Setting up the Dell DR Series System with IBM Tivoli Storage Manager

Dell Engineering
June 2015

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release
August 2014	Added screenshots where new functionality is introduced in 2014
April 2015	Updated for v3.2 release
June 2015	Updated the cleaner recommendations

Table of contents

Executive summary

This document provides information about how to set up the Dell DR Series as a backup to disk target for IBM Tivoli Storage Manager.

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

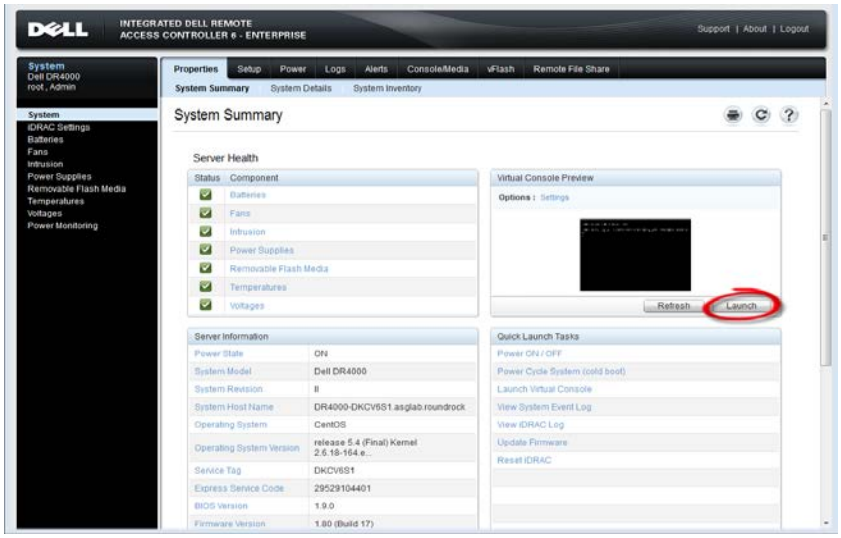
http://www.dell.com/powervaultmanuals

NOTE: The DR Series/Tivoli Storage Manager screen shots used for this document may vary slightly, depending on the versions of the DR Series/Tivoli Storage Manager Software you are using.

1 Installing and configuring the DR Series system

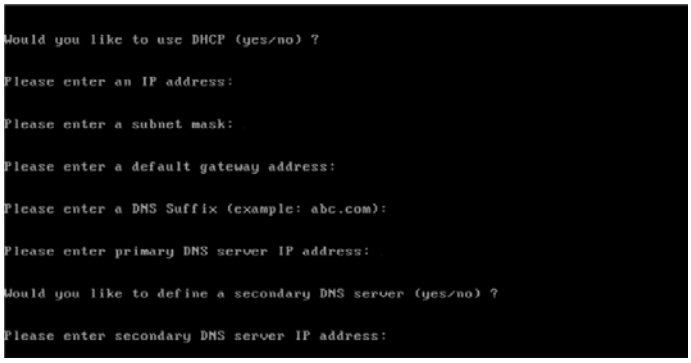
1. Rack and cable the DR Series system, and power it on.
   In the *Dell DR Series System Administrator Guide*, refer to the sections "iDRAC Connection", "Logging in and Initializing the DR Series System", and "Accessing IDRAC6/Idrac7 Using RACADM" for information about using the iDRAC connection and initializing the appliance.

2. Log on to iDRAC using the default address **192.168.0.120** or the IP address that is assigned to the iDRAC interface with the user name and password: **root/calvin.** Launch the virtual console.

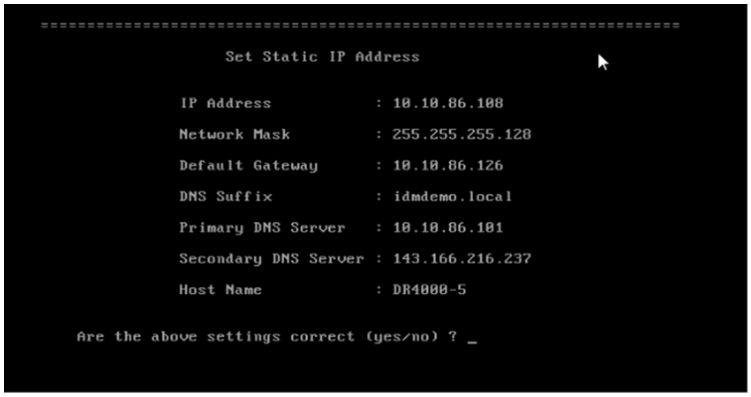


3. After the virtual console is open, log on to the system as the user **administrator** with the password **St0r@ge!** (The "0" in the password is the numeral zero).

