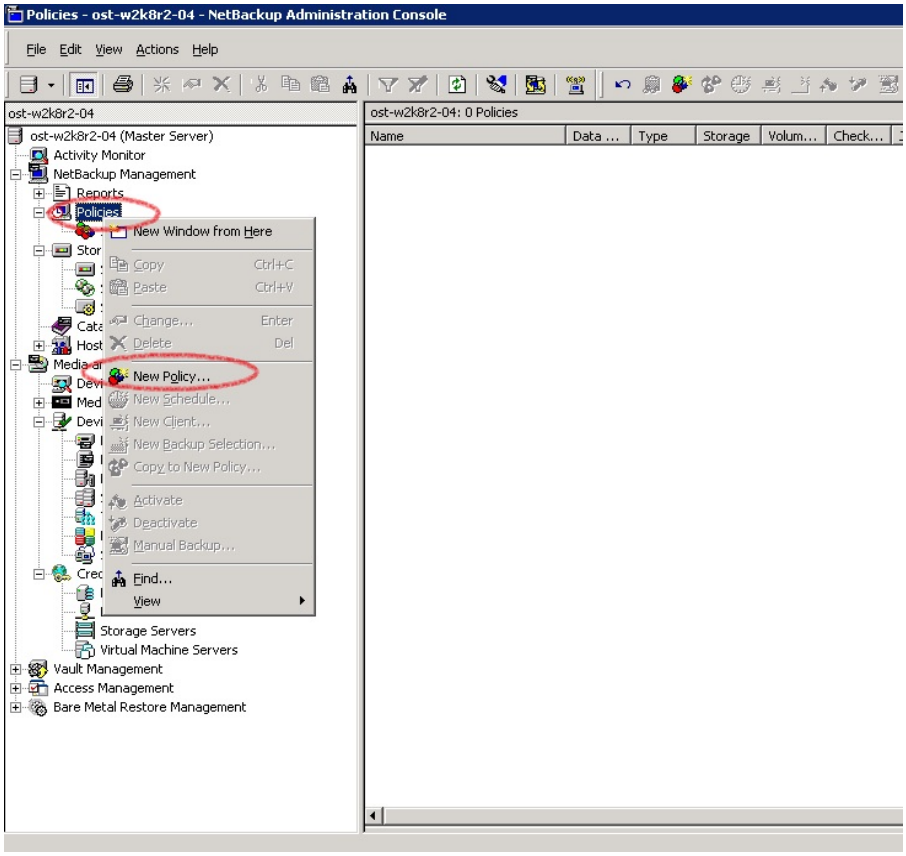
15. For the New Storage Unit, enter a **Storage unit name**, and then specify the **Storage unit type** as **Disk**, the **Disk type** as **OpenStorage (DELL)**, and **Storage unit configured for** as **Backup.** Select the disk pool that was created previous steps, and select the media server that will be used for backup.



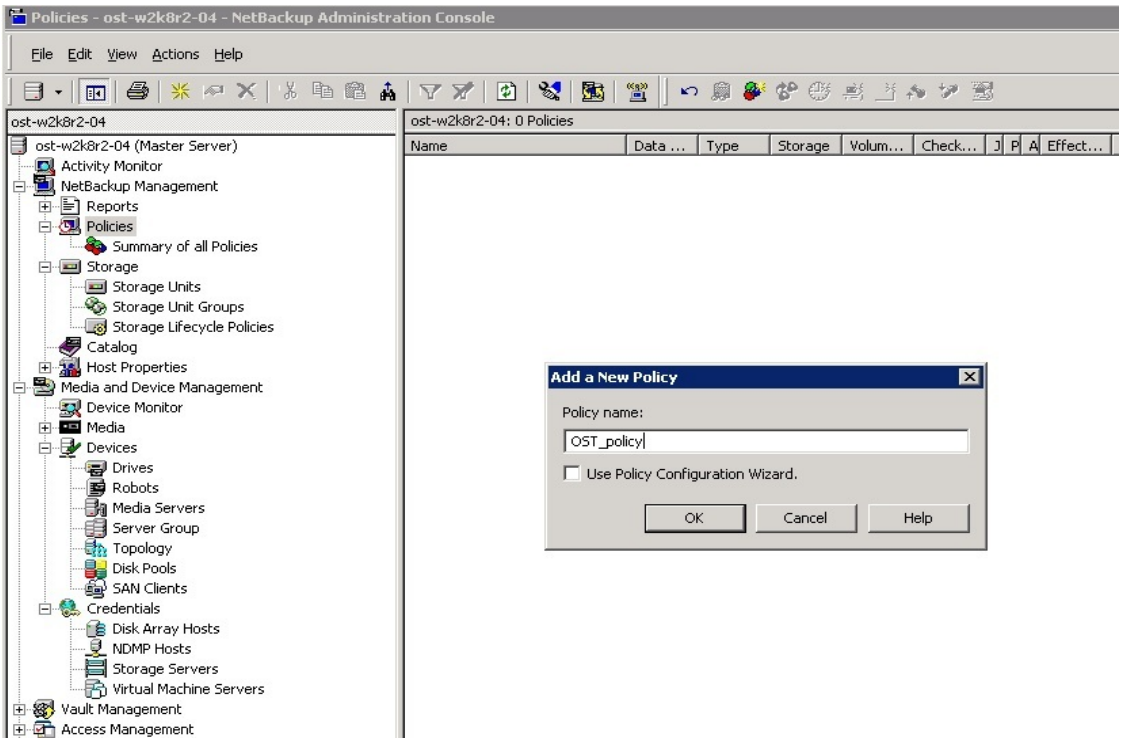
16. Make sure that the **Storage Unit** is listed after creation.



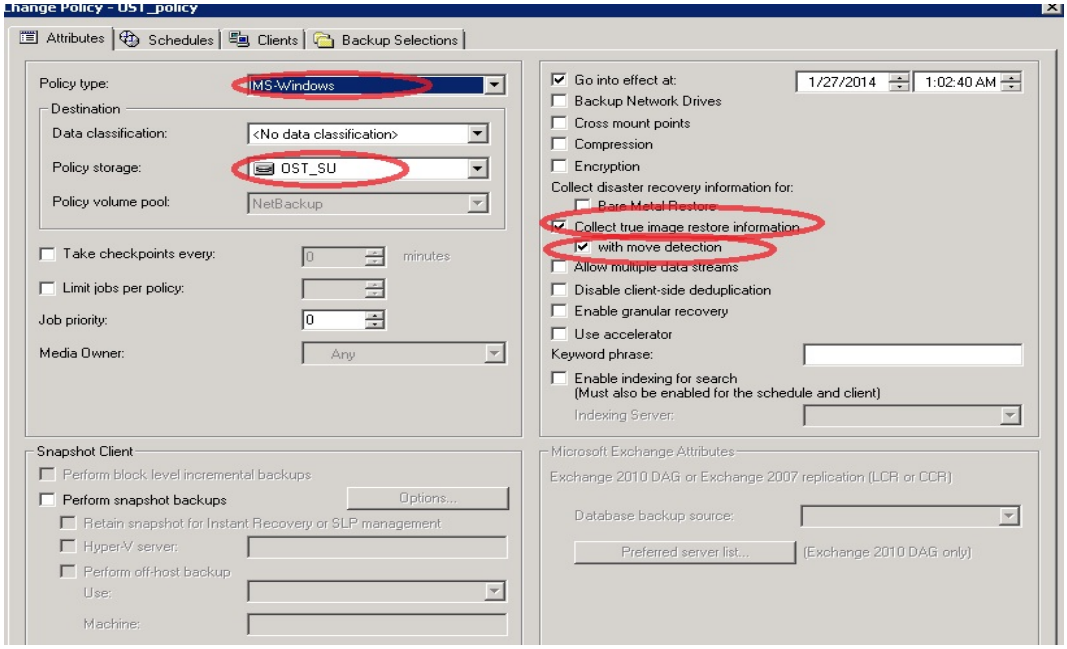
17. Right-click **Netbackup Management** > **Policies** and click **New Policy**.



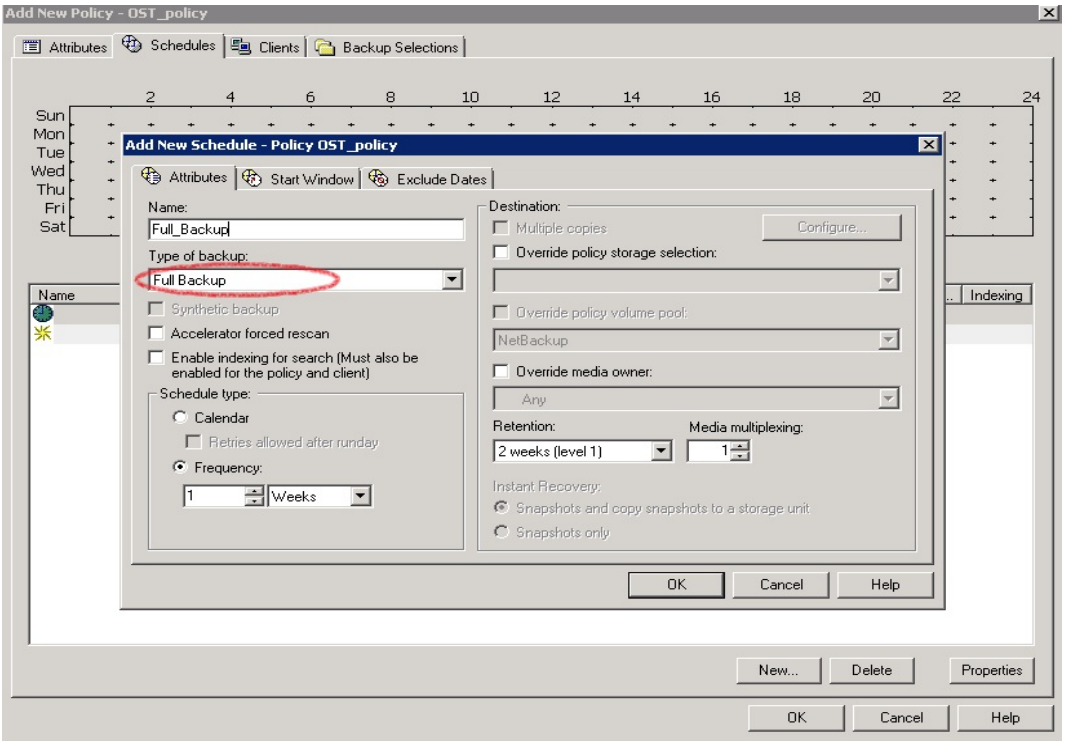
18. Enter a **Policy name**.

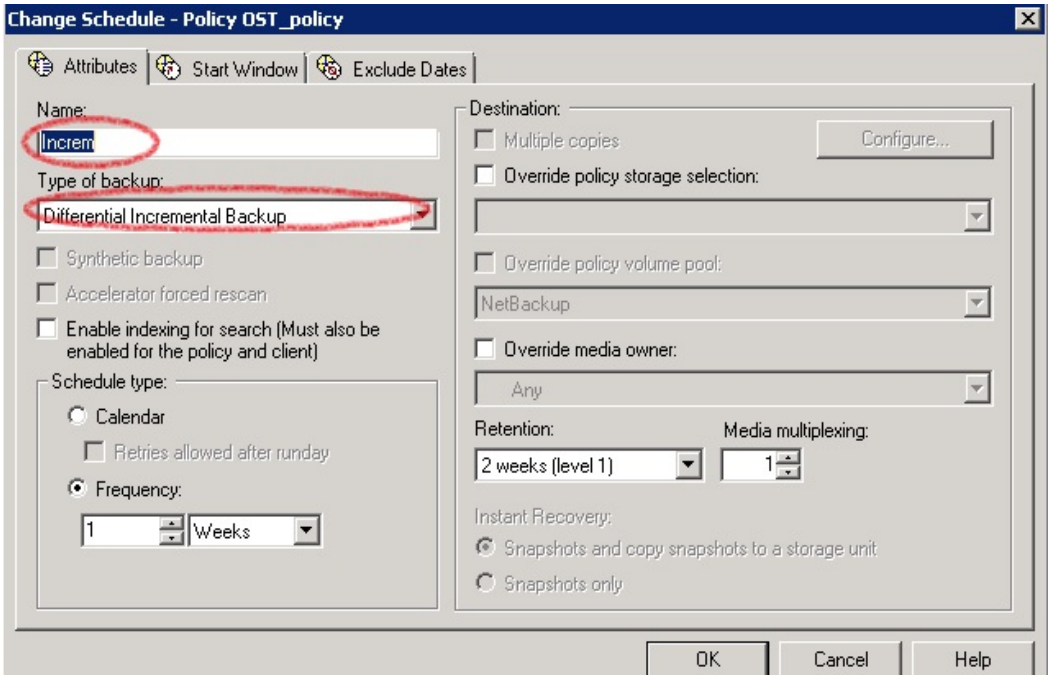


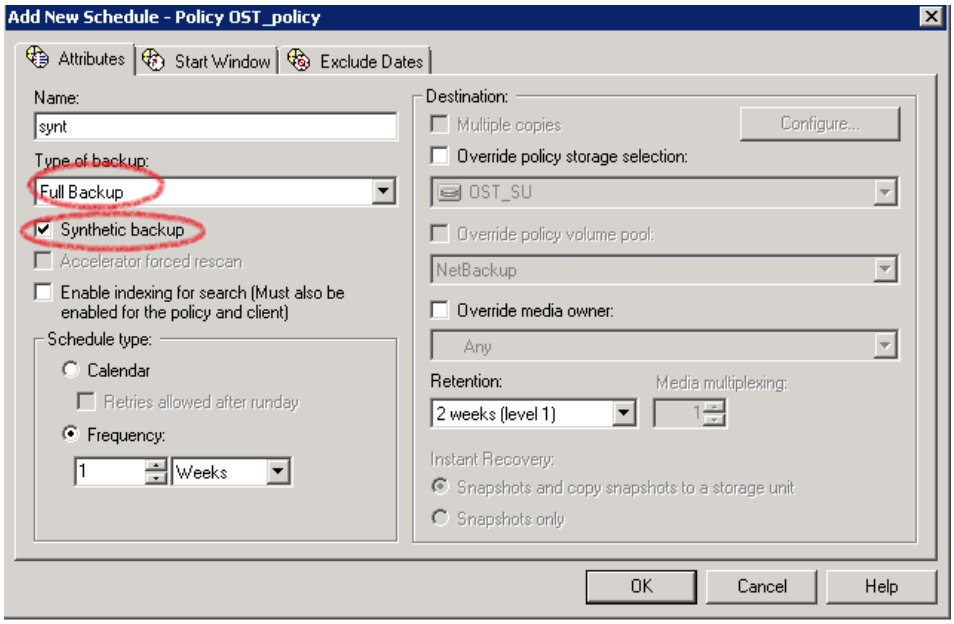
19. Enter the following policy attributes on the **Attributes** tab: **Policy type** as **MS-Windows** (for Windows) or **Standard** (for Linux); **Policy storage** as the DR storage unit that was created in previous steps; select **Collect true image restore information** > **with move detection**.



20. On the **Schedules** tab, create three schedules: one for **Full Backup**, a second one for either **Differential Incremental Backup** or **Cumulative Incremental Backup**, and a third one for **Full Backup** with the **Synthetic backup** option enabled.
    The schedule should be set so that first a full backup runs, then an incremental backup, and finally a synthetic full backup.


Add New Policy - OST_policy
Attributes
Schedules
Clients
Backup Selections
Add New Schedule - Policy OST_policy
Attributes
Start Window
Exclude Dates
Name:
Full_Backup
Type of backup:
Full Backup
Synthetic backup
Accelerator forced rescan
Enable indexing for search (Must also be enabled for the policy and client)
Schedule type:
Calendar
Retries allowed after runday
Frequency:
1
Weeks
Destination:
Multiple copies
Configure...
Override policy storage selection:
Override policy volume pool:
NetBackup
Override media owner:
Any
Retention:
2 weeks (level 1)
Media multiplexing:
1
Instant Recovery:
Snapshots and copy snapshots to a storage unit
Snapshots only
OK
Cancel
Help
New...
Delete
Properties
OK
Cancel
Help

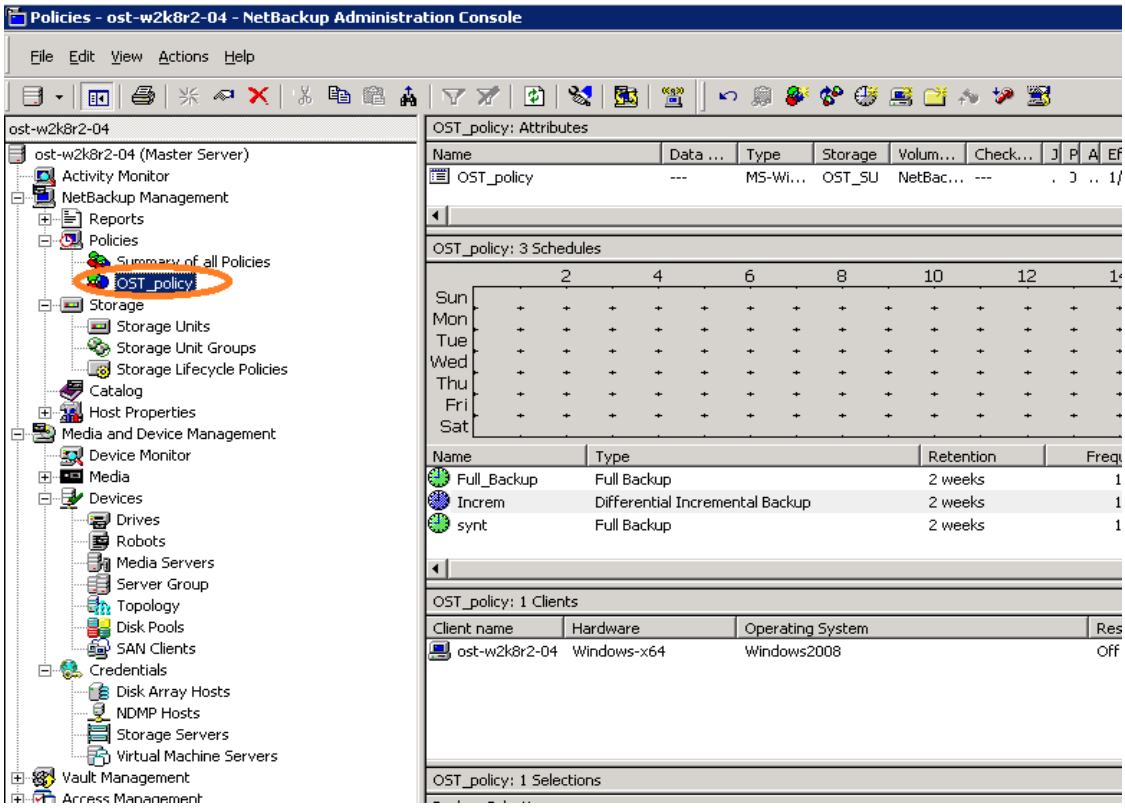

Change Schedule - Policy OST_policy
Attributes
Start Window
Exclude Dates
Name:
Increm
Type of backup:
Differential Incremental Backup
Synthetic backup
Accelerator forced rescan
Enable indexing for search (Must also be enabled for the policy and client)
Schedule type:
Calendar
Retries allowed after runday
Frequency:
1
Weeks
Destination:
Multiple copies
Configure...
Override policy storage selection:
Override policy volume pool:
NetBackup
Override media owner:
Any
Retention:
2 weeks (level 1)
Media multiplexing:
1
Instant Recovery:
Snapshots and copy snapshots to a storage unit
Snapshots only
OK
Cancel
Help



21. On the **Clients** tab, select the client(s) from which data is backed up.

22. On the **Backup Selection** tab, provide the data set that needs to be backed up.

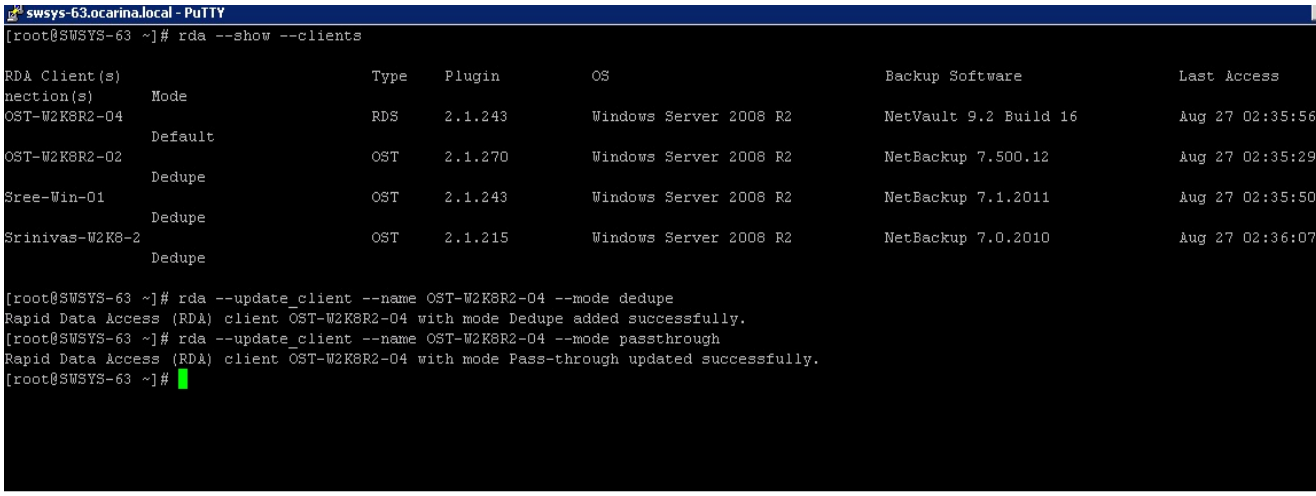
23. Make sure that the policy is created successfully.