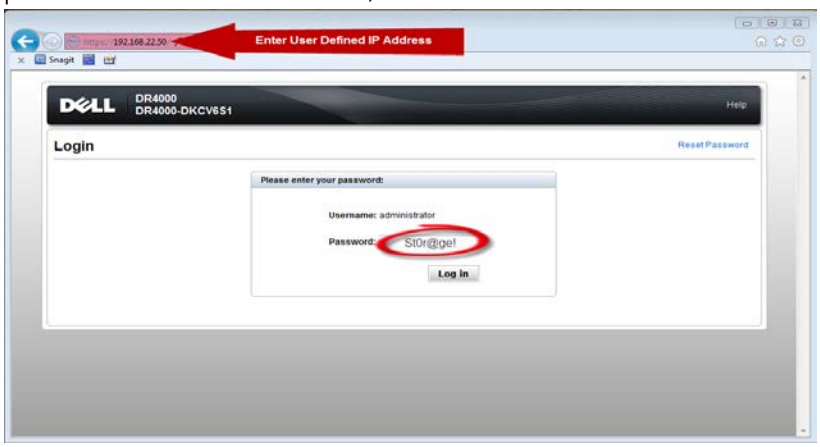
4. Set the user-defined networking preferences.



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

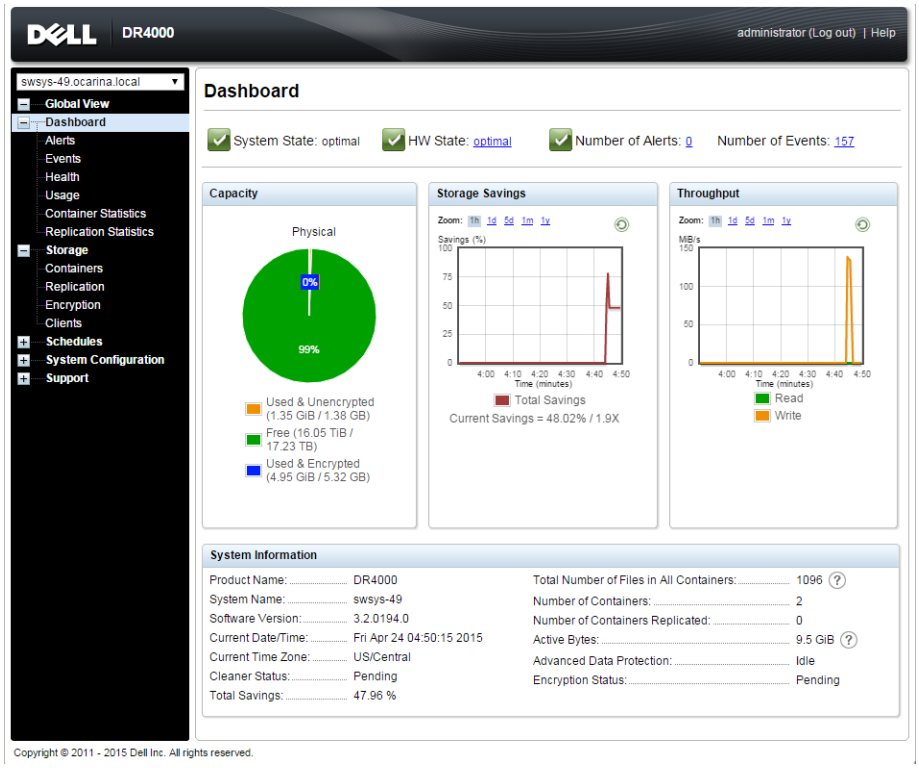


6. Log on to the DR Series system administrator console using the IP address you just provided for the DR Series system with the username: **administrator** and password: **St0r@ge!** (The "0" in the password is the numeral zero.).

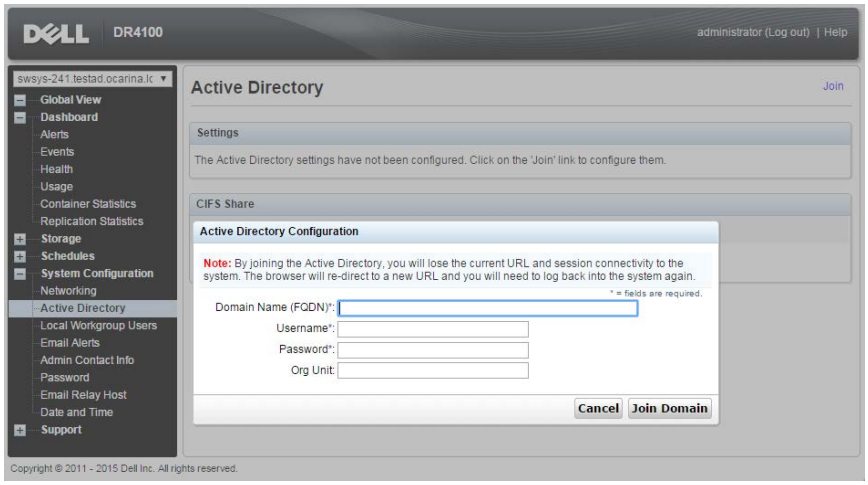


Note: if you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

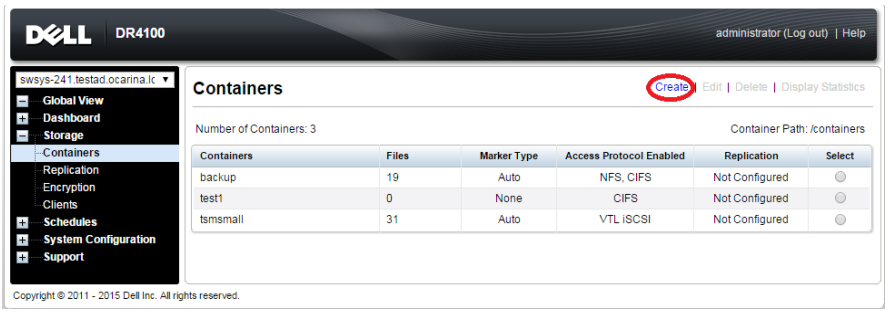
7. Join the DR Series system into the Active Directory domain.
   a. Select **System Configuration** > **Active Directory** from the left navigation area of the DR Series system GUI.



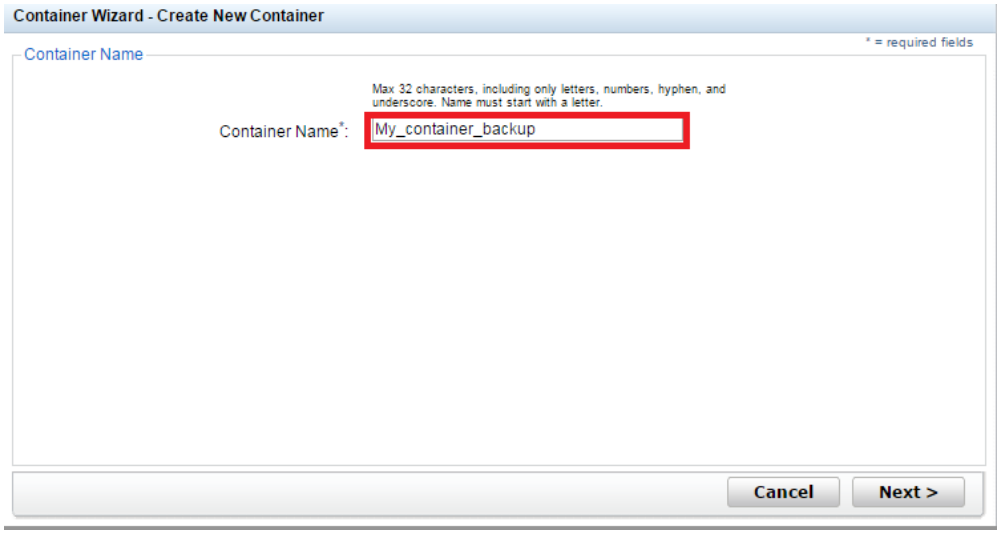
b. Enter your Active Directory credentials.