24. Activate the policy before proceeding to backup. Right-click the policy and click **Activate**.

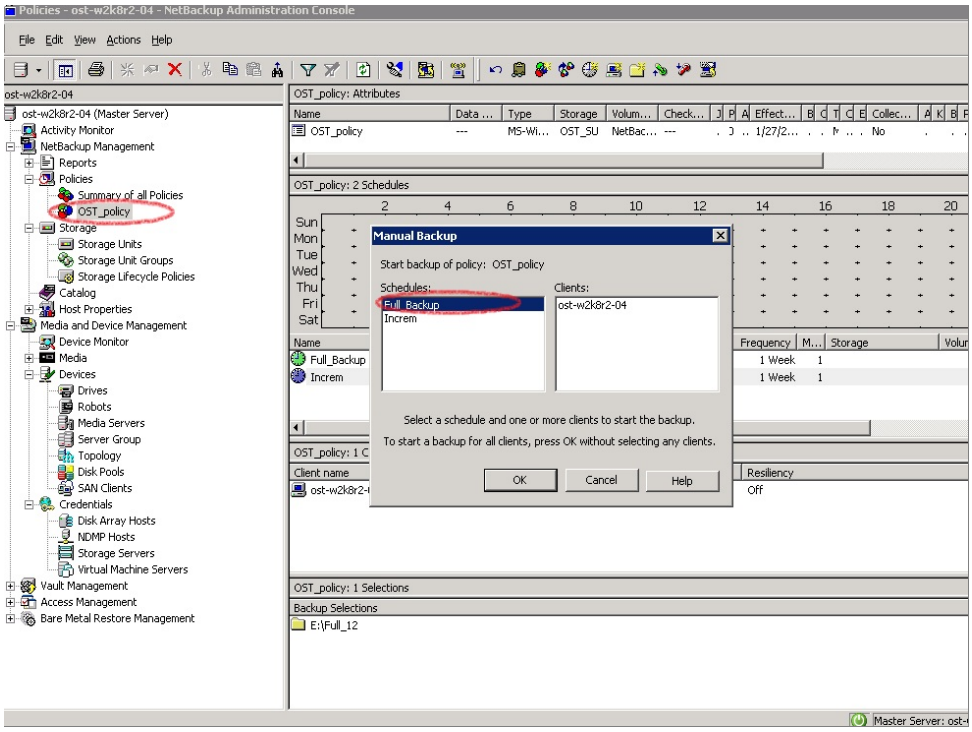
3.1.2 Backing up using NetBackup virtual synthetic backup

1. Before running backup, ensure that you have decided on a backup mode to use: **Passthrough** or **Dedupe**. This can be done by setting the RDA mode in the DR Series system command line interface (CLI), as shown in the following example screenshot.

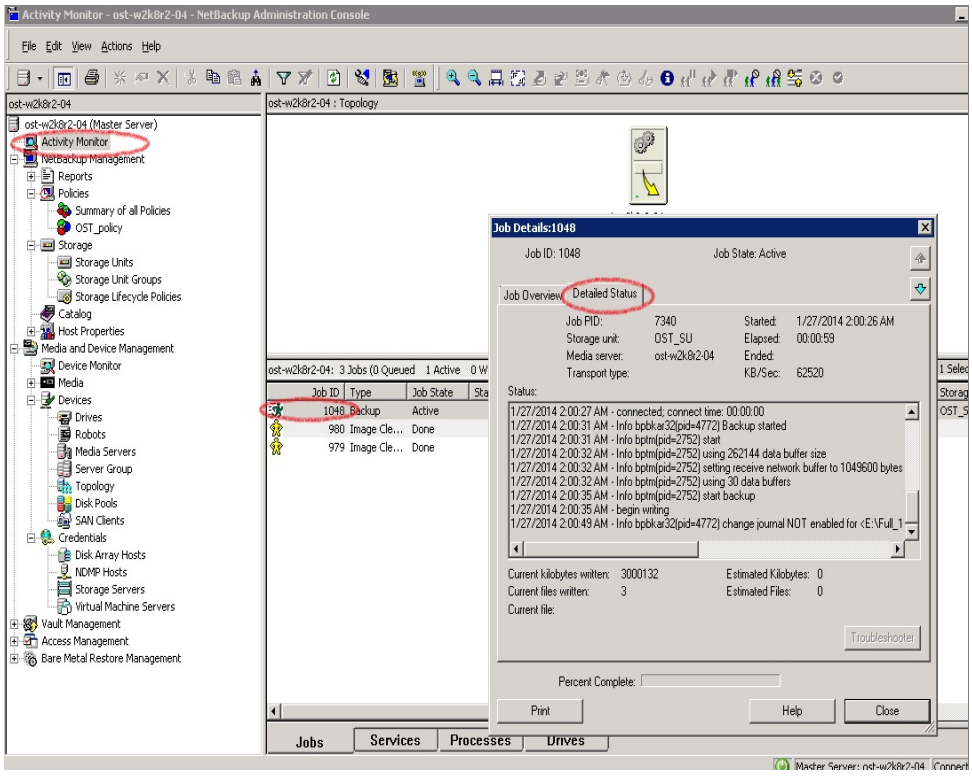


Note: You can schedule the backups or run them at a convenient time. This procedure uses a manual backup configuration.

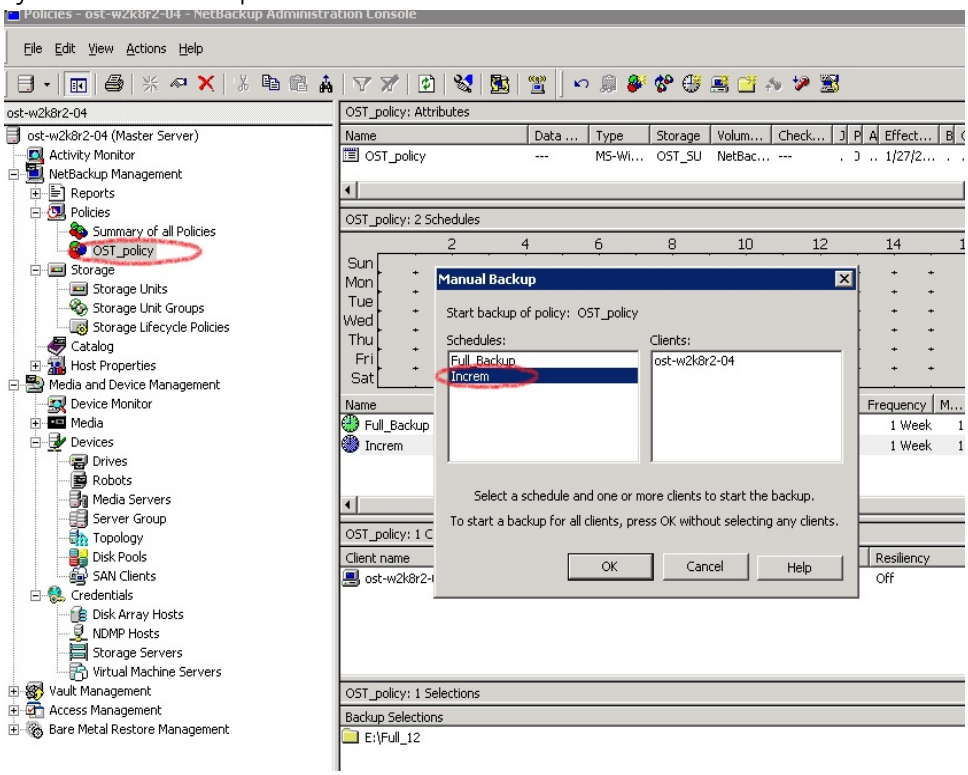
2. Under **Netbackup Management** > **Policies**, right-click the policy created in the previous procedure and select **Manual Backup** to run the backup manually.



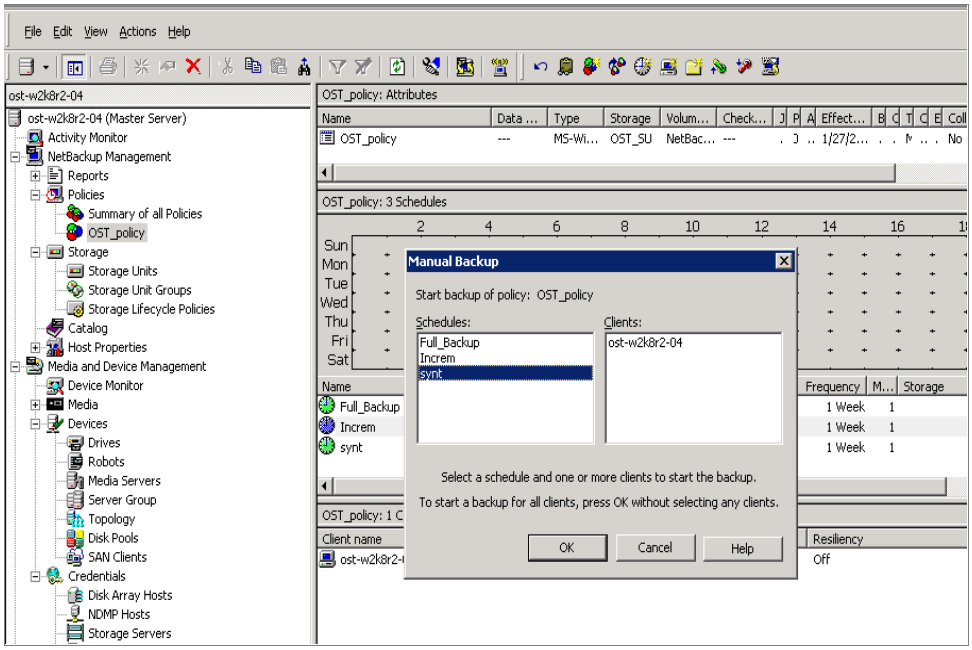
3. Run a manual **Full Backup** and check the status in the Activity Monitor. Double-click the job to see the detailed status.



4. Run one or more configured **Incremental** backups to generate a set of backups that can make a synthetic full backup.

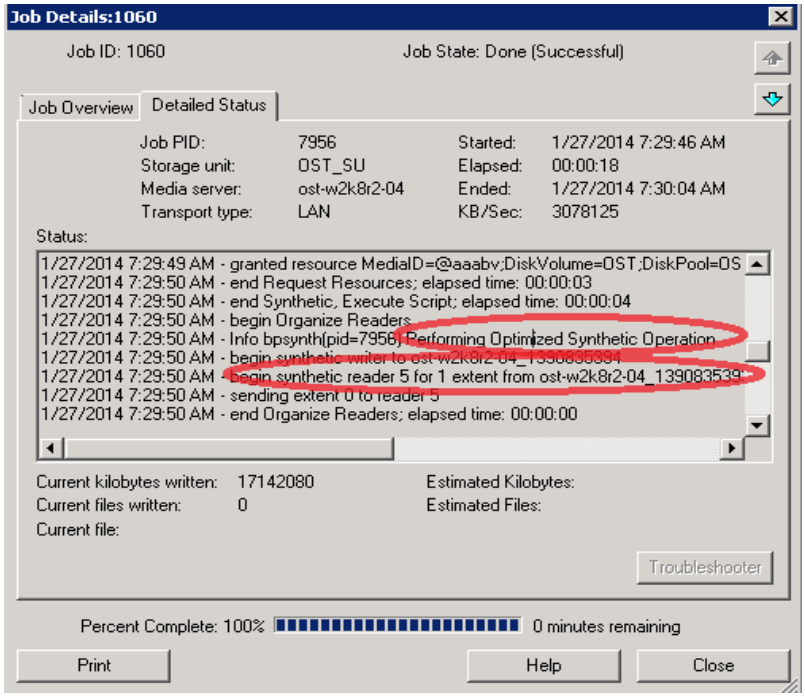


5. Then, run a **Full Backup** with the **synthetic backup** option enabled.



6. Confirm that the final full backup is synthesized.

Note: The throughput of the final backup should be much faster as it synthesizes the full and incremental backups.



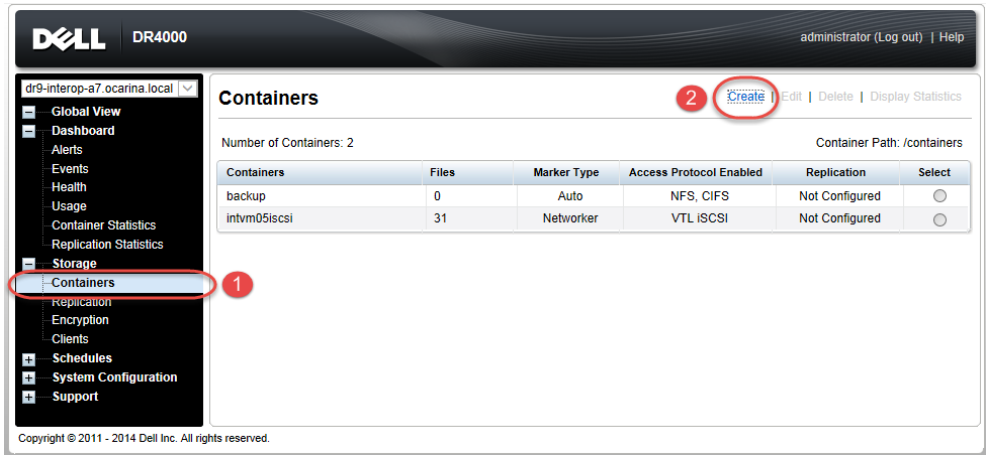
4 Configuring VTL type containers for use with Symantec NetBackup

4.1 Creating and configuring NDMP target container(s) for NetBackup

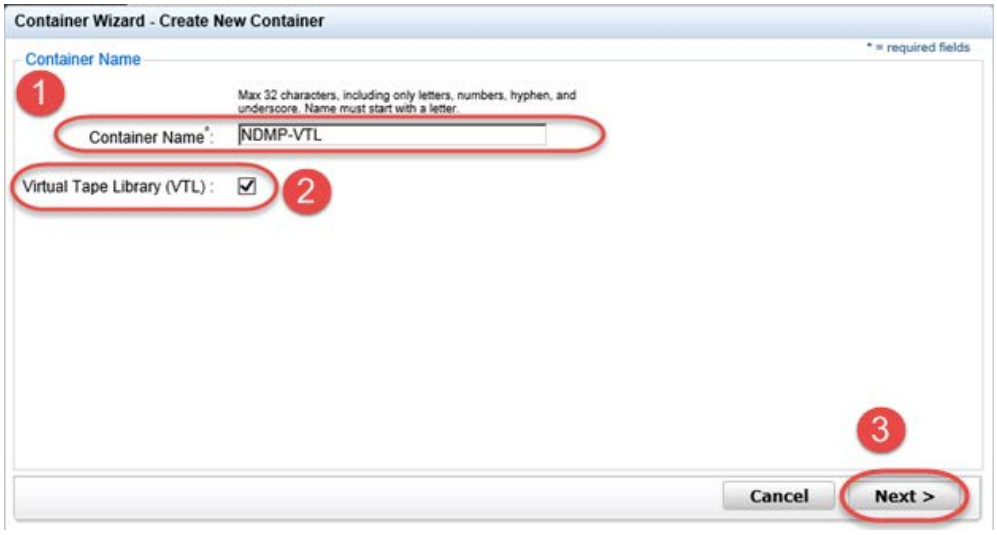
4.1.1 Creating the NDMP VTL container

Before you begin, ensure that the NetBackup OEM patch is installed. Contact Dell Support for the instructions.

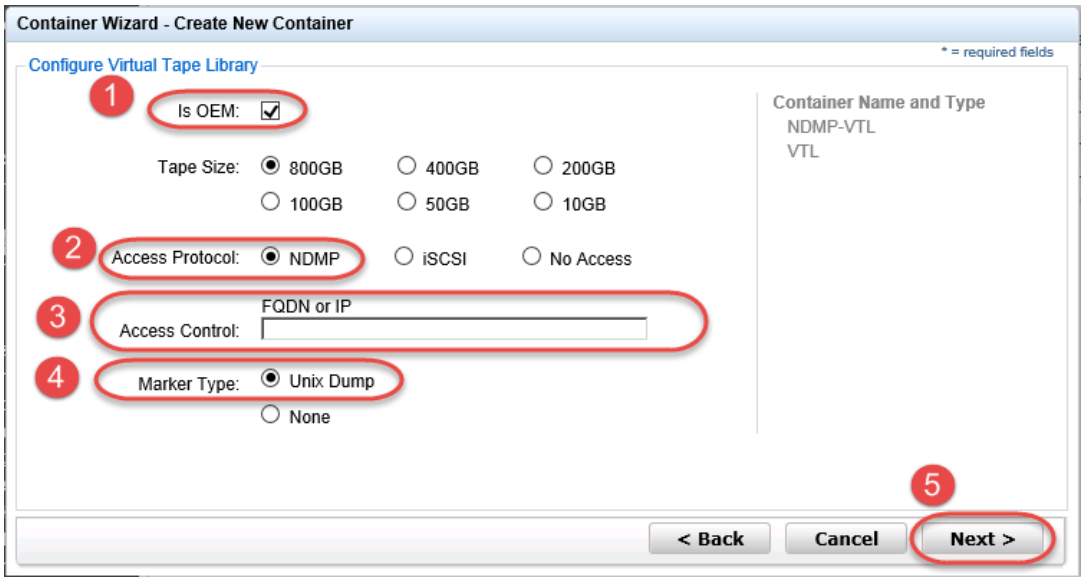
1. Create a VTL container in the DR Series system GUI by selecting **Containers** in the left navigation area, and then clicking **Create** at the top of the page.



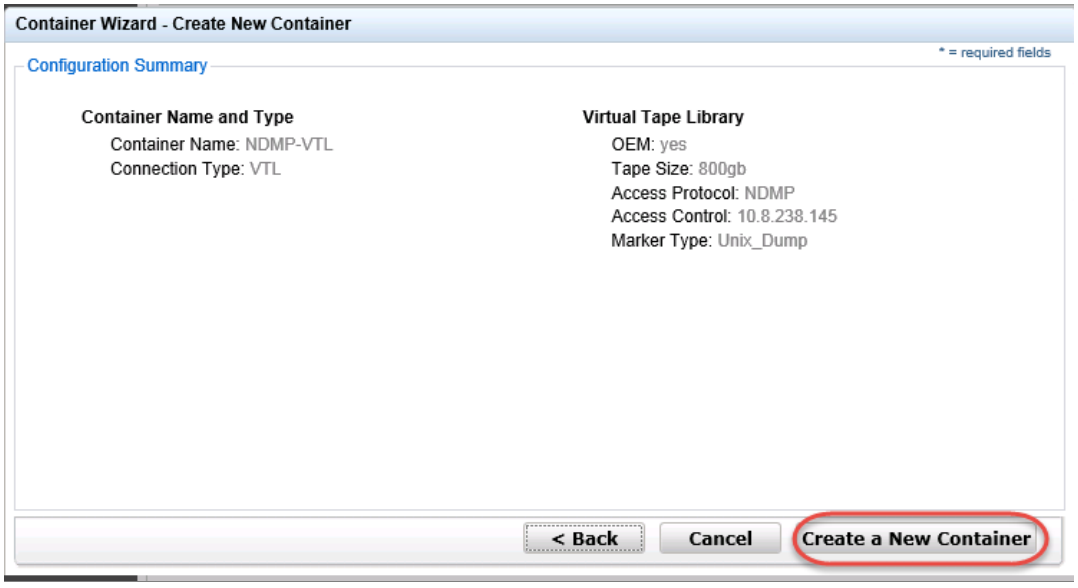
2. Enter a container name, select the **Virtual Tape Library (VTL)** check box, and then click **Next**.



3. Select the **Is OEM** checkbox, **NDMP Access Protocol** radio button, **Unix Dump Marker Type** and enter the **Access Control** IP address. Click **Next**.