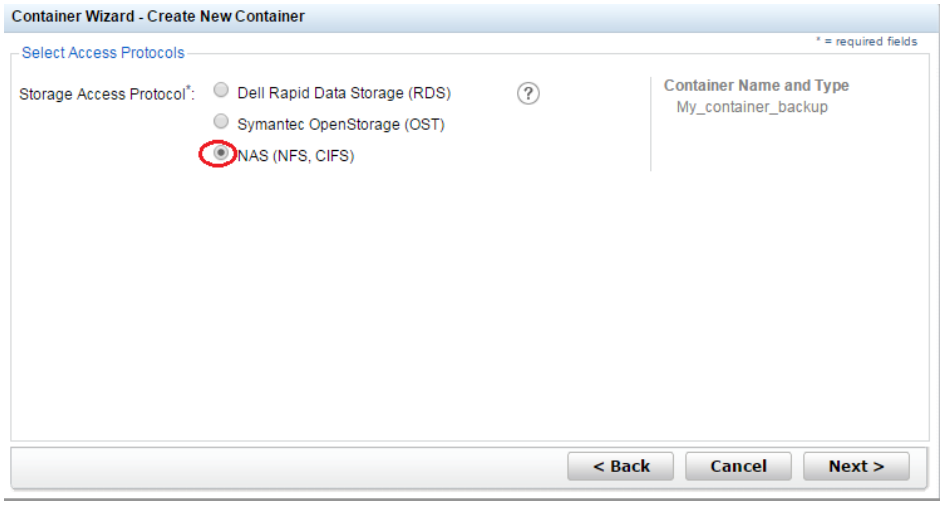
8. Create and mount the container by selecting **Containers** in the left navigation area and then clicking **Create** at the top of the page.



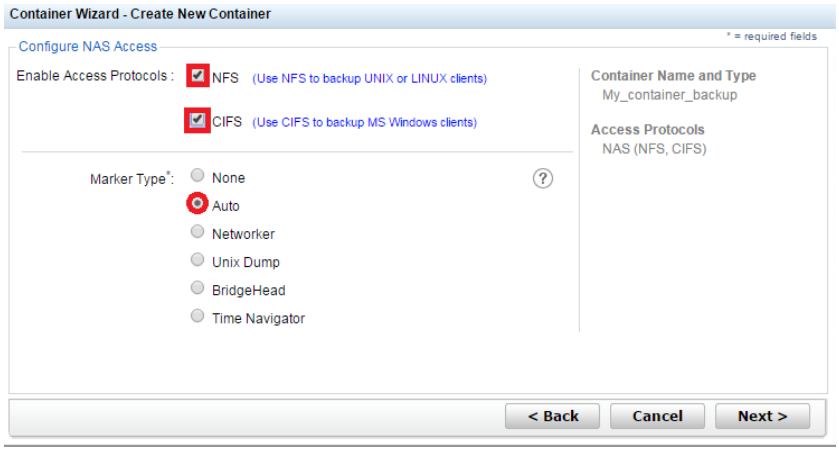
9. Enter a Container Name, and click **Next**.



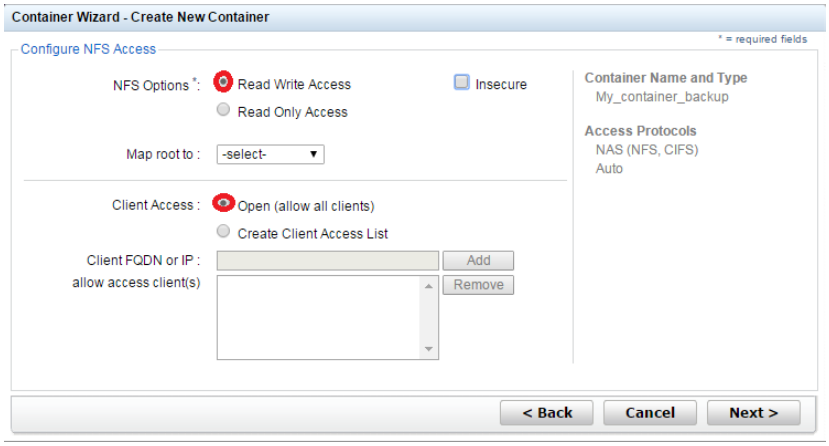
10. Select the storage access protocol you want to use, and then click **Next**.



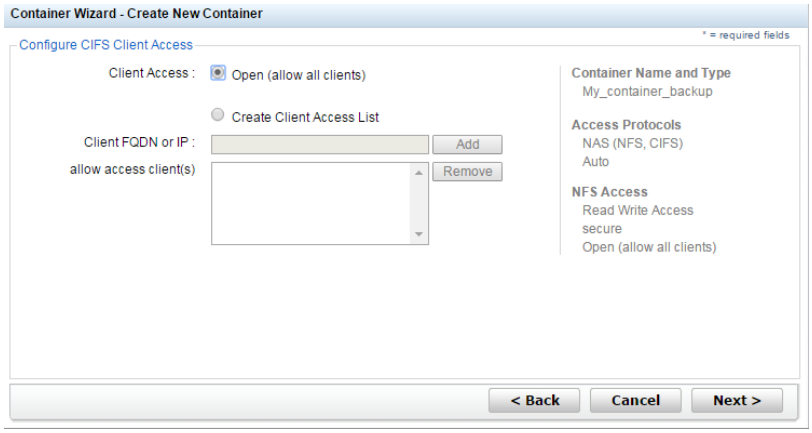
11. Select to Enable Access Protocols (**NFS** or **CIFS**) as appropriate and select the Marker type as **Networker**. Click **Next**.



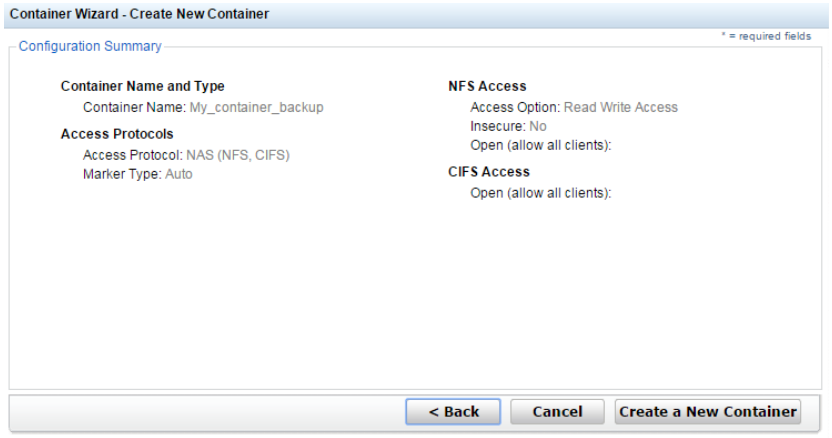
12. For NFS, select the preferred client access credentials, and click **Next**.



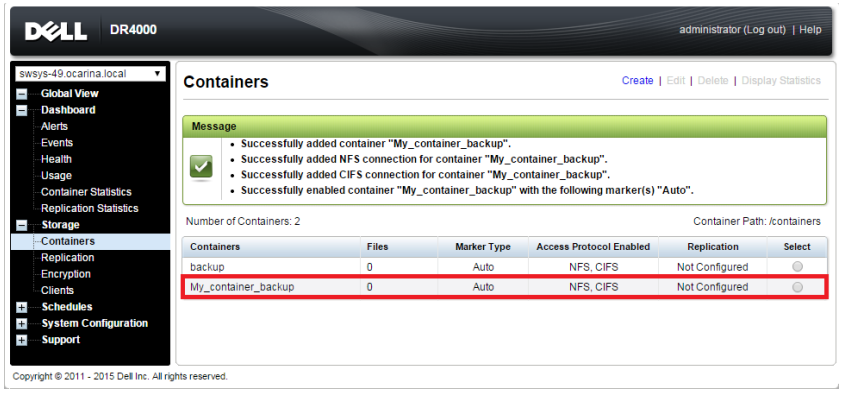
15. For CIFS, select the preferred client access credentials, and click **Next**.