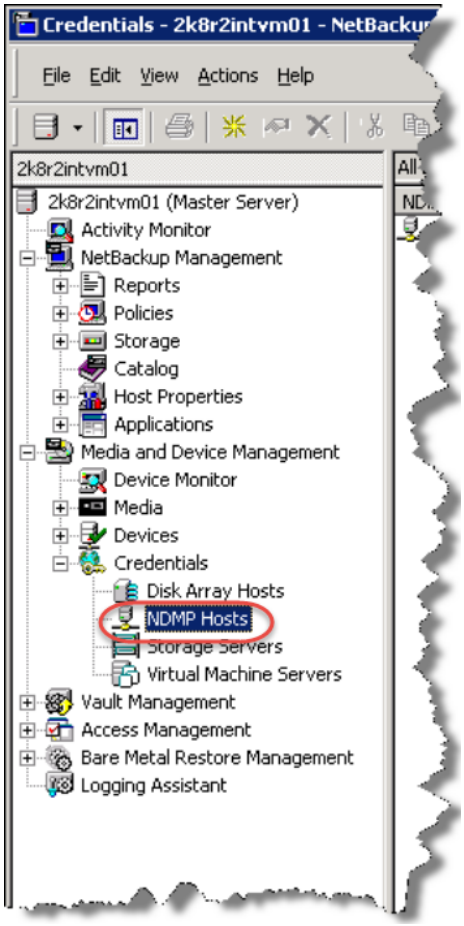


4. Click **Create a New Container** to finish container creation.

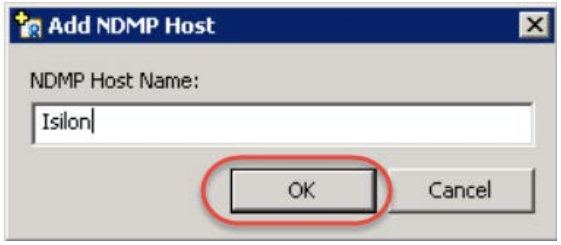


4.1.2 Setting up NetBackup to use the newly created NDMP VTL

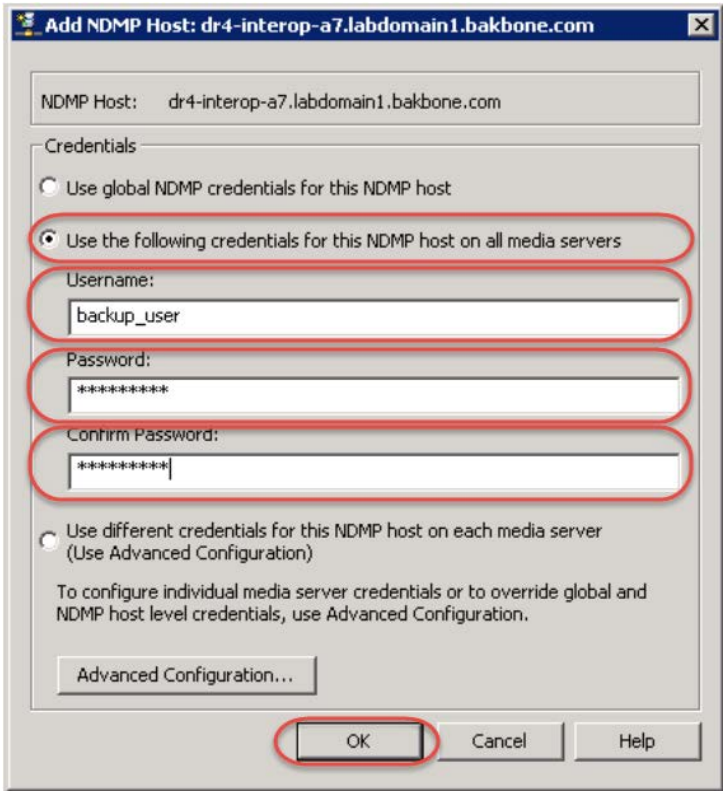
1. Open the NetBackup Administration Console, go to **Media and Device Management** > **Credentials**, right-click **NDMP Hosts**, and select **New**.



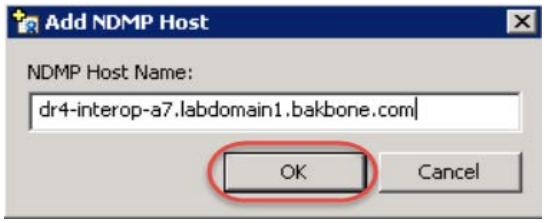
2. Enter the NDMP host name of the filer from which you want to back up and click **OK**.



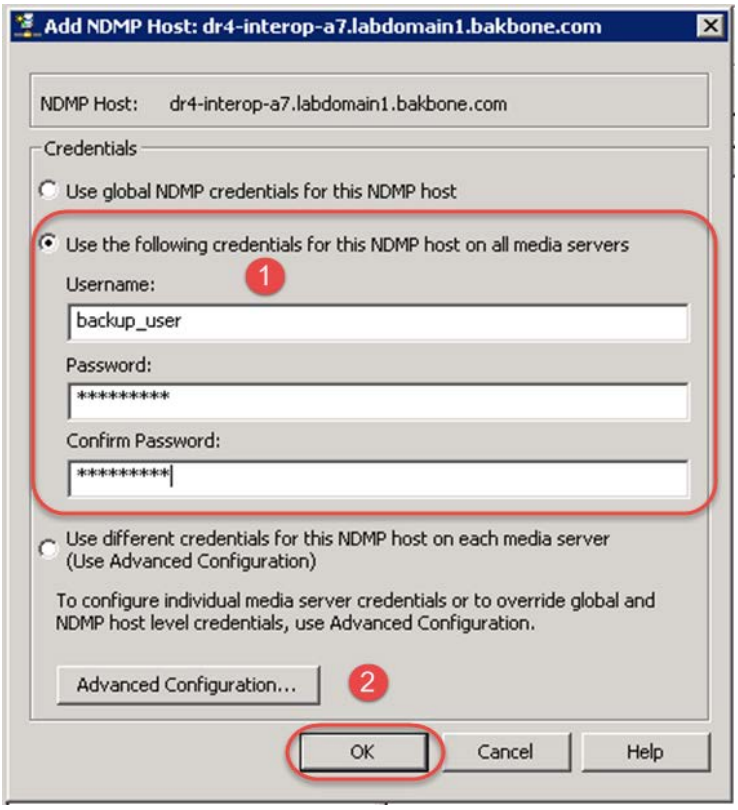
3. Enter the backup user logon information for the filer and click **OK**.



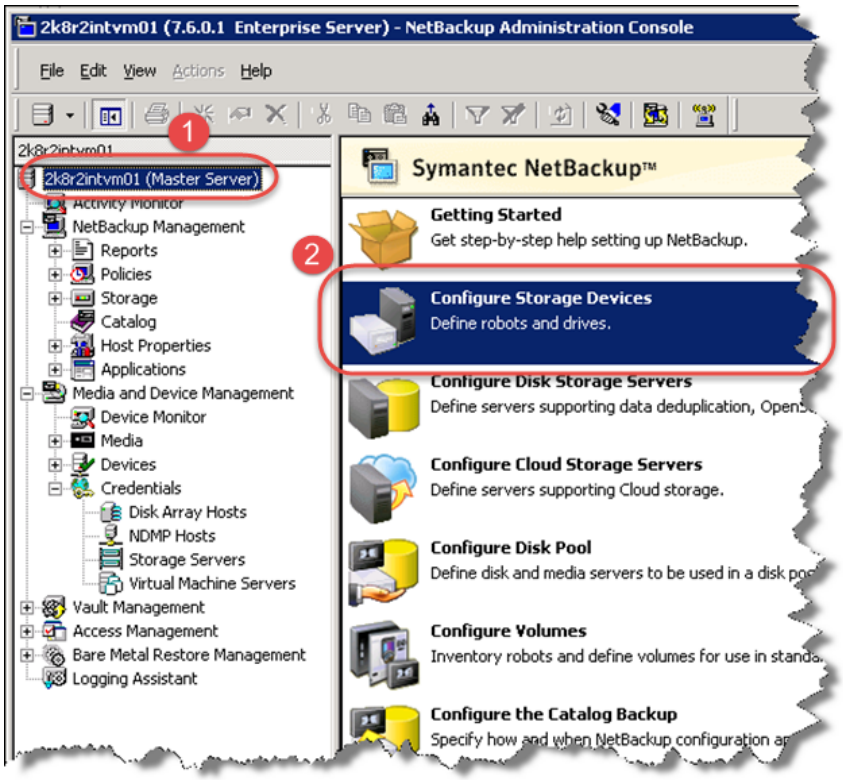
4. Click Add again and specify the DR Series system host name and click OK.



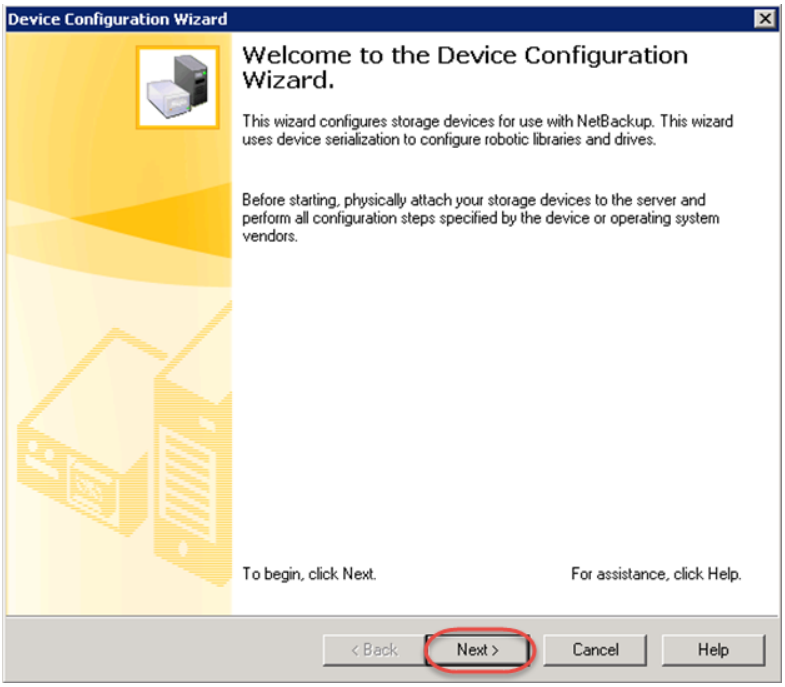
5. Enter the backup user logon information for the DR Series system, and click **OK**.



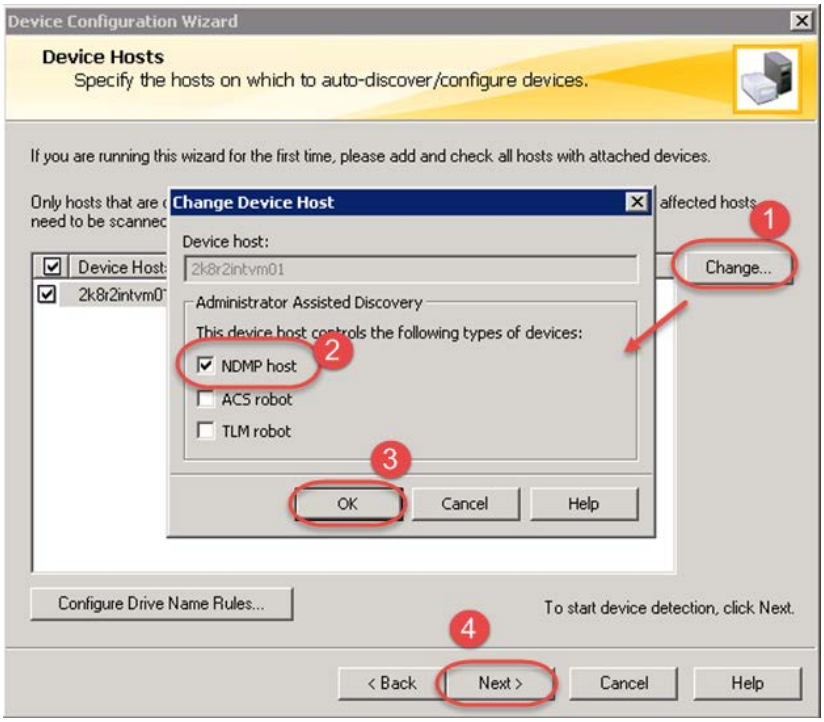
6. Click the master server in the navigation pane, and then click **Configure Storage Devices**.



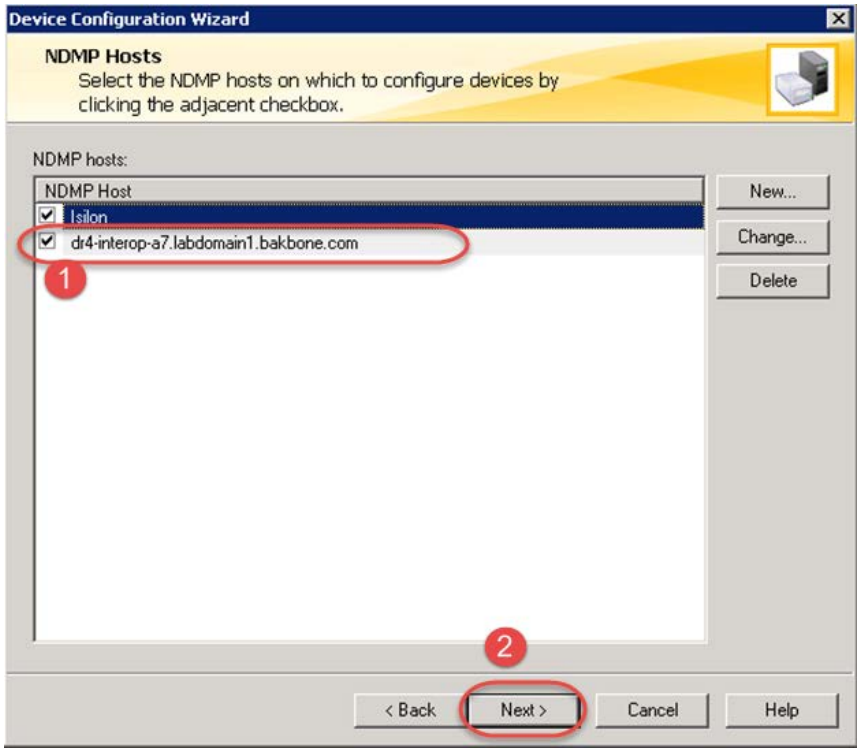
7. Click **Next>**.



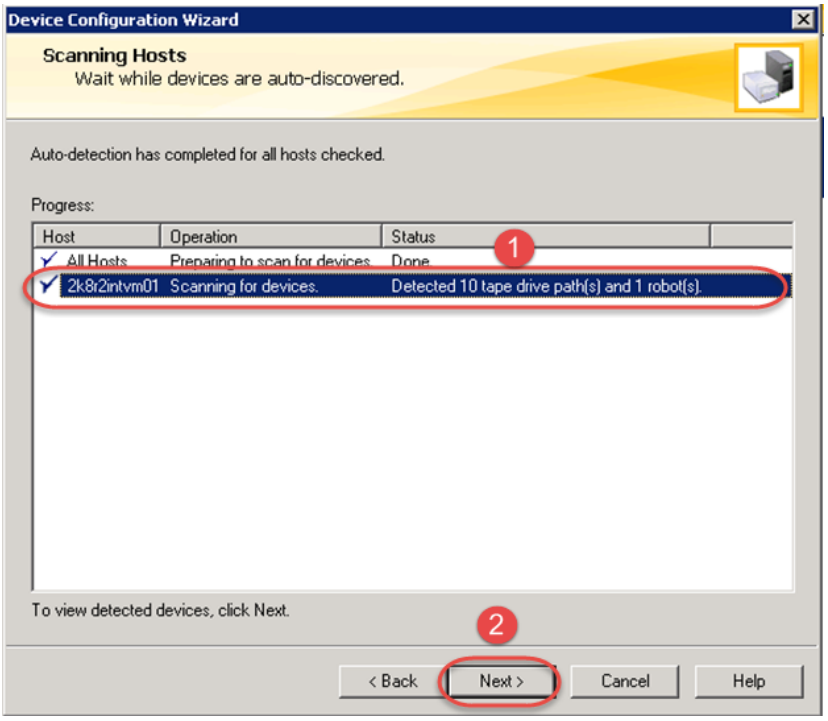
8. Click **Change**, select the **NDMP Host** check box, and click **OK**. Click **Next>**.



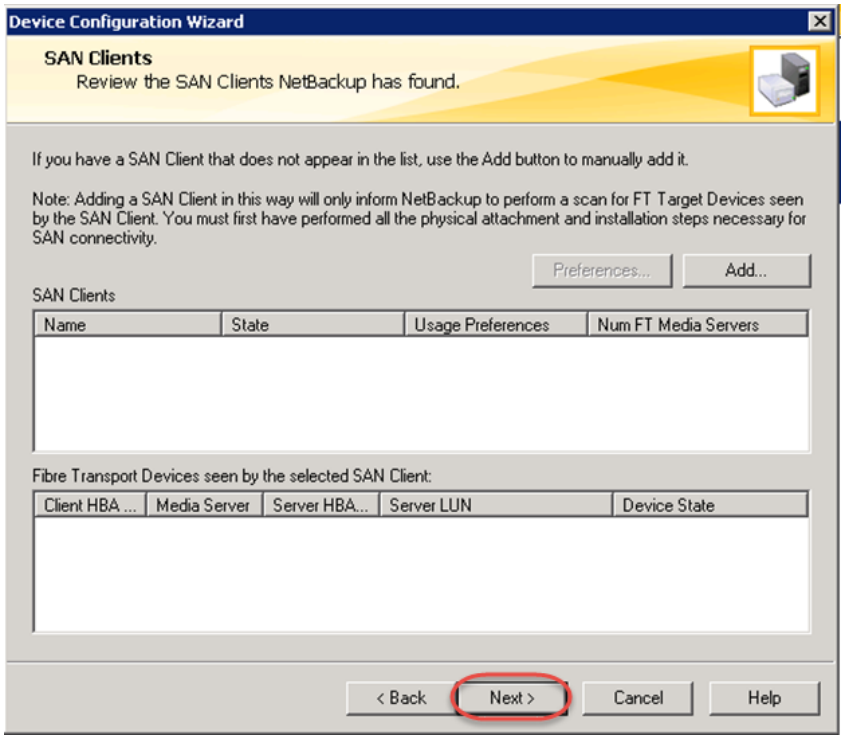
9. Ensure that the DR's host name is selected and click **Next**.



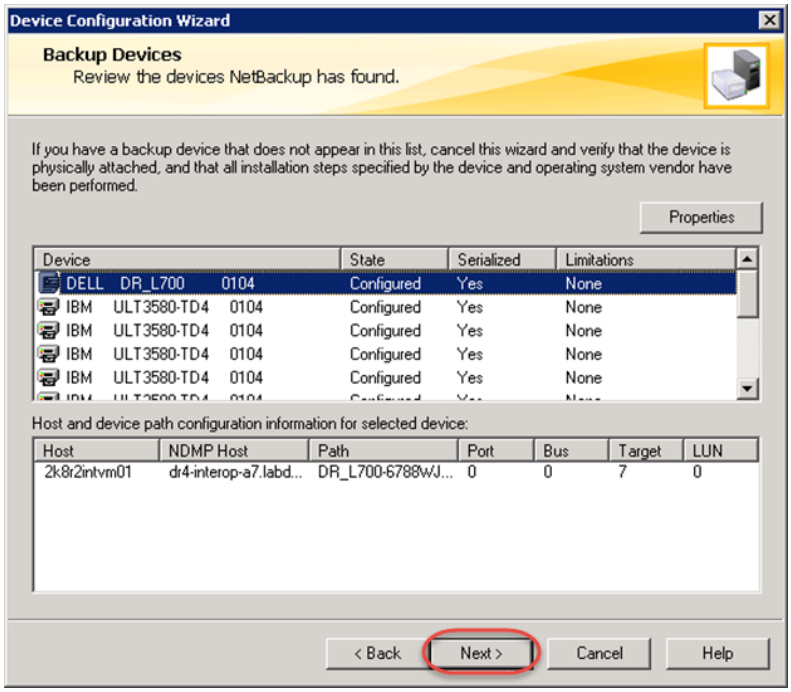
10. Verify that the VTL was detected successfully and click **Next**.



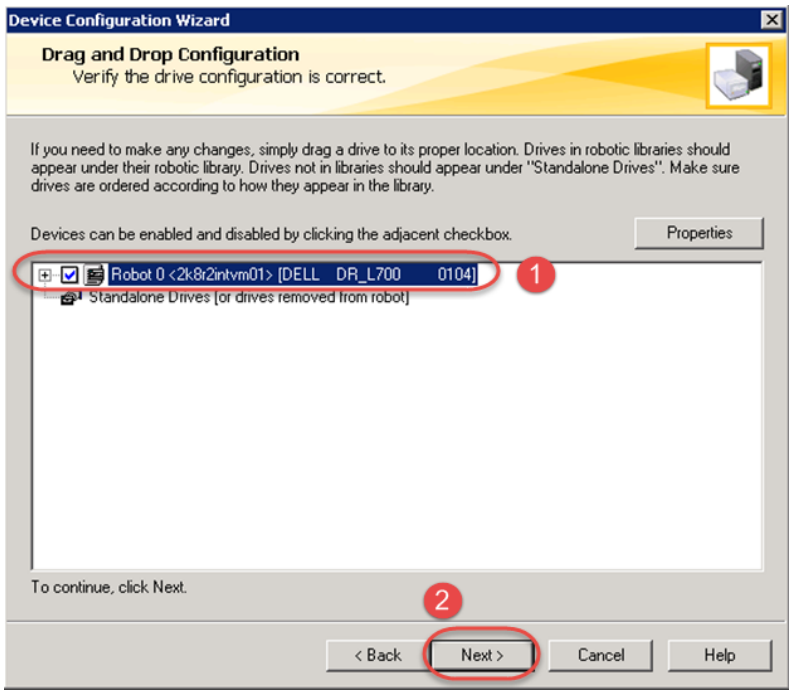
11. Click **Next**.