16. Check the configuration summary, and click **Create a New Container**.



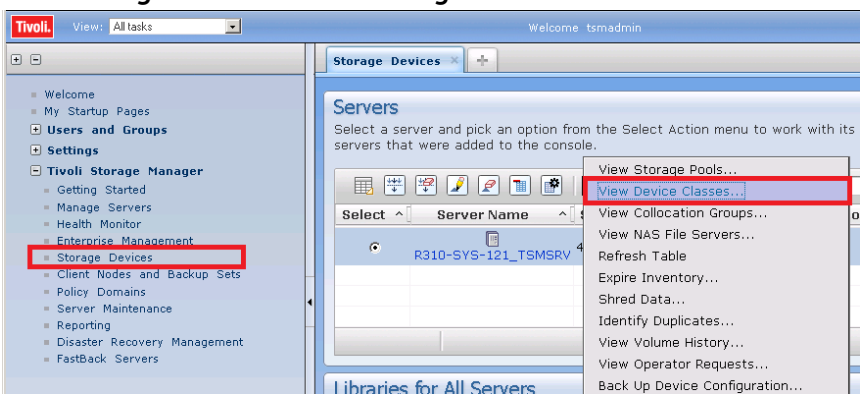
17. Confirm that the container is successfully added on the Containers page.



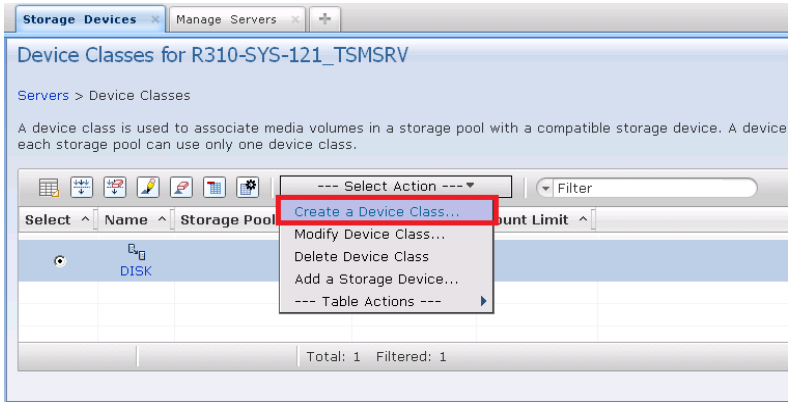
2 Configuring IBM Tivoli Storage Manager

These instructions walk you through a basic configuration for connecting a DR Series system appliance with the Windows version of Tivoli Storage Manager (v6.3).

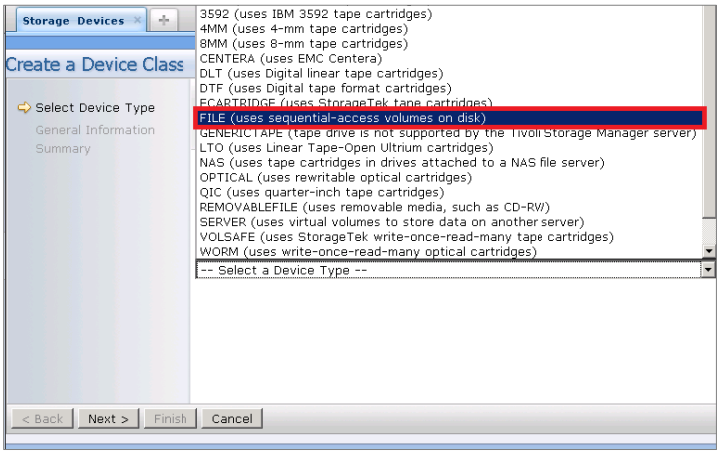
1. Open the IBM Tivoli Storage Manger Administration Center.
2. Click **Storage Devices** > **View Storage Classes**.



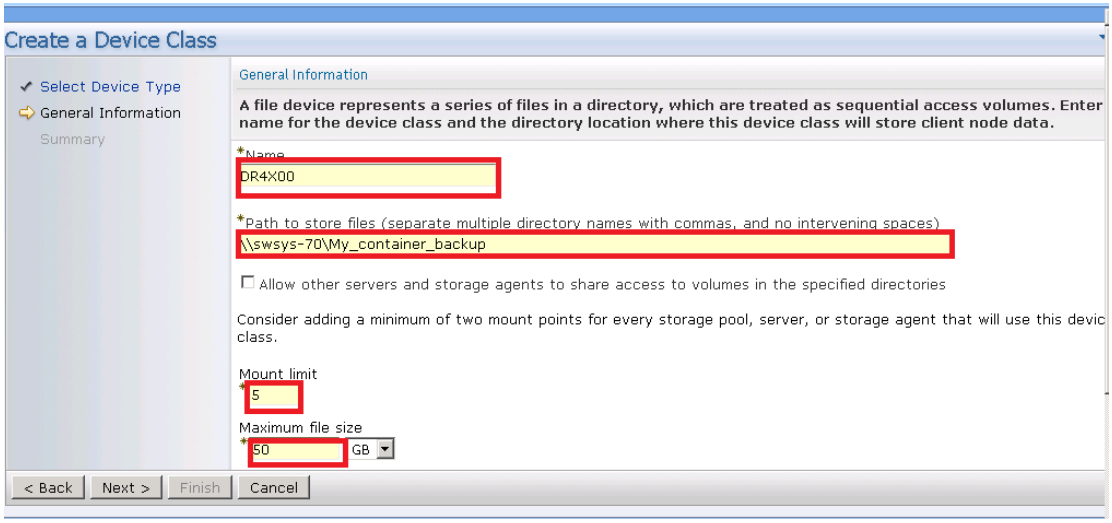
3. Click **Create Device Class**.



4. Select the **FILE** device type and click **Next**. (This device type is optimized for writing to disk based storage.)



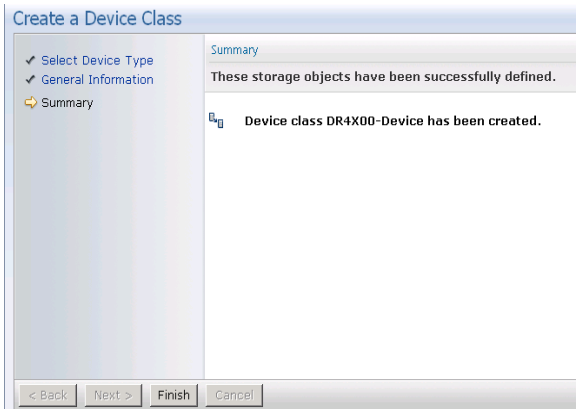
5. Enter the appropriate information under General Information and click **Next**.



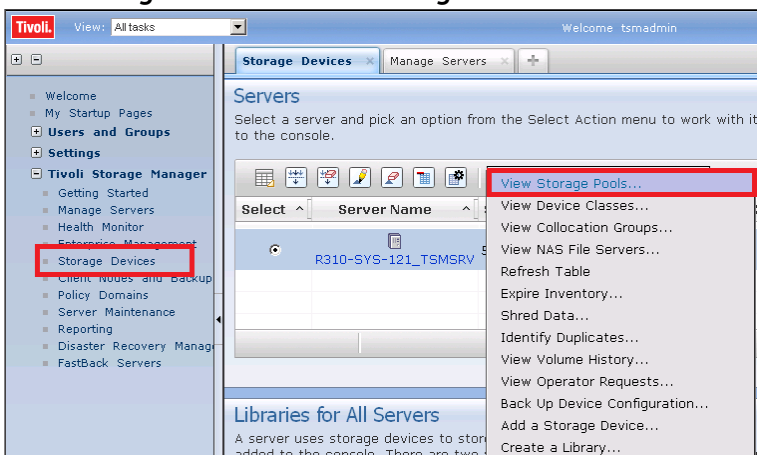
- **Name:** Enter a descriptive name for the device class.
- **Path:** Add the UNC path to the DR container for CIFS and the mount point of DR Series appliance export for NFS.
- **Mount Limit:** Set the limit. The DR Series system supports up to 32 concurrent CIFS connections. The optimal number of connections is five.
- **Maximum File Size:** Set the maximum. The DR Series system supports very large files such as 1TB. The recommended file sizes for TSM are between 1GB and 50GB to allow for fast space reclamation and replication of files to remote sites.

NOTES: The service account for Tivoli Storage Manager needs to have the correct permission to the DR Series system CIFS share for this step to complete successfully. Before providing the information, see Appendix A for information about setting up the TSM service account correctly.

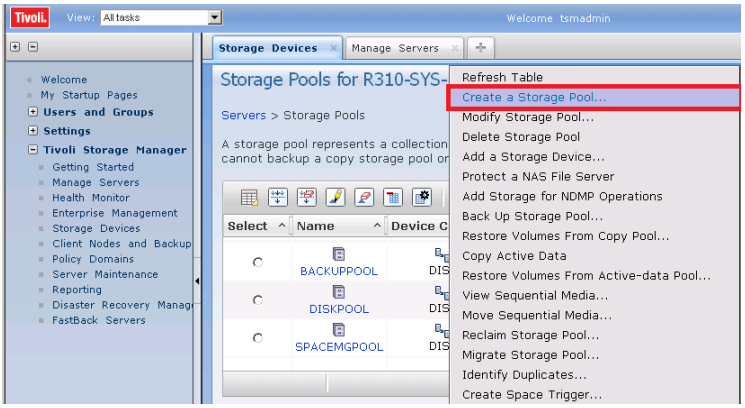
6. Click **Next** and then click **Finish**.