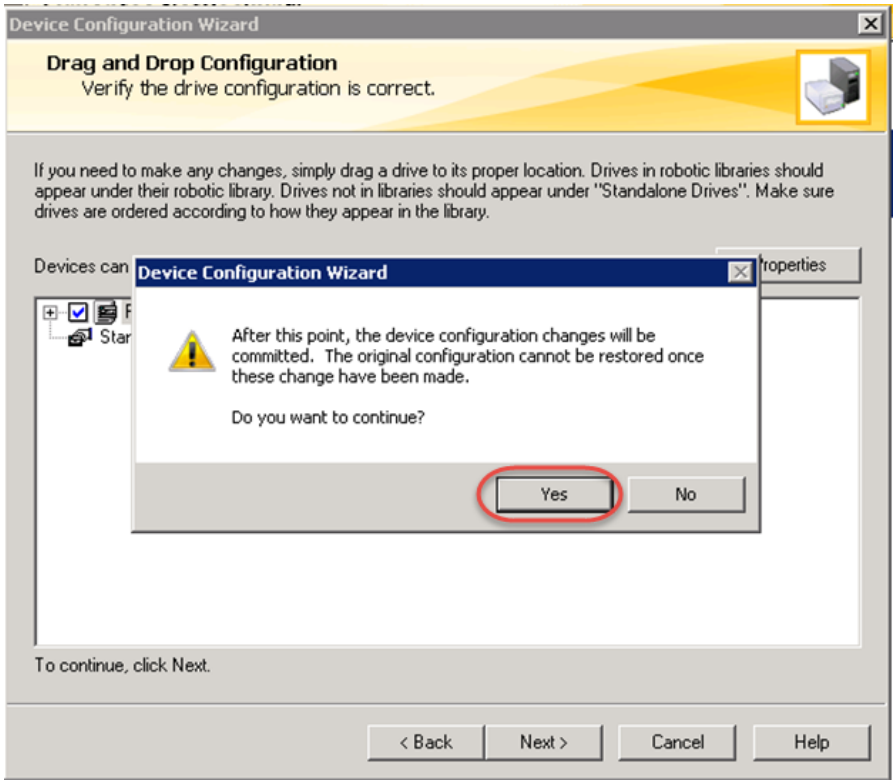
12. Click **Next**.



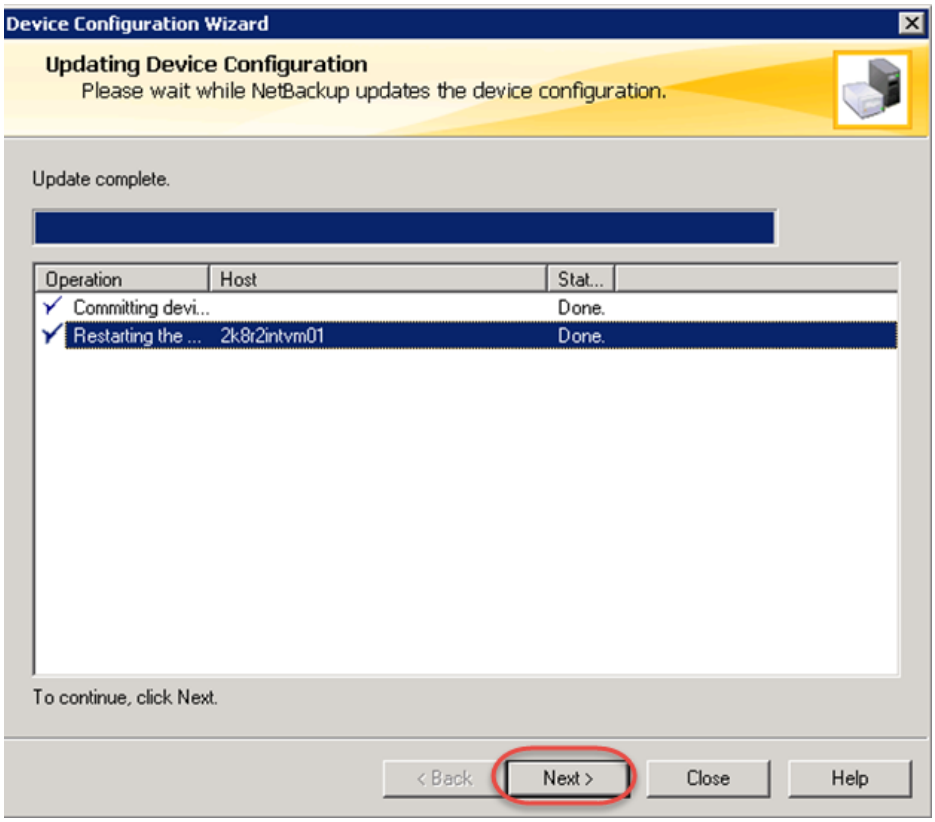
13. Click **Next**.



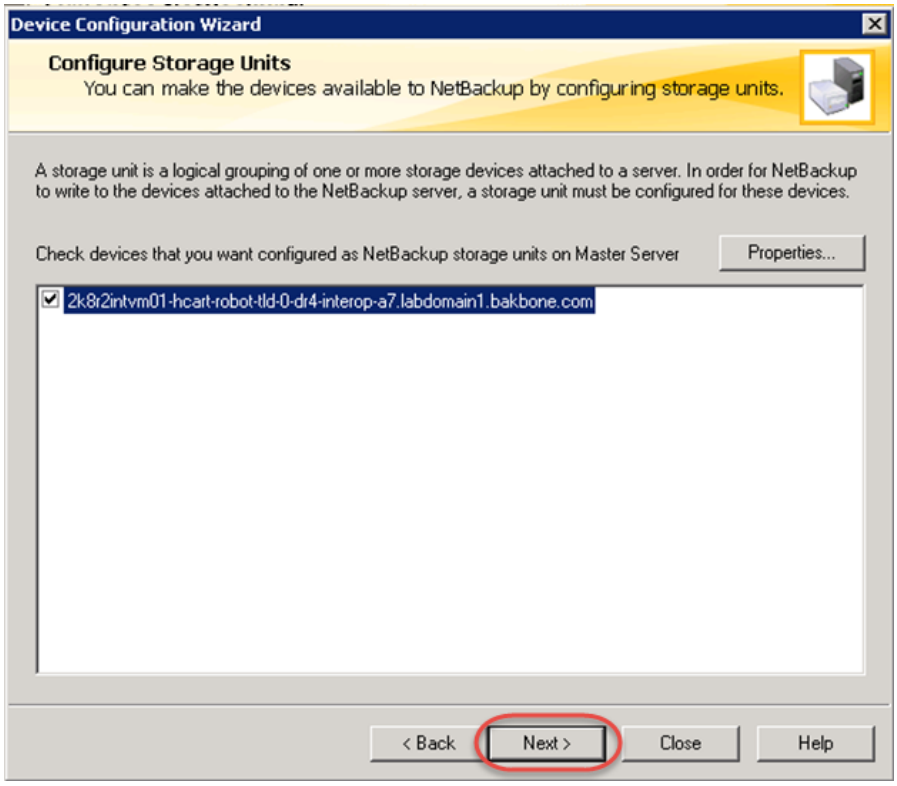
14. Click **Yes** to confirm you want to continue.



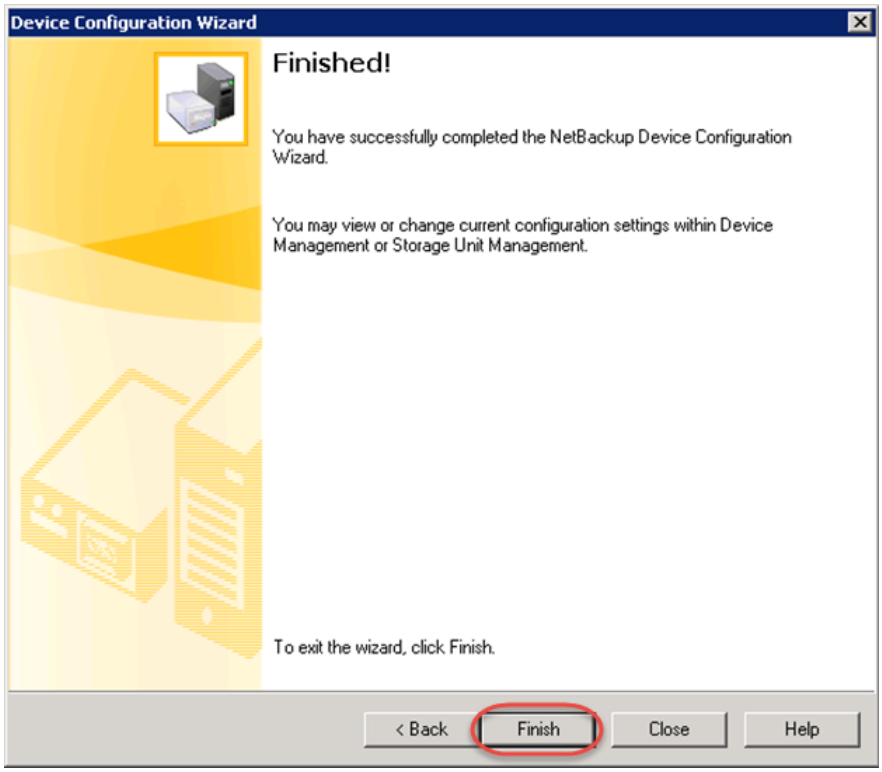
15. Click **Next**.



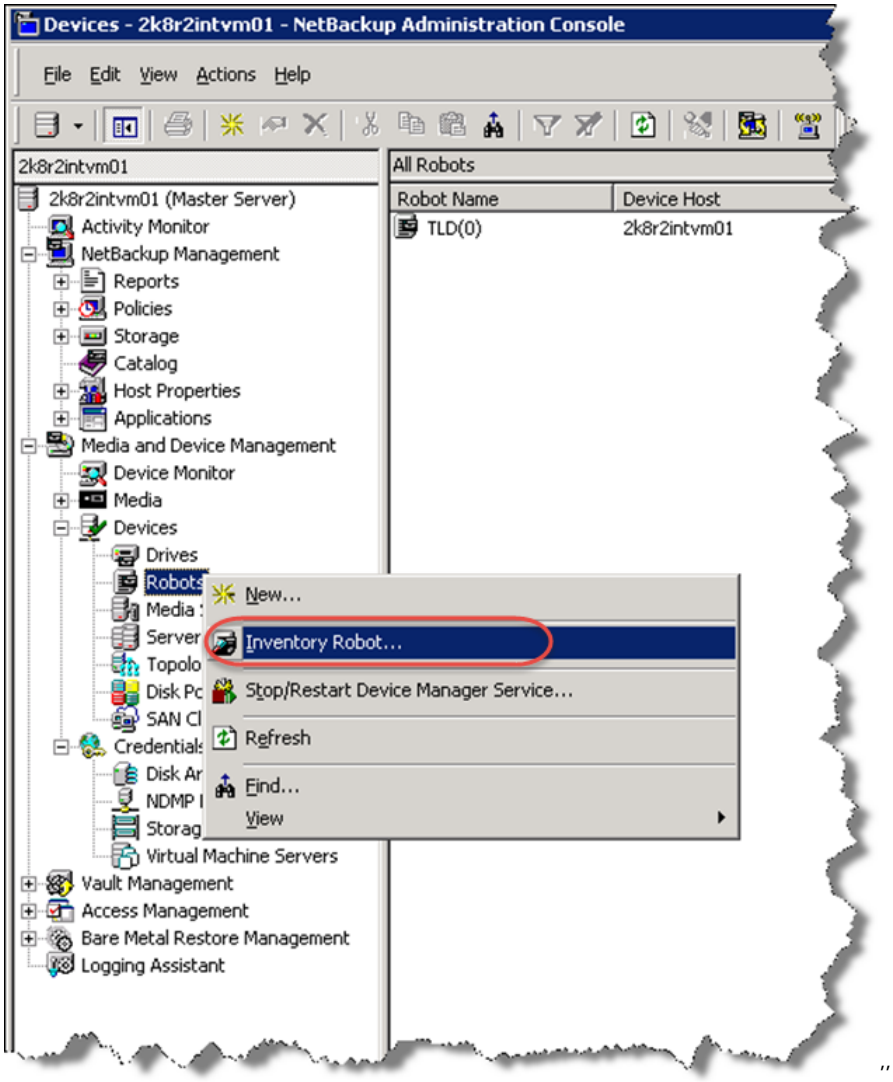
16. Click **Next**.



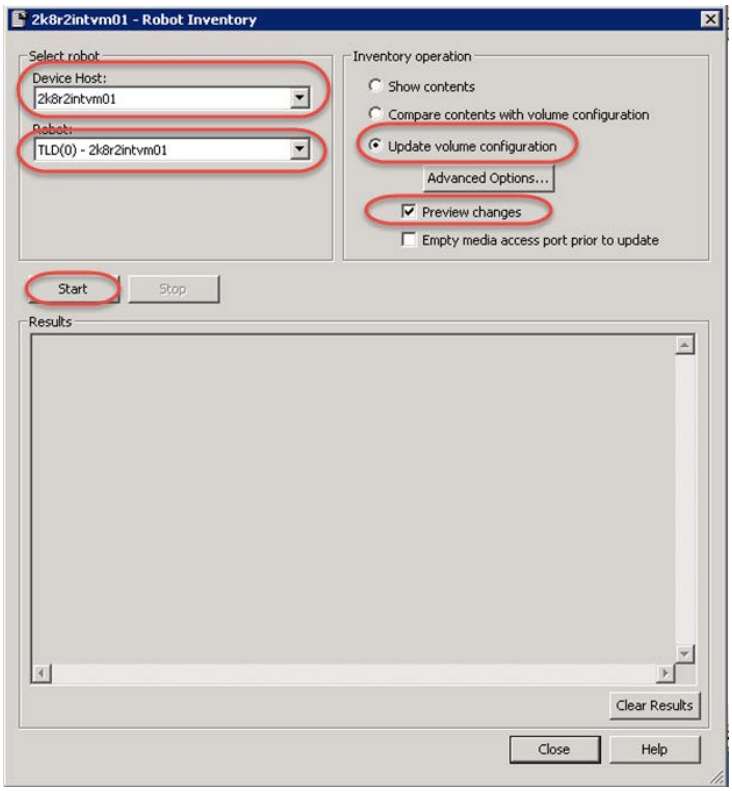
17. Click **Finish**.



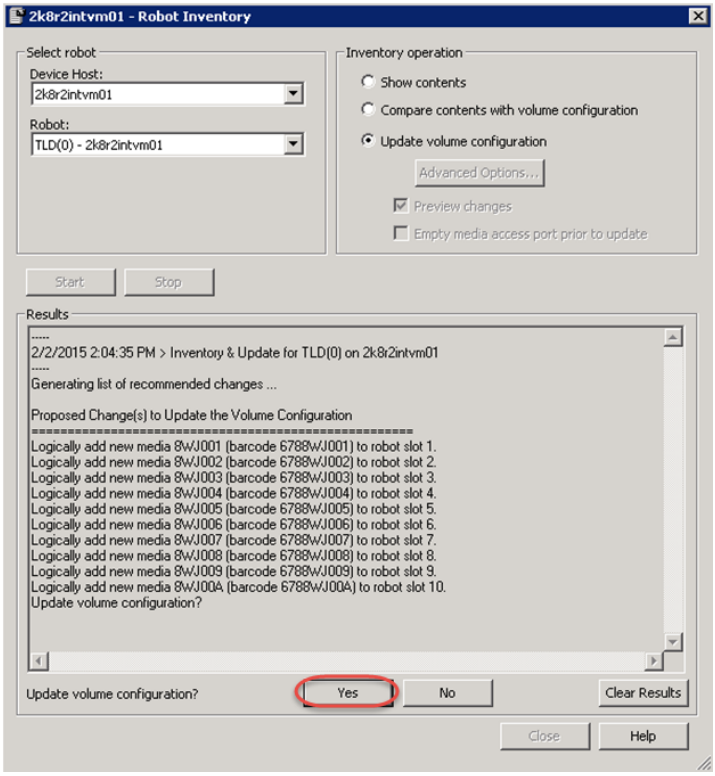
18. Go to **Media and Device Management** > **Devices** and then select **Robots** > **Inventory Robot**.



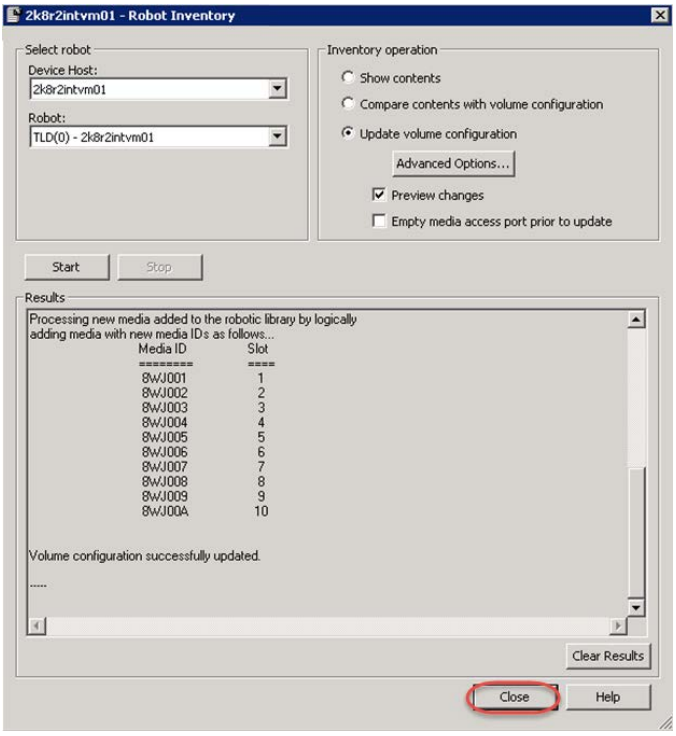
19. Select the Robot you want to inventory. Select the **Update Volume Configuration** and **Preview Changes** options, and then click **Start**.



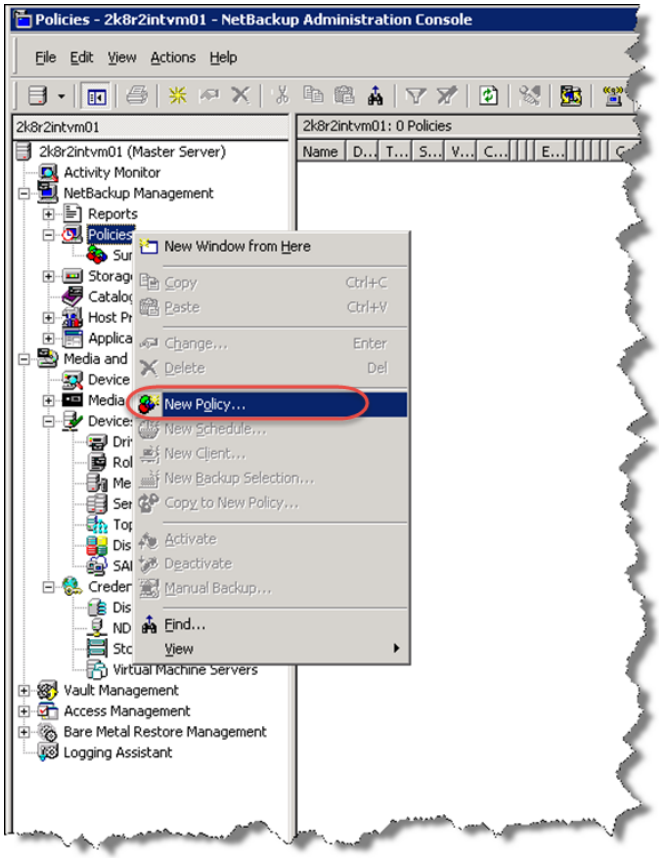
20. When it completes, click **Yes**.



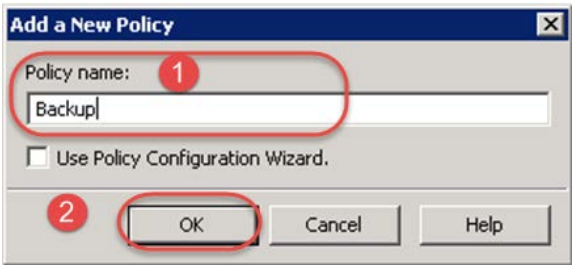
21. Click **Close**.



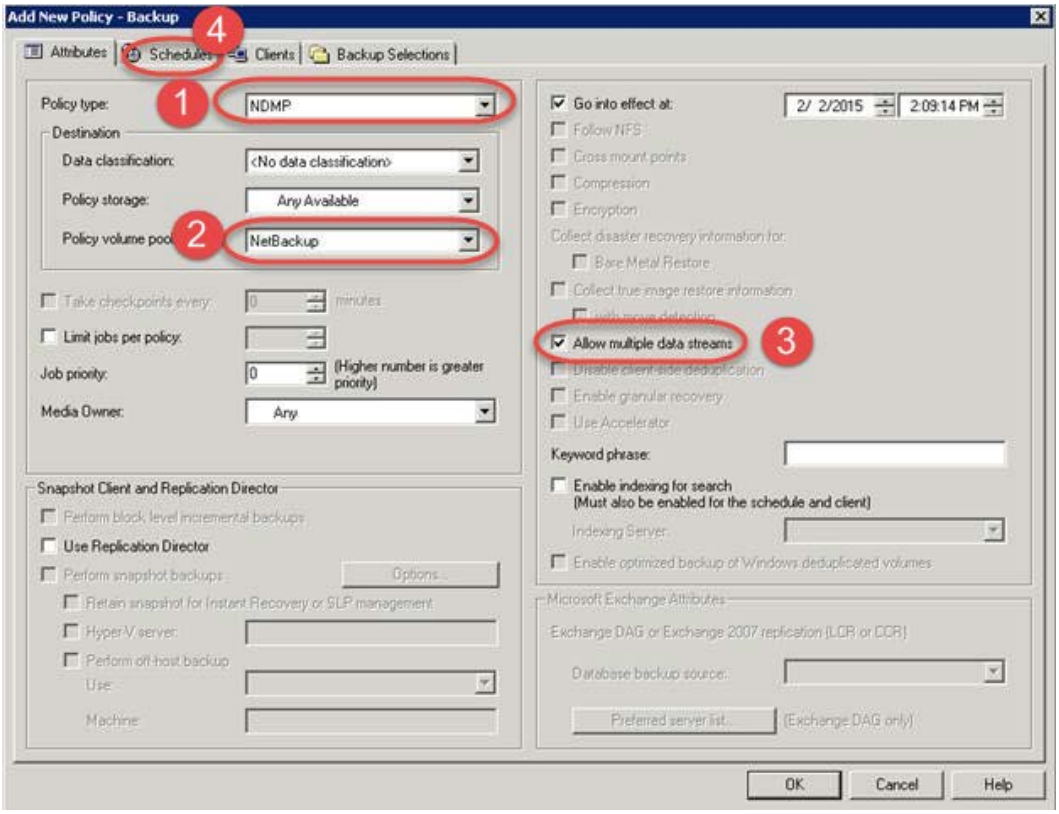
22. Select **NetBackup Management** > **Policies** and then select **New Policy**.



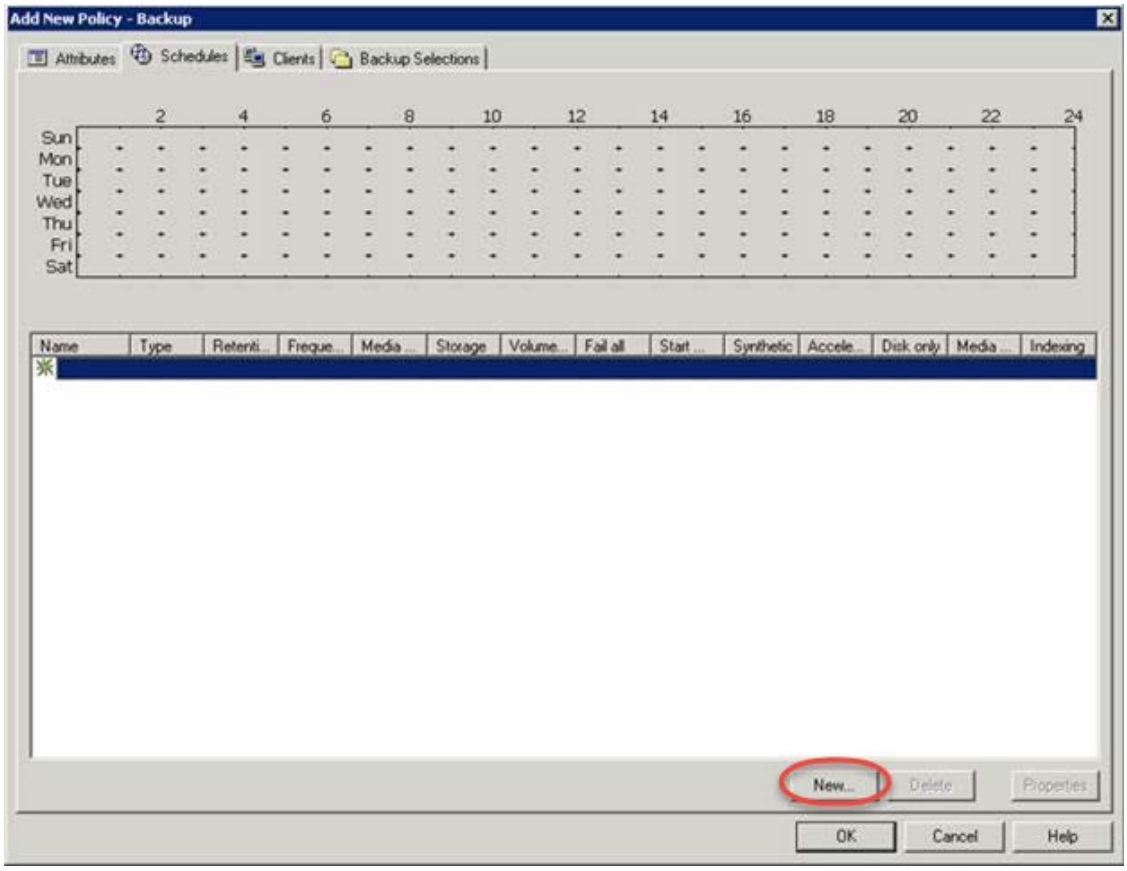
23. Enter a policy name for the backup job and click **OK**.



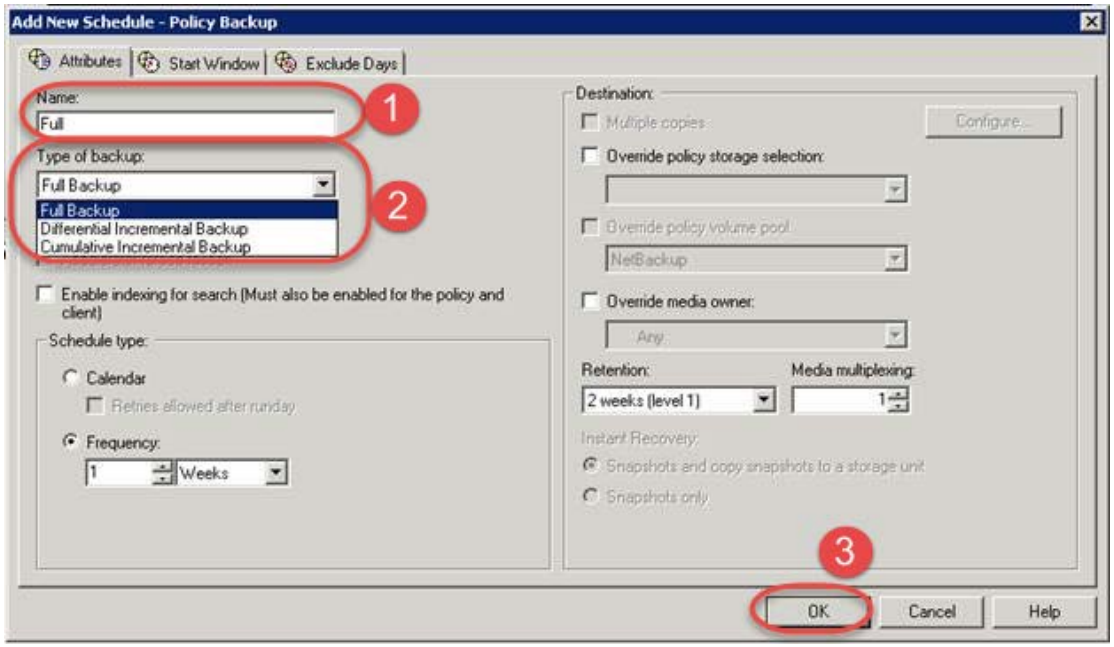
24. Select **NDMP** for the **Policy Type**, and select the **Allow Multiple Data Streams** check box on the Attributes tab. Click the **Schedules** tab.



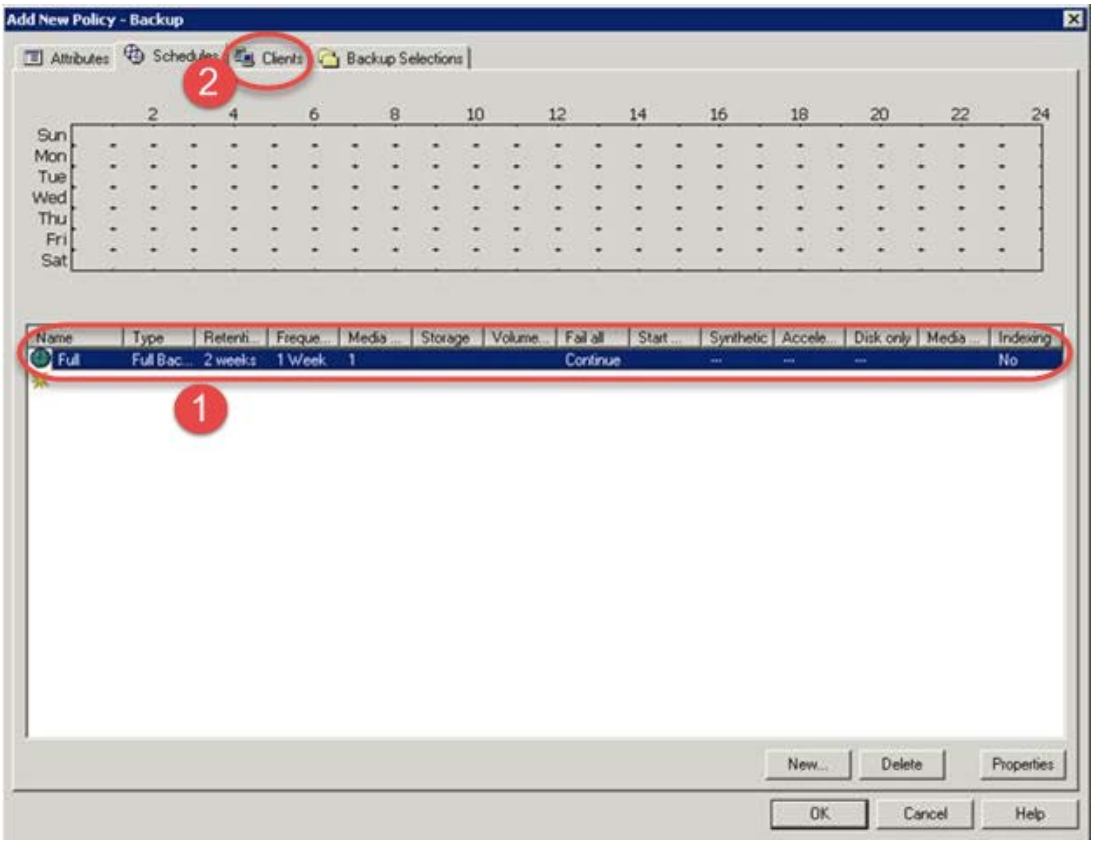
25. Click **New** on the **Schedules** tab.



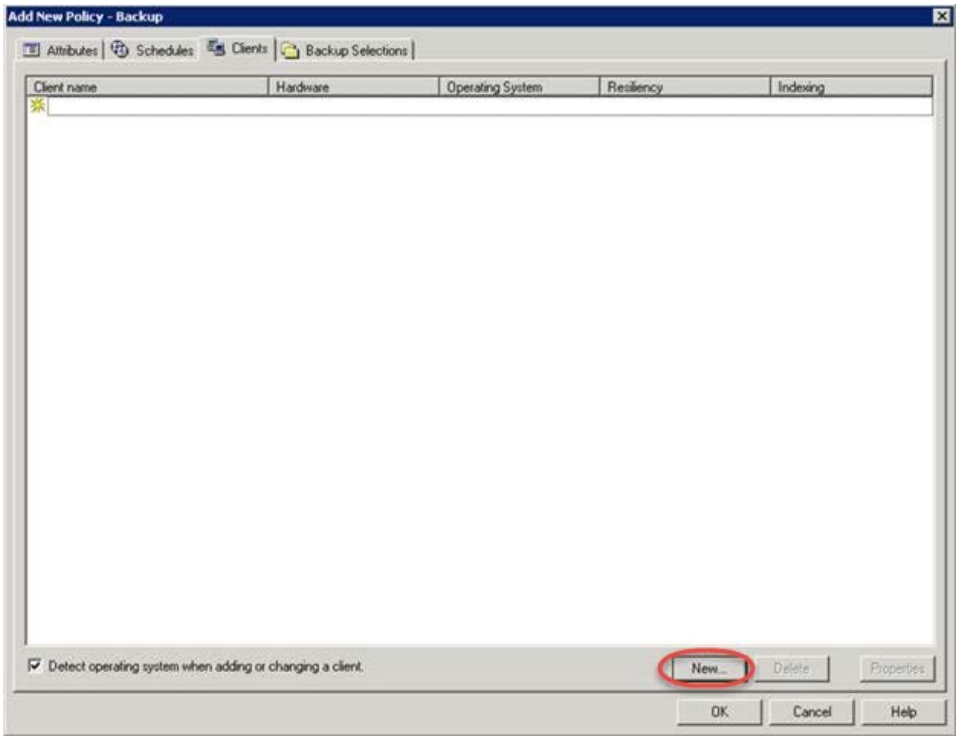
26. Select **Full Backup** for the initial backup, enter a name, and click **OK**.



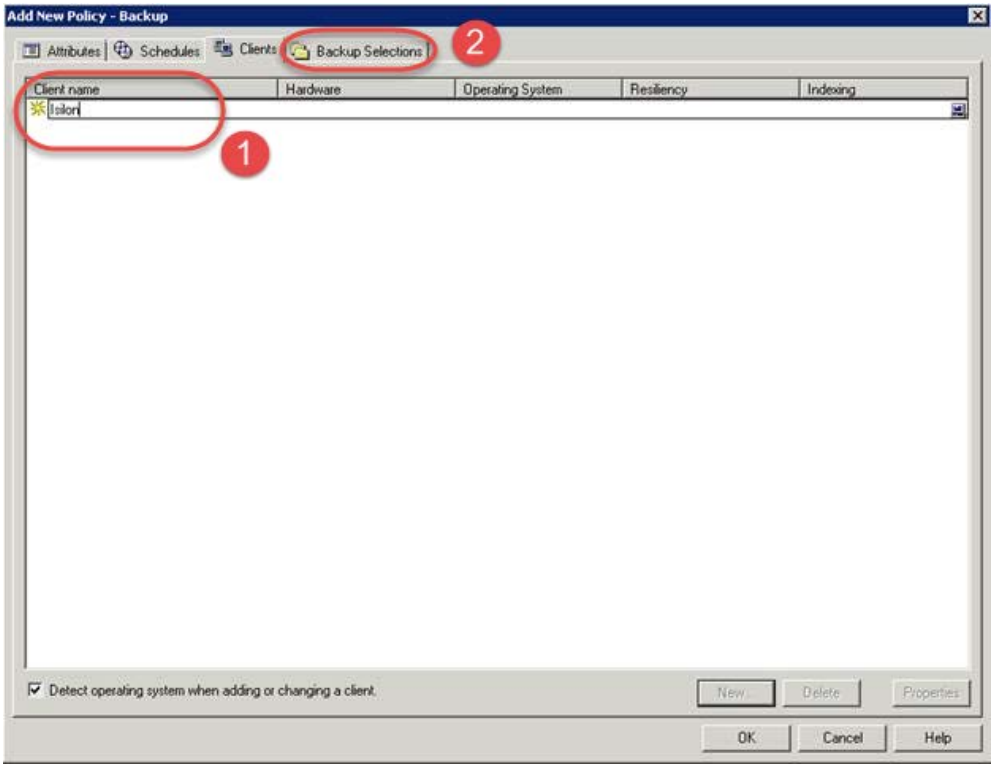
27. Verify the results, and click the **Clients** tab.



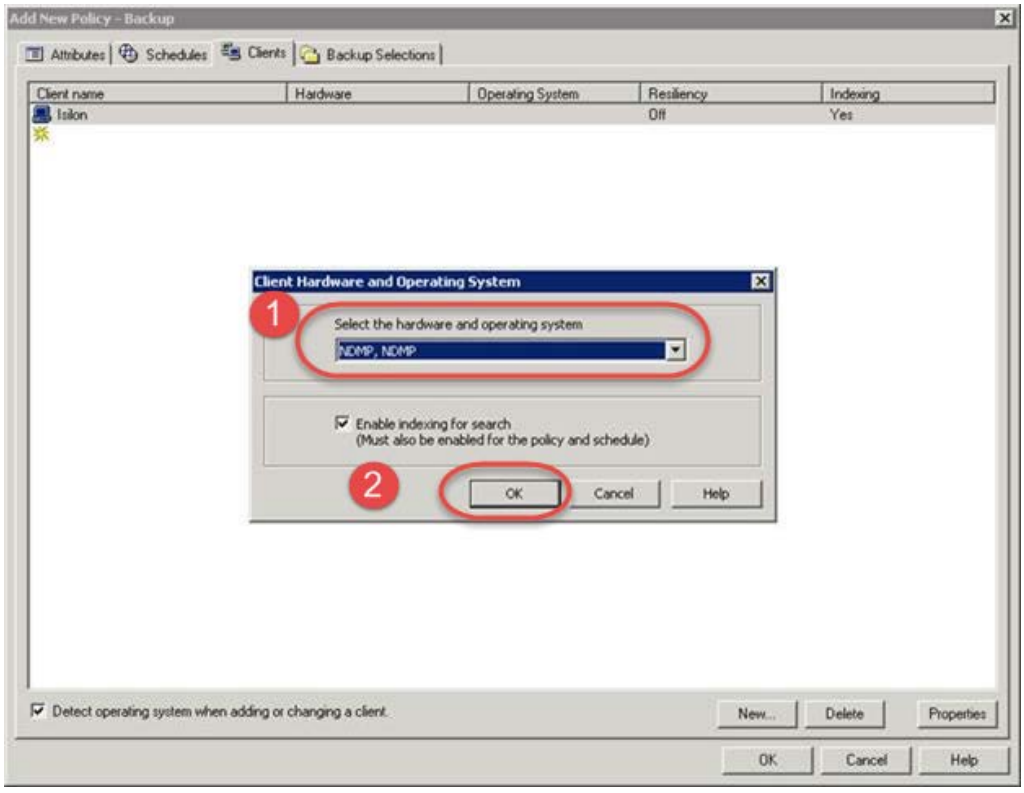
28. Click **New...** on the **Clients** tab to specify the client you want to backup.



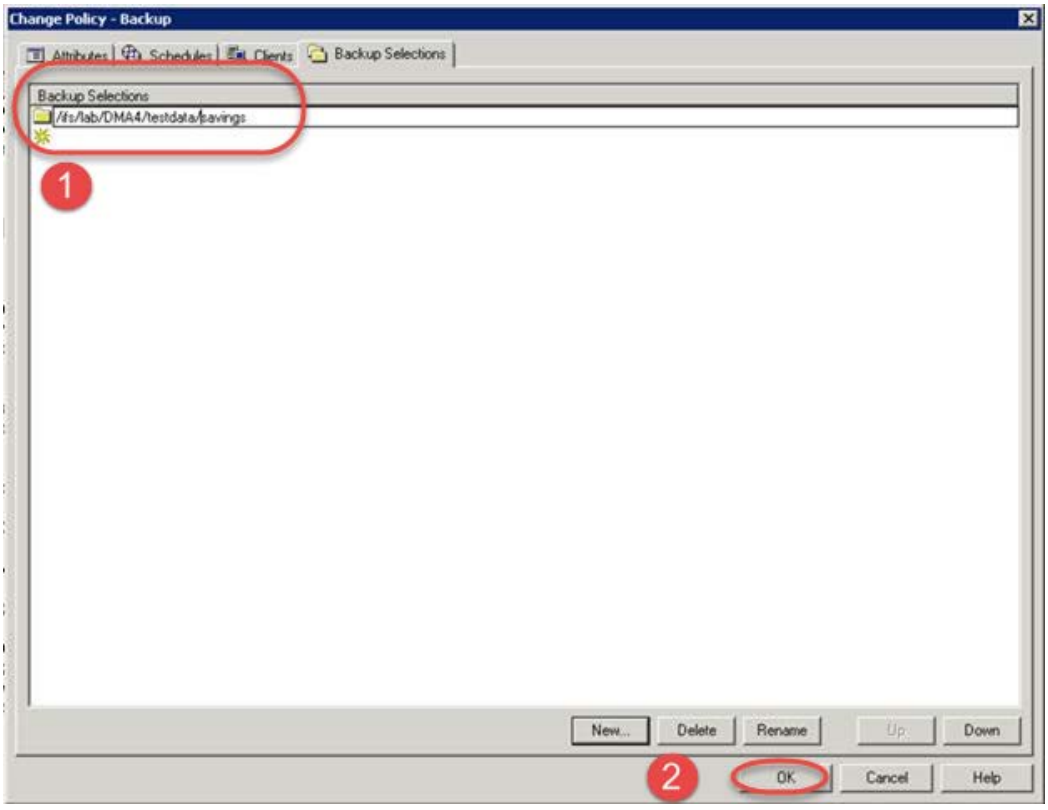
29. Enter the name of the filer and click outside of the edit box.



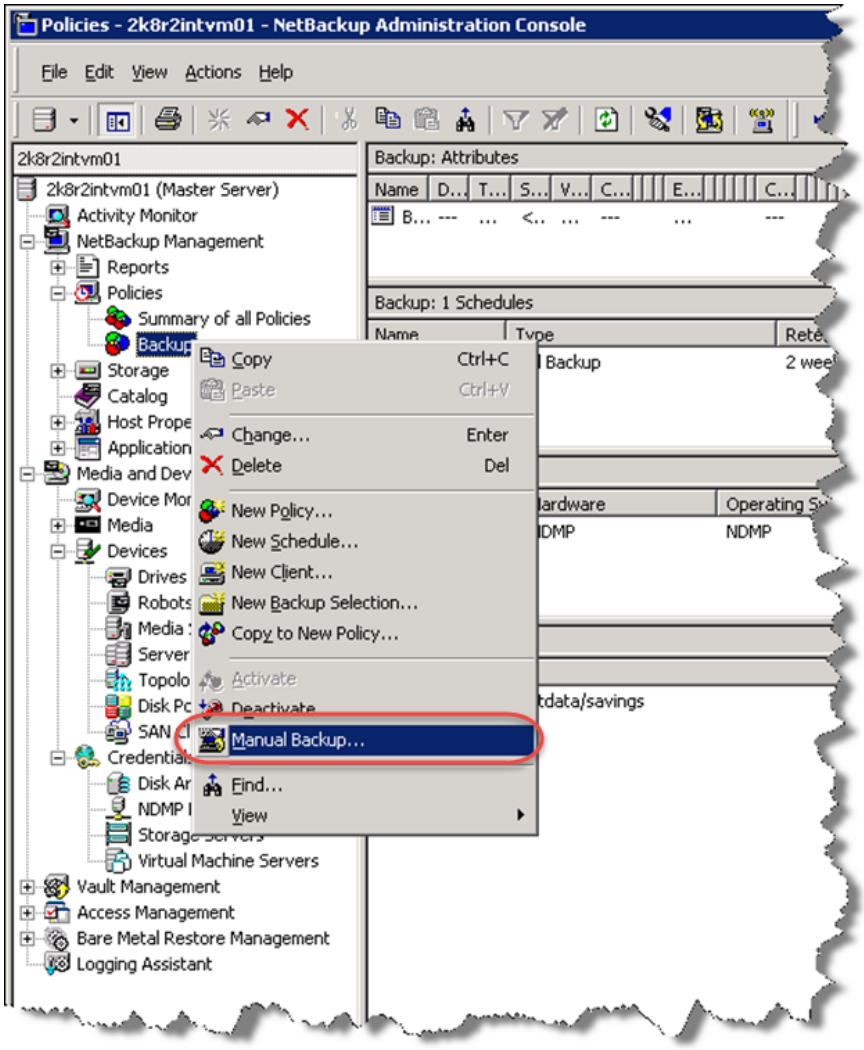
30. Select **NDMP, NDMP** in the drop down menu, and click **OK**. Then, click the Backup Selections tab.



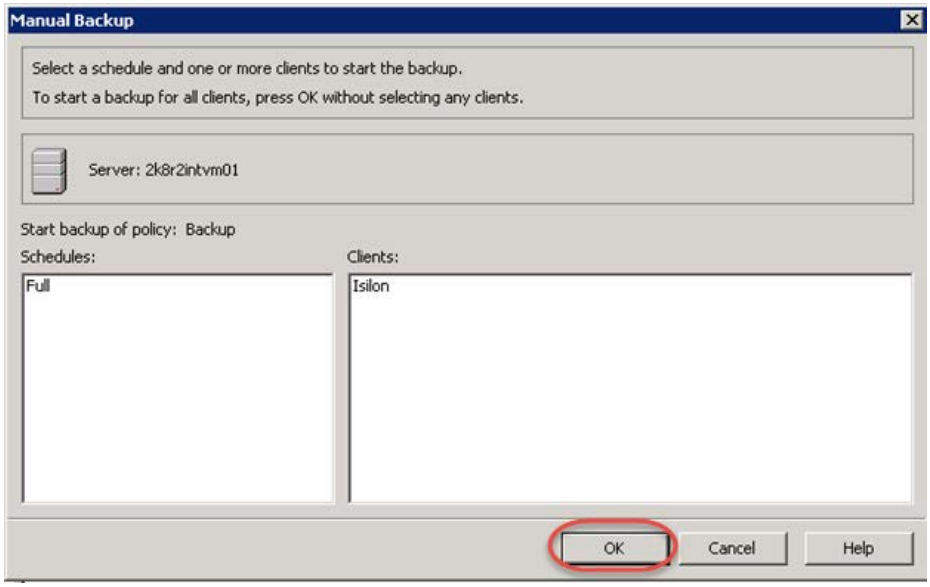
31. Click **New...** and enter the path to the location you want to back up. Click **OK**.



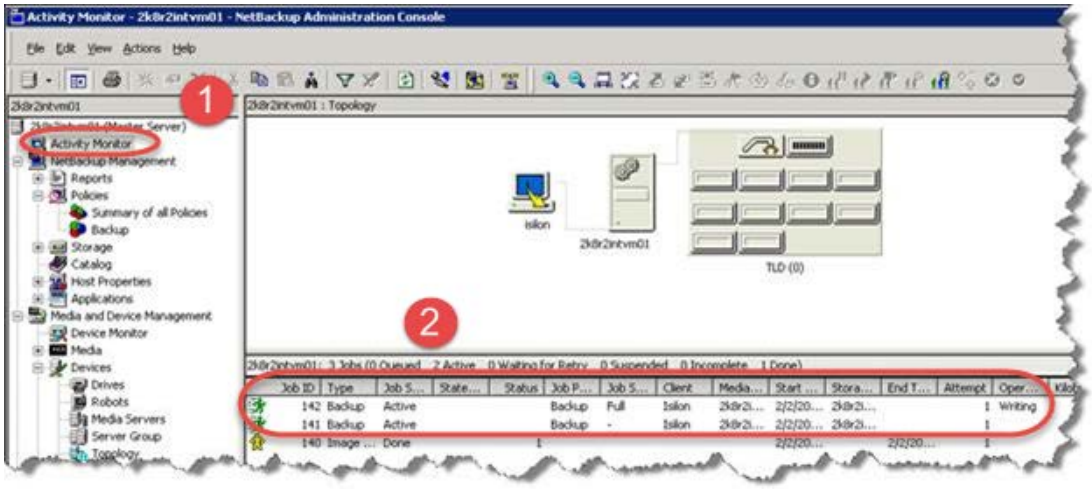
32. Right-click the policy that you just added and select **Manual Backup...** to start the backup.



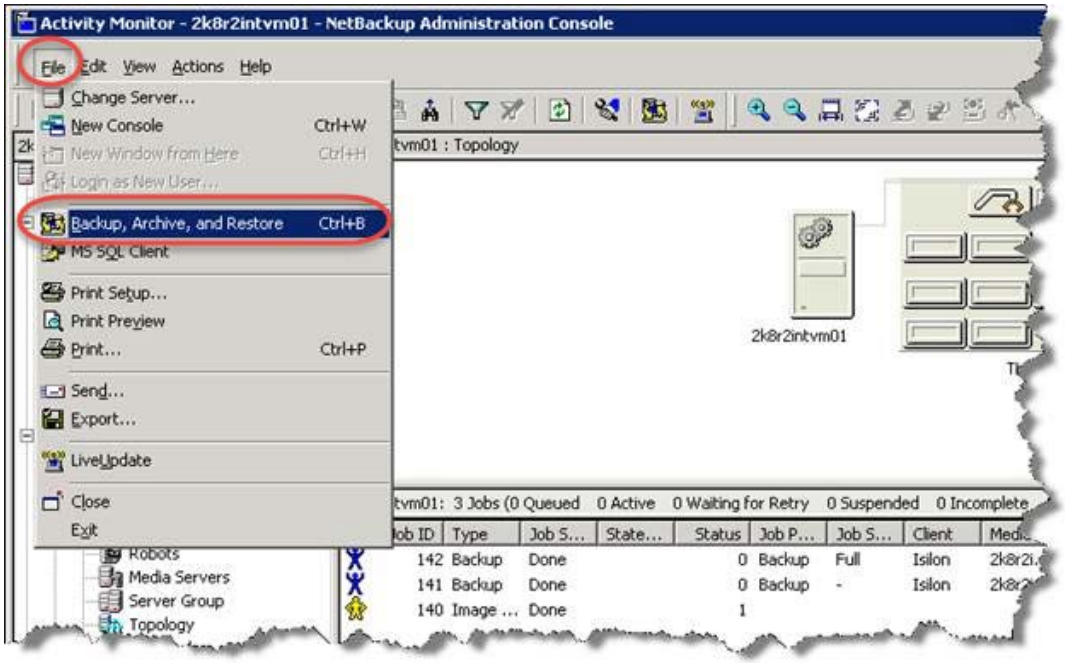
33. Click **OK**.



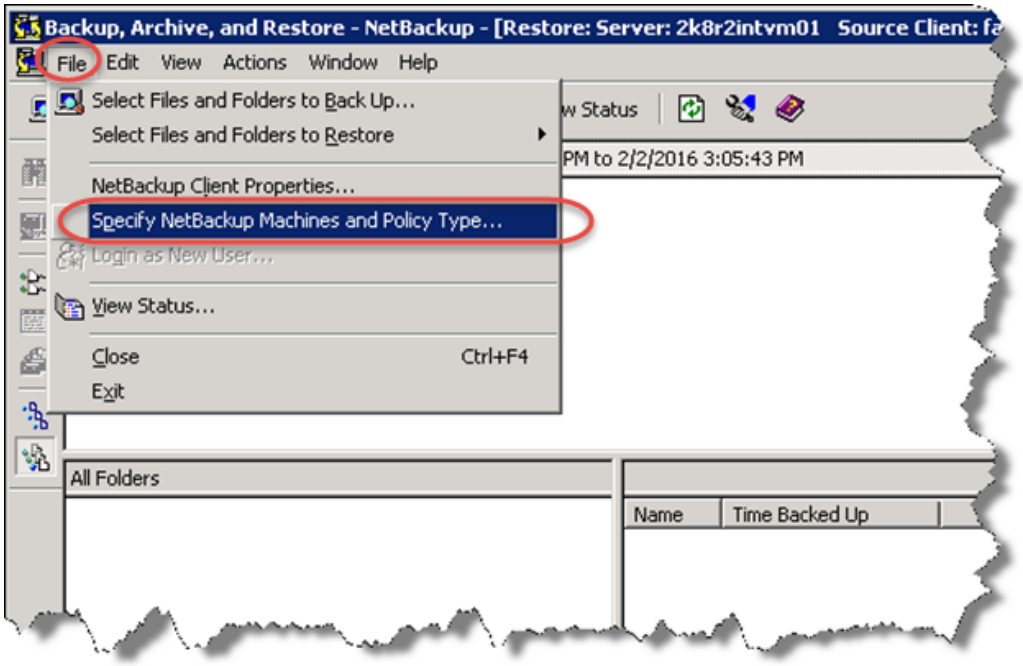
34. Select the **Activity Monitor** in the navigation pane to watch the progress of the backup job.



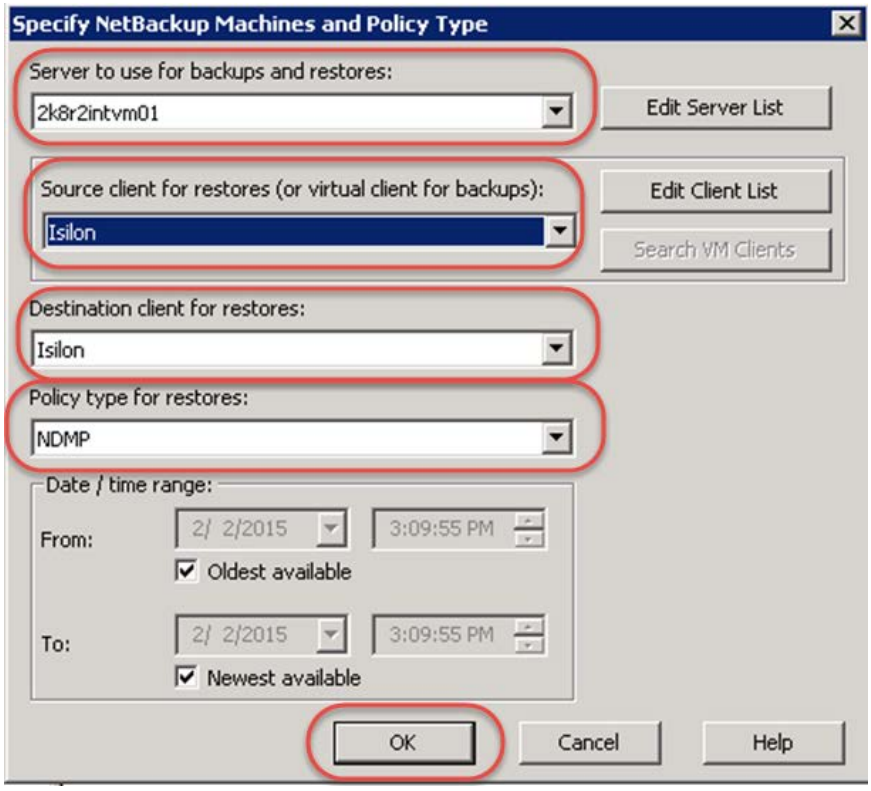
35. Select **File** > **Backup, Archive, Restore** to start the restore process.



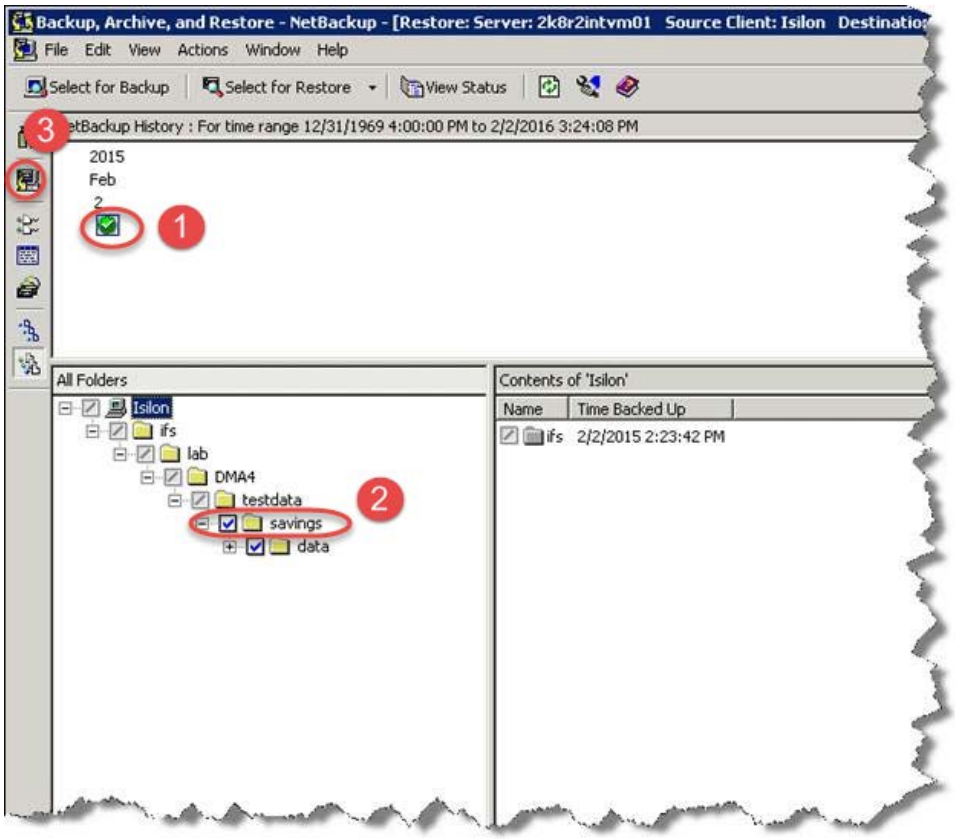
36. Select **File** > **Specify NetBackup Machines and Policy Type**.



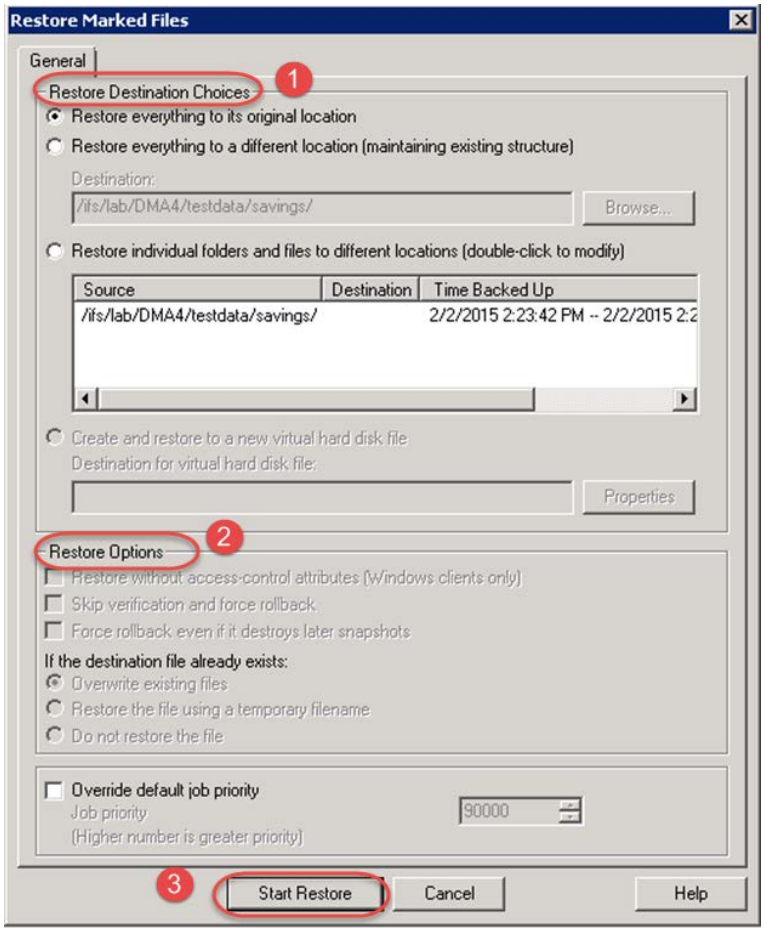
37. Select the Clients you want to restore to and from and click **OK**.



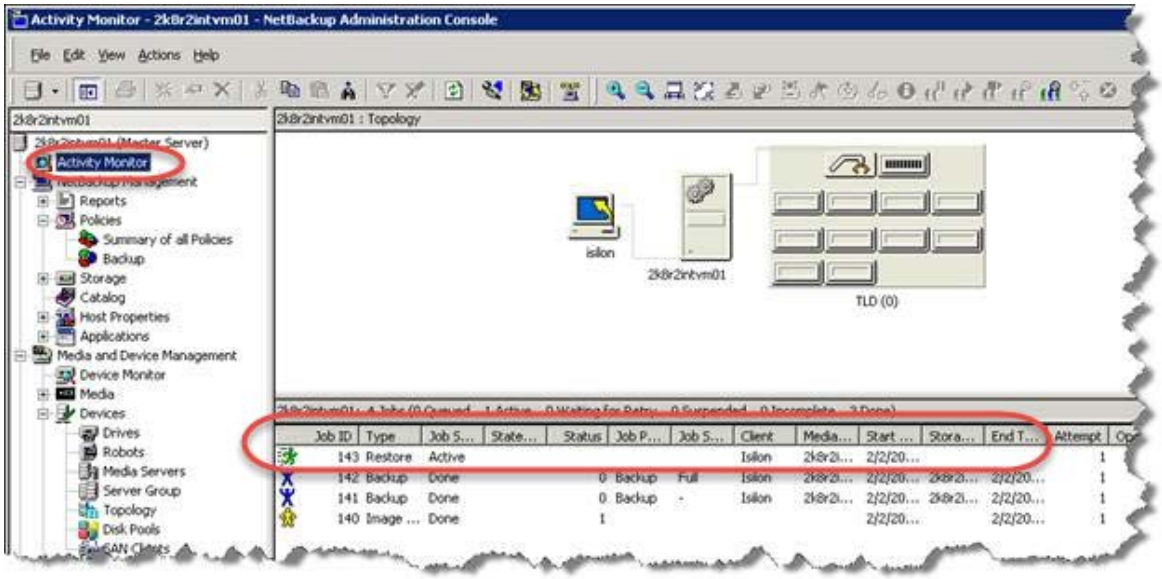
38. Select the backup you want to restore (green check mark for a full backup). Select the checkbox of the data you want to restore in the bottom left pane. Click the restore icon button in the left toolbar.



39. Select the location you want to restore to and restore options. Click **Start Restore**.



40. Monitor the restore progress from the Activity Monitor in the NetBackup Administration Console.

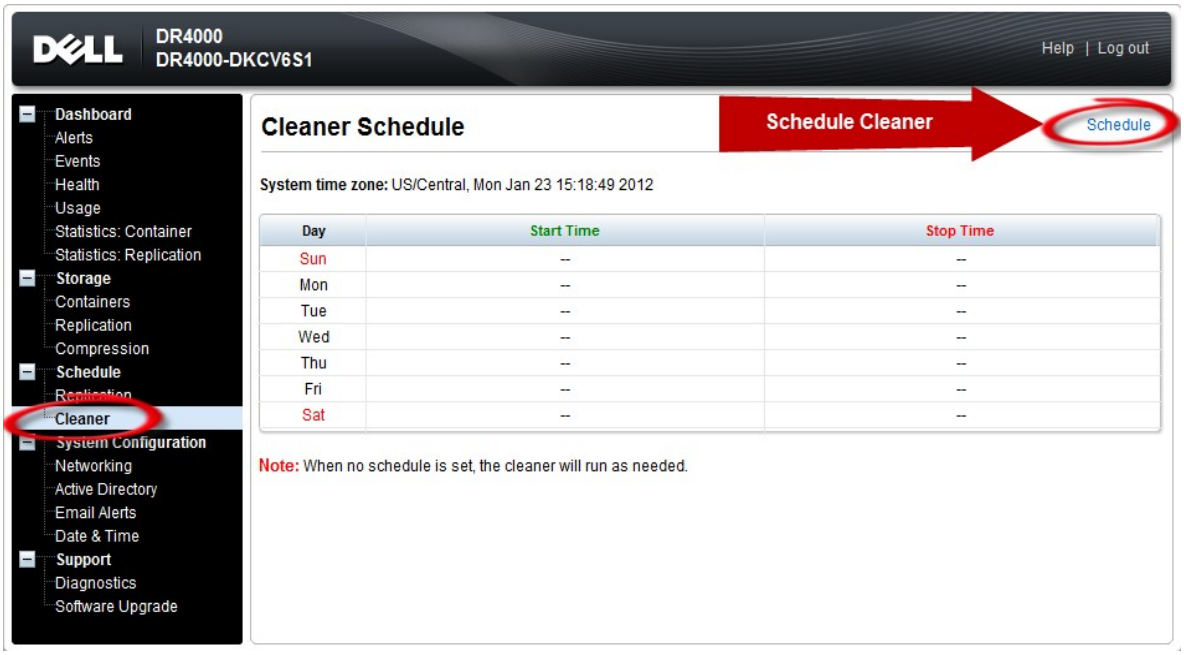


5 Setting up the DR Series system cleaner

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

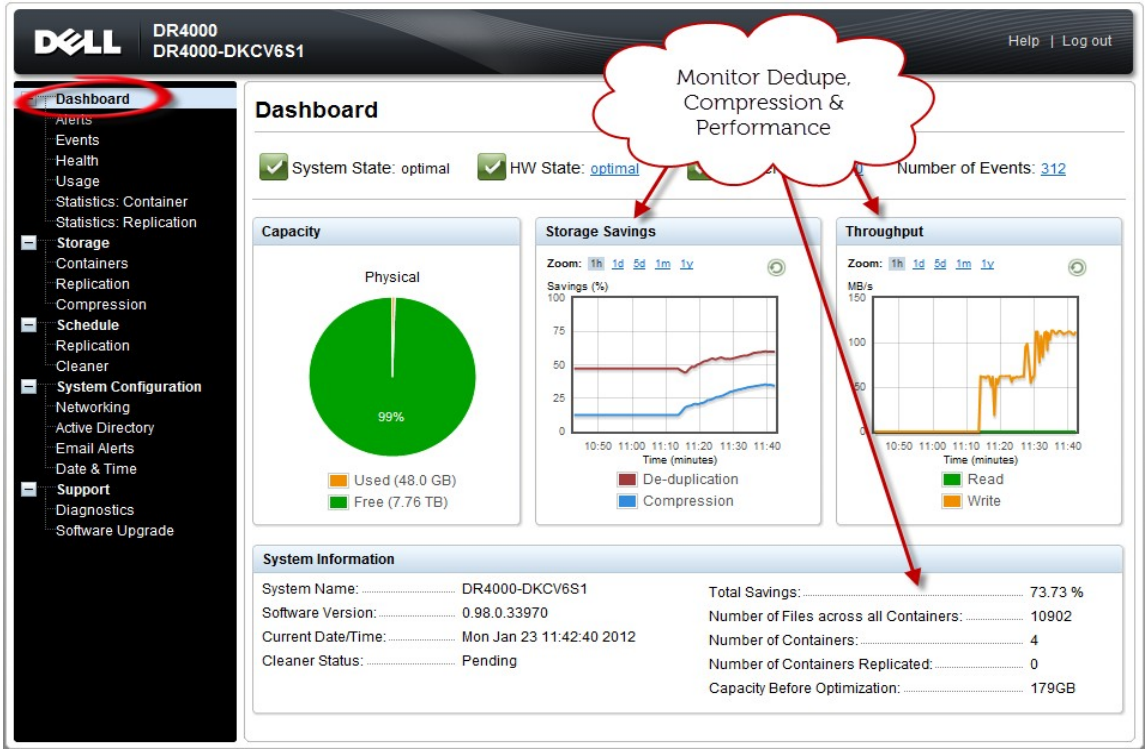
If necessary, you can perform the procedure shown in the following screenshot to force the cleaner to run. After all of the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place, and generally after a backup job has completed.



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 Creating Symantec NetBackup storage units for CIFS and NFS

A.1 Creating a storage unit for CIFS

There are two options for Symantec NetBackup to authenticate to a DR Series system through CIFS as described below.

- Integrating Symantec NetBackup Server and the DR Series system with Active Directory
  - Ensure the AD user has appropriate ACLs to the DR Series Deduplication Appliance Container share
  - Set the Symantec NetBackup service to run with this AD user <Domain\User>

- Ensure that the following services are run by a service or domain account that has full access to the DR Series system container share UNC path:
  - NetBackup Client Service
  - NetBackup Remote Manager and Monitor Service
  - NetBackup Service Layer

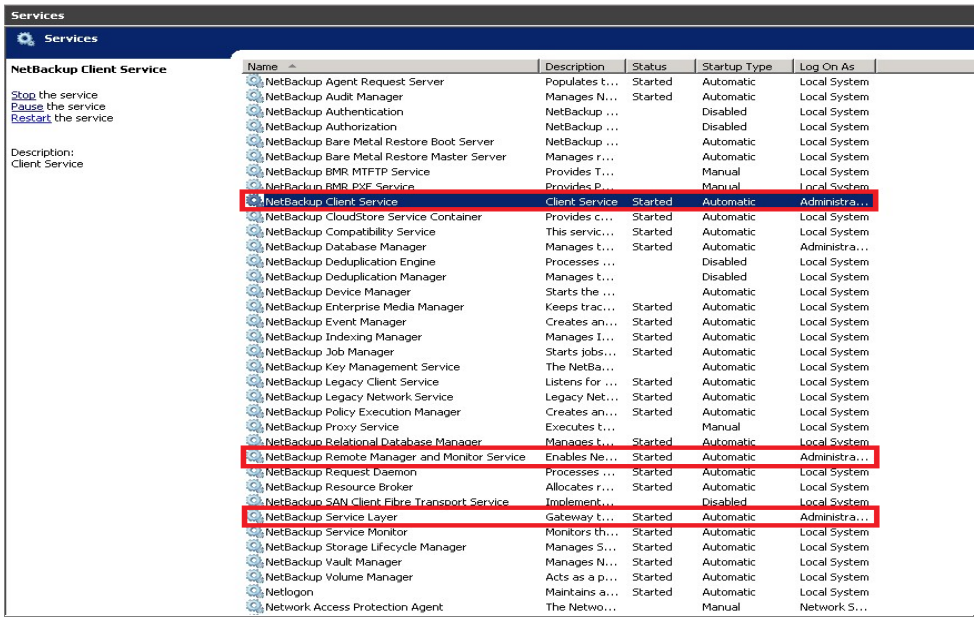
  i. To set the password for local CIFS administrator on the DR Series system, log on to the DR using SSH with username: Administrator, password: St0r@ge!
  ii. Run the following command:

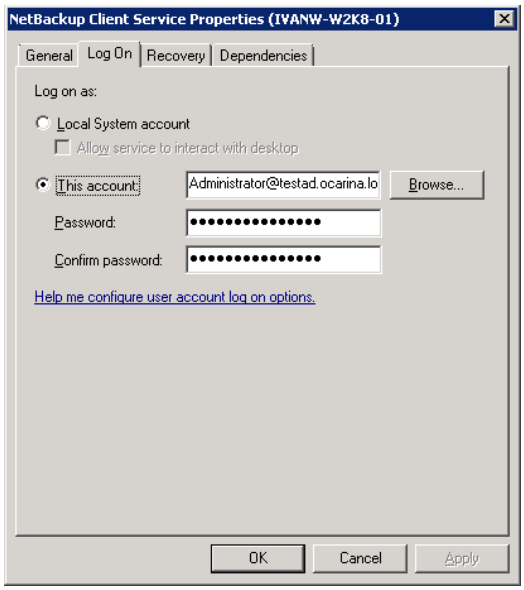
```
authenticate --set --user administrator
```

```
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 Symantec NetBackup service account to use the CIFS administrator account.

  iii. Launch the Microsoft Services Snap-in by clicking **Start > Run > Services.msc > Enter**.
  iv. Locate the 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 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]

v. Click **OK**.

vi. Restart the NetBackup services from the command line to take effect. For example:

```
<install dir>\Veritas\NetBackup\bin\bpdown –v –f

<install dir>\Veritas\NetBackup\bin\bpup –v –f
```

A.2 Creating a storage unit for NFS

For NFS backup using Symantec NetBackup, you need to create a target folder as the NFS share directory. This is the location to which backup objects will be written. (This is not required while adding a CIFS share.)

1. Mount the DR Series system NFS share onto the NFS share directory to which backup objects will be written in the Symantec NetBackup environment.
2. Verify the NFS share. One way is to use the Linux command "cat /proc/mounts". The rsize and wsize of the connects in the command output should be 512K.

B VTL configuration guidelines

B.1 Managing VTL protocol accounts and credentials

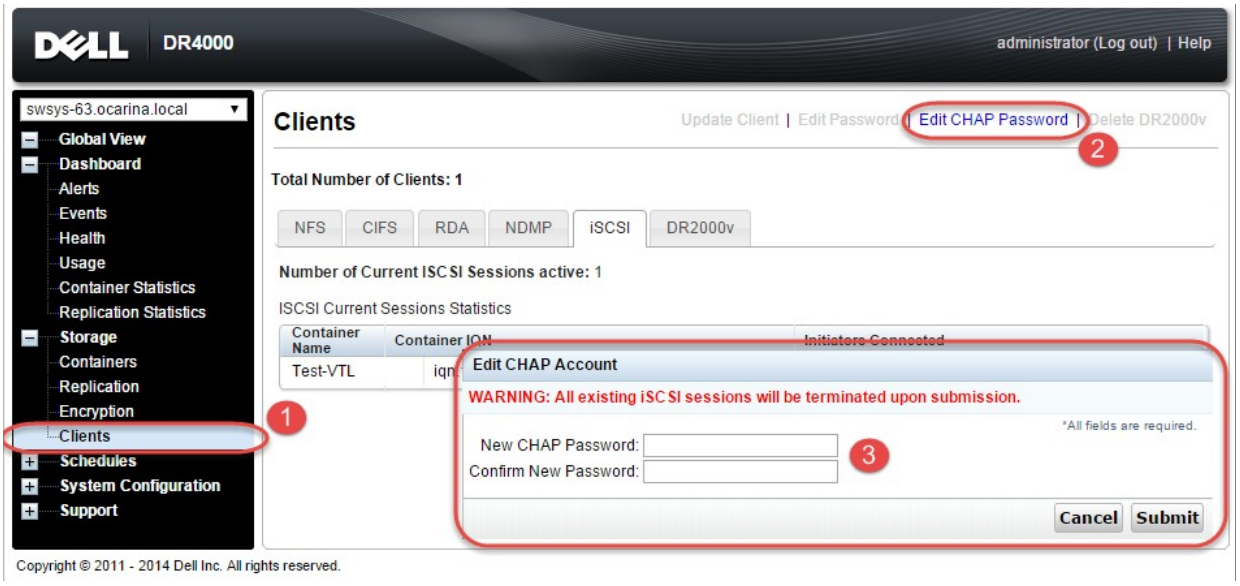
B.1.1 iSCSI Account Details and Management

By default, the iSCSI username is the hostname of the DR Series system and can be confirmed by reviewing the output of the iscsi –account --user CLI command. For example:

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

The default iSCSI password is St0r@ge!iscsi. You can modify this password in the iSCSI tab of the Clients page. Click Edit CHAP Password and enter a new password as needed.

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

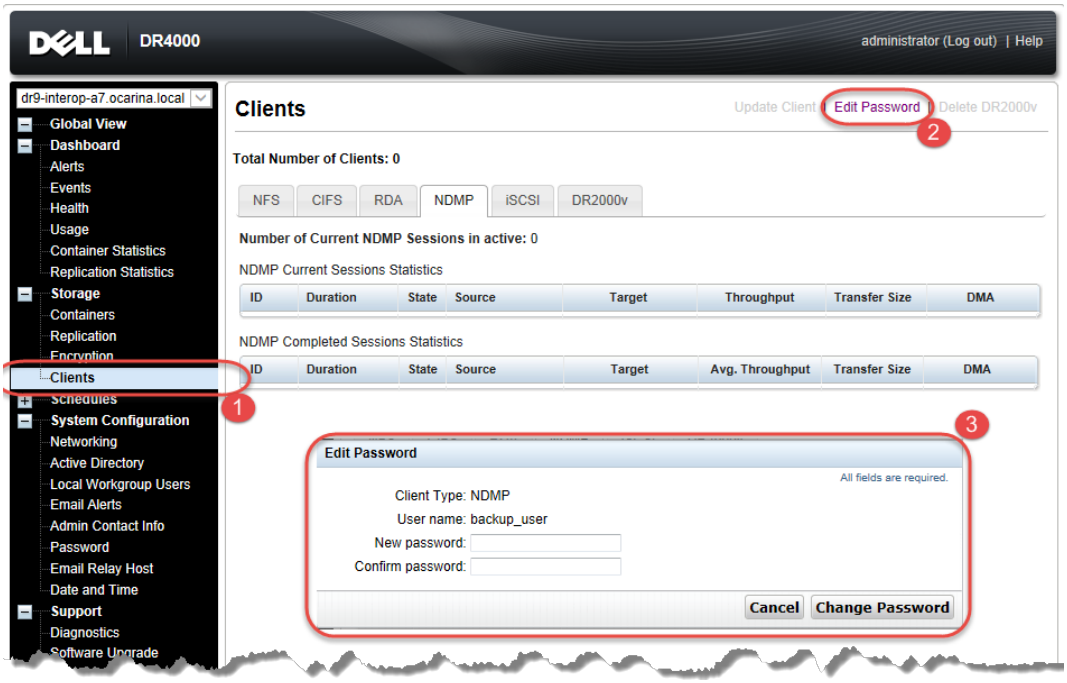


Alternatively, you can also use the iscsi--setpassword CLI command to change the iSCSI CHAP password as shown in the following example:

```
> 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:############
```

B.1.2 NDMP account details and management

The default username for the NDMP service is "ndmp_user." This can be confirmed on the NDMP tab of the Clients page in the DR Series system GUI.



You can also use the CLI command ndmp –show as shown in the following example.

```
> ndmp --show
NDMP User:      ndmp_user
NDMP Port:      10000
```

The default password is St0r@ge! It can be modified by running the ndmp –setpassword command:

```
> ndmp --setpassword
Enter new NDMP password:#########
Re-type NDMP password:#########
NDMP password successfully updated.
```

B.1.3 VTL default account summary table

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

B.2 Managing VTL media and space use

B.2.1 General performance guidelines for DMA configuration

The DR Series system version 3.2 (and later) provides inline VTL deduplication, compression, and encryption at rest. Backup Applications (such as Dell NetVault, Symantec BackupExec, Symantec NetBackup, etc) should be configured so that any multiplexing, pre-compression, software side deduplication or encryption is disabled. Enabling any of these features may adversely affect the space savings and ingest performance of the DR Series Appliance VTL feature.

Slots and media should be configured so as to accommodate the environment backup requirements. Initially the logical capacity of a VTL should be no more than twice the physical size of the DR Series Appliance. If the initial VTL setup is oversubscribed at a higher than a 2-1 ratio without proper planning the DR Series Appliance could fill up prematurely and cause unexpected system outage. It is highly advisable to configure the DR Series Appliance VTL such that the media count be made to accommodate the customer's initial logical data protection requirements and then media be added as the deduplication statistics become available to ascertain growth, media and space requirements.

Media Type selection will depend on a number of factors including the DMA used, the backup cycles and data sources to name a few. As a general rule using smaller tapes is better than using larger tapes so as to allow for a higher level of control over space usage by backup operations. This also allows for easier handling in the event of a system running out of physical space as well as the normal data cleanup procedures.

Adding media to an existing DR Series Appliance VTL is painless and should be leveraged to incrementally add media as needed. Although this may require a higher level of involvement in managing the media usage it will result in better performance and avoid unplanned outages.

B.2.2 Physical DR space sizing and planning

Various factors such as total data footprint, change rate, backup frequency and data lifecycle policies will dictate how much physical space will be needed to accommodate the Virtual Tape Libraries within a DR environment. In addition if other container types are hosted these two must be factored into space requirement calculations. As a general rule the following can be used as a reference to determine the basic capacity needed for a given virtual tape library container:

1. Determine existing data set
2. Determine the change rate (Differential)
3. Determine the retention period

4. Calculate the data footprint during the retention period for existing data sets based on a 10-1 deduplication ratio
5. Calculate the data footprint during the retention period for change rate data sets based on a 10-1 deduplication ratio
6. Calculate the ratios within the retention period for each of the data sets
7. Determine the lowest ratio data set to be retired within the retention period and create media of size that closest matches this data footprint so that when a retention period is met the most amount of media is recycled to invoke data reclamation alignment and optimizing media consumption.

IMPORTANT: If other containers are being configured to host CIFS/ NFS / RDA or OST, these must also be factored into the planning and management of space.

B.2.3 Logical VTL geometry and media sizing

The logical size of the VTL including media size and media count should be made such so as to accommodate the existing data footprint targeted for protection. The calculation for such should include the initial footprint, change rate and retention period. It should also take in account the size of both full and incremental data sets. Using the smallest iteration of the data sets to dictate the logical size of the VTL media affords users the ability to retire media in smaller increments which results in high levels of use and also provides the users the ability to conduct operations across smaller objects which results in higher levels of flexibility such as when a restore is needed during backup operations.

We can review a typical full weekly plus incremental daily example to demonstrate one method of conducting this calculation. In our example the total logical foot print for the customer environment is 20TB and with a 10% change within a weekly recovery point objective period for a complete weeks' worth of protection we calculate that we will require 22TB of total logical media to retain the data footprint for the given environment for one week. In order to allow for disparities we also include a 10% increase to allow for flexibility in the deployment and use of the VTL which results in a 24.2TB total virtual media requirement for a single weekly retention period.

Important Note: Media can always be added as needed. Media cannot, however, be deleted, so care must be taken to avoid creating too many media items.

In the previous example, at the end of the 5-week cycle the 1st week retires and frees up media to be reused or recycled, which once processed will allow the DR Series system to reclaim the physical space associated with the virtual media. Since the smallest data set footprint resulting from the change rate is 2TB in each incremental iteration, we create our media at 800GB increments and add as we grow. For this example, the initial VTL would be created with **152** (*121TB divided by 800GB*) pieces of media at **800GB** for each piece media.

20TB Total initial footprint with a 10% change rate

	Pre-Deduplication		
Week	Logical Size	Logical Full Metrics	10% Change Rate Logical Incremental Metrics
1	24.2TB	20TB	2TB
2	24.2TB	20TB	2TB
3	24.2TB	20TB	2TB
4	24.2TB	20TB	2TB
5	24.2TB	20TB	2TB
Total	121TB		

B.2.4 Media retention and grouping

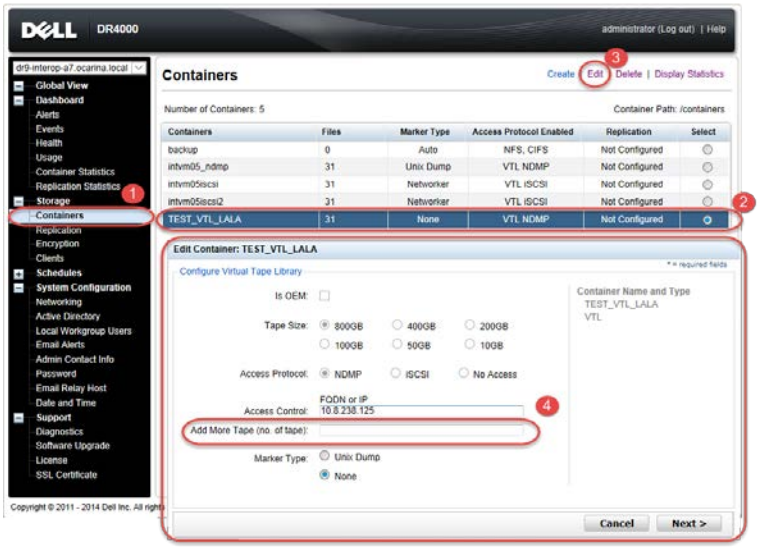
Due to the nature of VTL, media must be managed to insure that physical capacity is reclaimed in an orderly fashion to avoid running out of space and disrupting operations. Media must be grouped within the data management application, in a way that full data sets are targeted to separate media as incremental data; and, they, in turn, are grouped by data sets that expire within the same period or that share the same recovery point objective. This insures that media can be reused effectively so that when full all incremental data expire the logical space can be reconciled thus enabling the physical space to be reclaimed.

B.2.5 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.2.6 Adding media to a VTL container

To add media to an existing VTL container, navigate to the Containers menu in the DR Series system GUI. Select and edit the target VTL container. In the resulting dialog box, in the **Add More Tape (no of Tape)** field, enter the number of tapes to add to the VTL container.



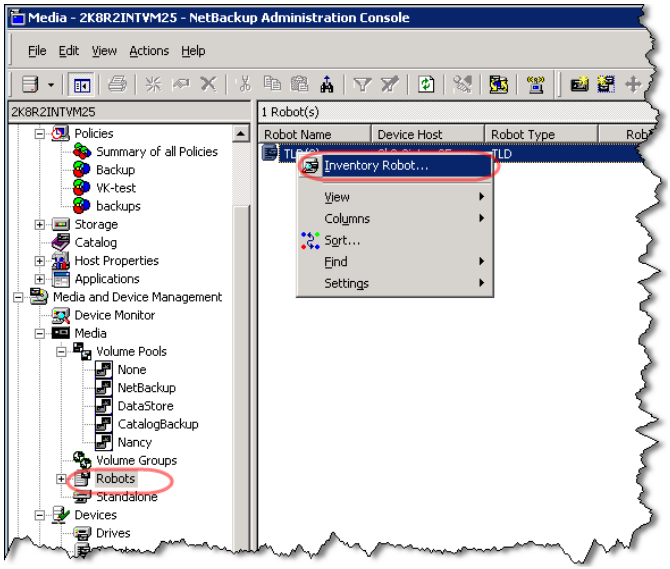
Alternatively, you may also use the "vtl –create_carts" CLI command. For example:

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

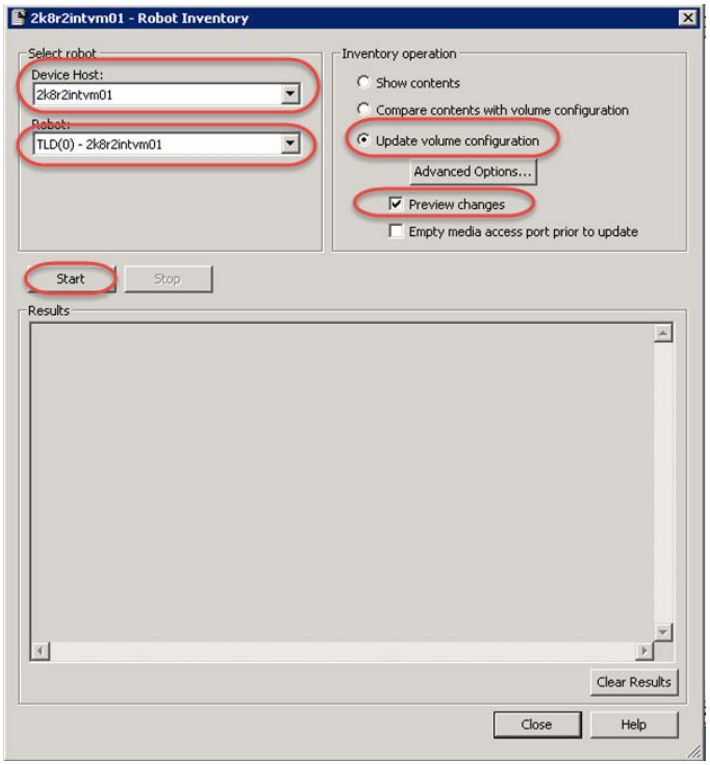
B.2.7 Updating NetBackup to identify newly added VTL media

After VTL media has been added to a target VTL container, NetBackup must be updated to use the newly created media.

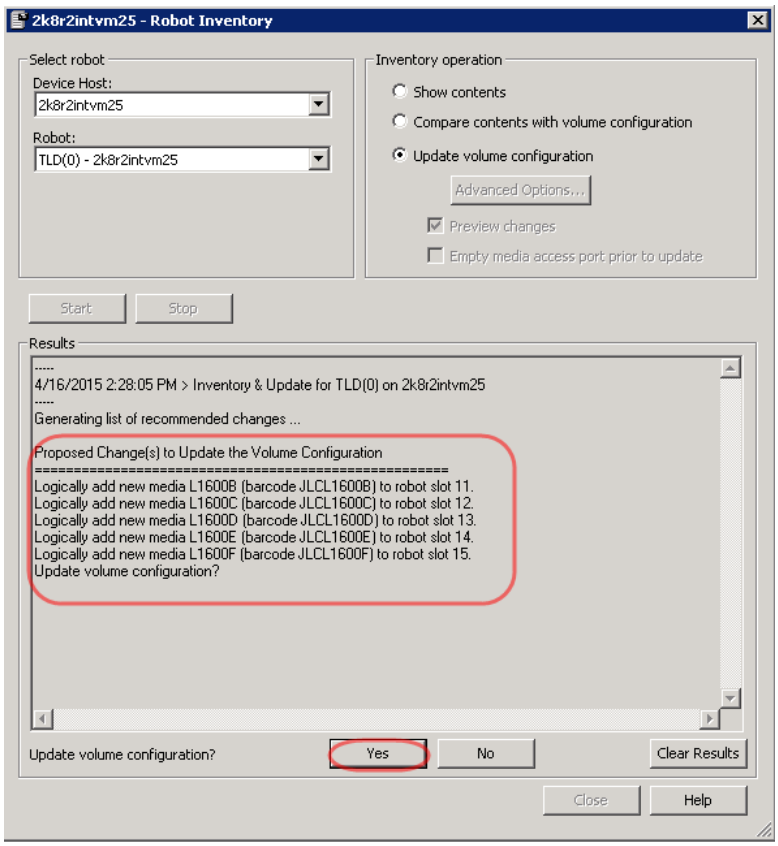
1. Select the robot of the VTL and perform an inventory update (as when you added the VTL initially).



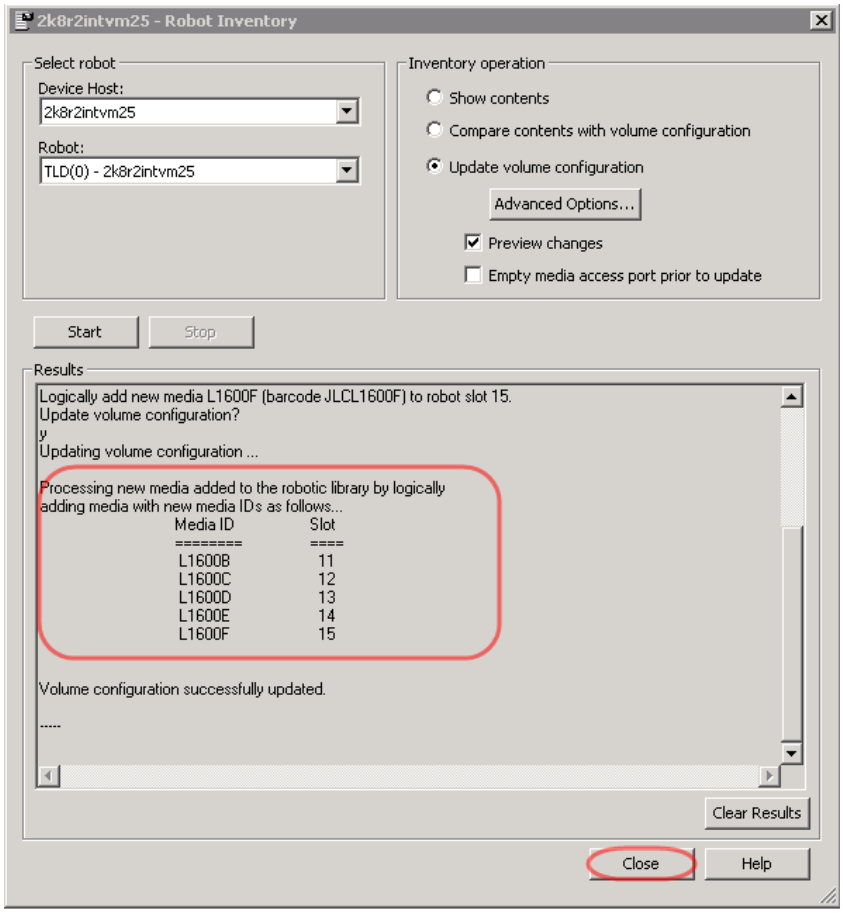
2. Select the options, **Update Volume Configuration** and **Preview Changes**, and then click **Start**.



3. Verify that the media is found, and click **Yes**.



4. Verify that the media is added and click **Close**.



B.2.8 Space reclamation guidelines

General Guidelines

The DR Series system version 3.2 VTL feature is presented to operating systems and data management applications alike as devices either through iSCSI or NDMP protocol connectivity. The DMA interfaces with the virtual tape library and all its underlying components including the drives and media though these specific protocols.

The DMA must interact with the virtual tape media during a recycle, reuse or media initialization process in order for the DR to be able to reclaim space during its own cleaning cycle.

This two-step process is required so that the backup software can reconcile the space by marking the media as expired then reusing it, consolidating space across volumes/tapes or by simply recycling the media into a scratch pool. Once these operations have been completed the DRs own cleaning cycle should be used to reclaim that virtual tape media space which in turn will free up physical space on the DR unit.

Implementing proper media pool, groups and recycling practices will allow the virtual tape media to be used at optimal levels and that the underlying physical space be reclaimed accordingly by the scheduled DR reclamation.

Note: In general the guidelines provided above should be sufficient for normal operations to insure proper reclamation of space is conducted preemptively. Refer your individual DMA applications for best practices and guidelines regarding tape reuse.

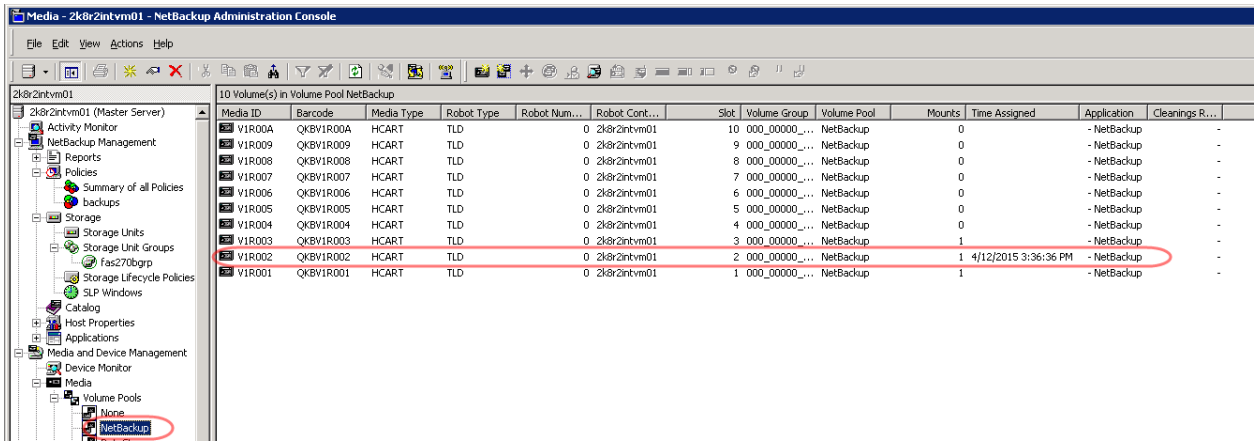
Product Specific Guidelines

In the event that space becomes an issue or a user impact requires manual cleaning, media can either be manually Erased, Blanked, Scratched or otherwise recycled and a manual cleaning cycle initiated on the DR Series system.

For NetBackup the following steps can be used when a situation dictates that space must be reclaimed manually.

1. Identify the DR Series system VTL tapes that have been written to via the **NetBackup Administrative Console**. Note down the **Media ID**s of the tapes that you want to erase and reclaim their storage on the DR. Be sure to only note the tapes you are assured can be erased.

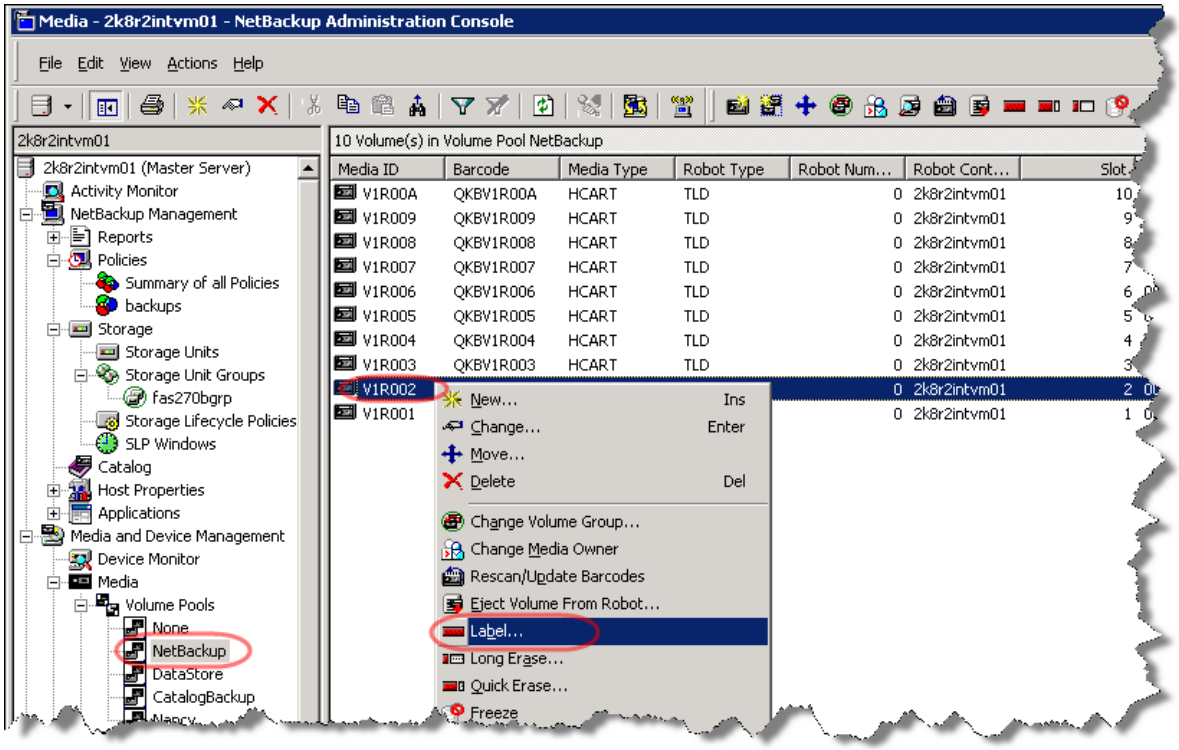
Important: This will permanently delete / destroy the data on these virtual volumes.



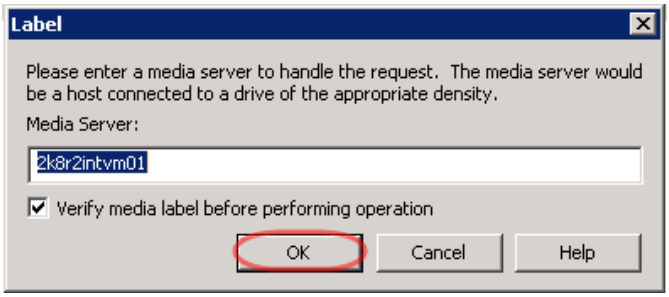
2. Run the following script with the media IDs to enable the tapes to be relabeled and erased.

```
set label="<media ID>"

"C:\Program Files\Veritas\NetBackup\bin\admincmd\bpmedialist.exe" -m %label%

"C:\Program Files\Veritas\NetBackup\bin\admincmd\bpexpdate.exe" -m %label% -d 0

"C:\Program Files\Veritas\Volmgr\bin\vmquery.exe" -m %label%
```

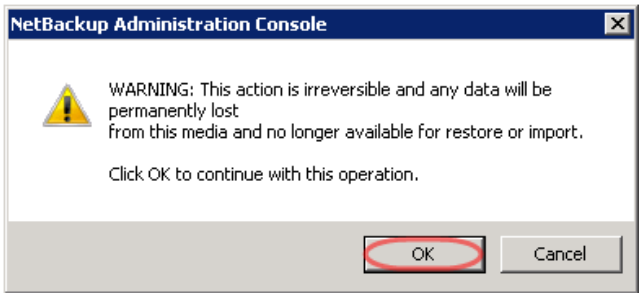
3. The tapes may now be re-labeled, which will clear the data from the tapes.



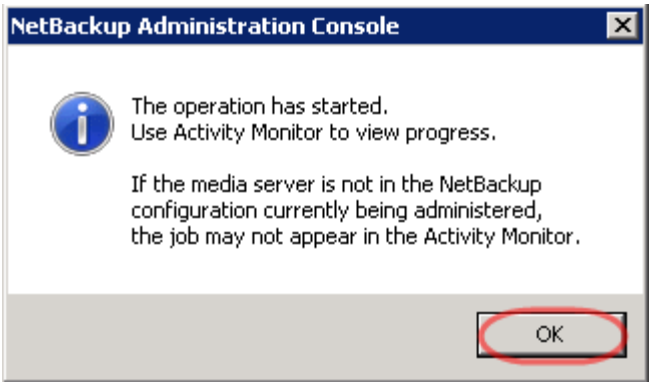
4. Click **OK** in the Label dialog box.



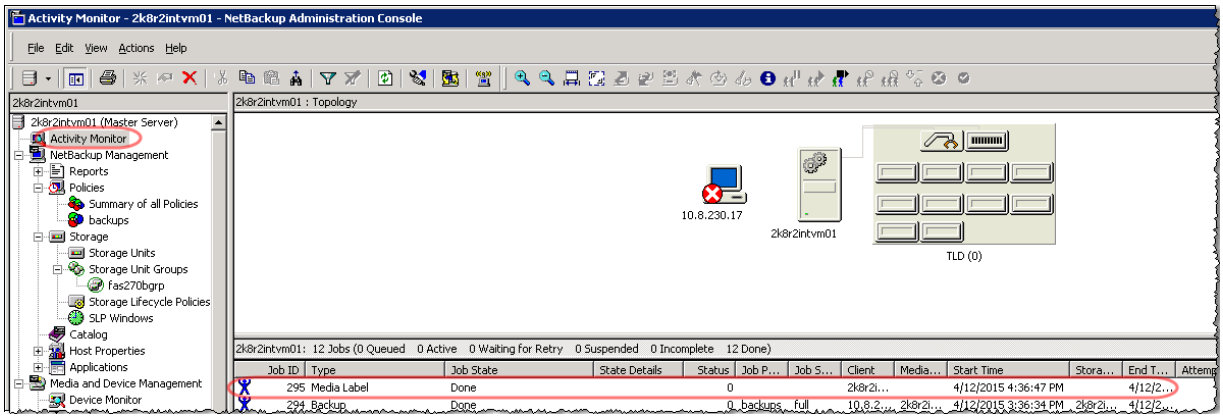
5. Click **OK** in the warning dialog box.



6. Click **OK** in this message dialog box.



7. Monitor the progress of the media labeling from the **Activity Monitor**.



8. Once the reconciliation process has completed on the NetBackup software, from the DR Series system, initiate a cleaning cycle either via the GUI or via the command line. For example:

```
> maintenance --filesystem --reclaim_space
Successfully started cleaner.
```

9. Ensure the space has been reclaimed via the GUI or via the command line. (The **Cleaner Status** should transition from *Running* to *Pending* at which time the statistics should change to reflect the reclaimed space.) For example:

```
> stats --system
Capacity Used                    : 22.0 GiB
Capacity Used in GB              : 23.666
Capacity Free                    : 7970.4 GiB
Capacity Free in GB              : 8558.199
Read Throughput                  : 0.00 MiB/s
Write Throughput                 : 0.00 MiB/s
Current Files                    : 66
Current Bytes                    : 33595753405
Post Dedupe Bytes                : 24926224990
Post Compression Bytes           : 22734553886
Post Encryption Bytes            : 0
Post Encryption Bytes in GiB     : 0.0 GiB
Compression Status               : Done
```