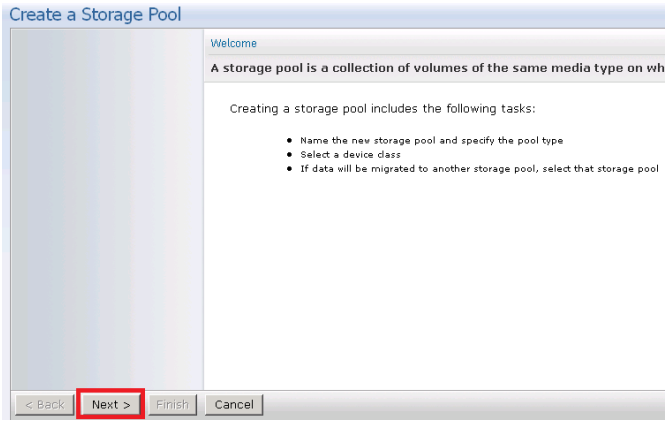
7. Click **Storage Devices** > **View Storage Pools**.



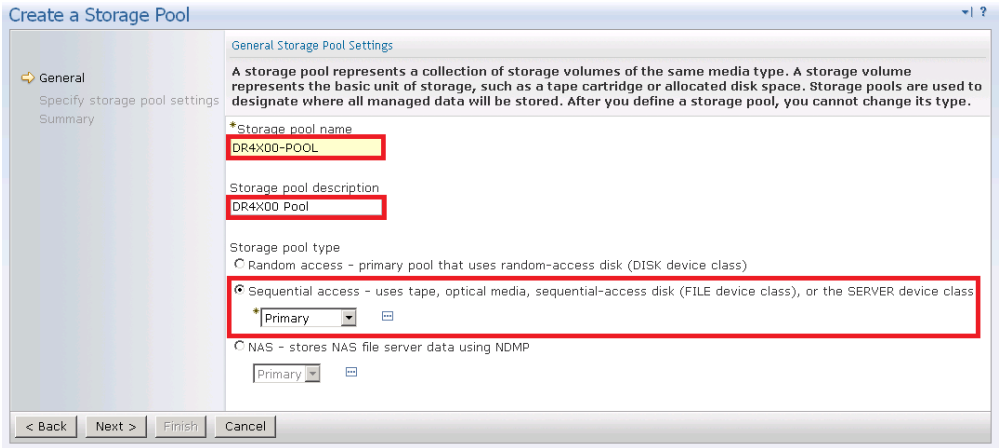
8. Click **Create Storage Pools**.



9. Click **Next**.

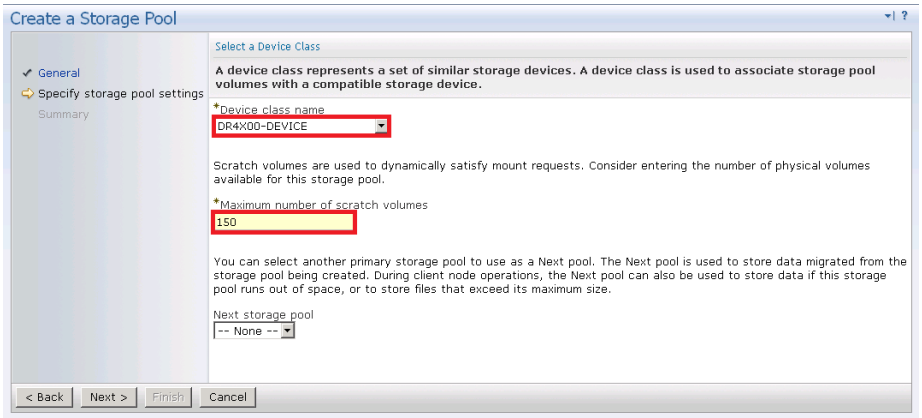


10. Enter the information for General Storage Pool Settings and then click **Next**.



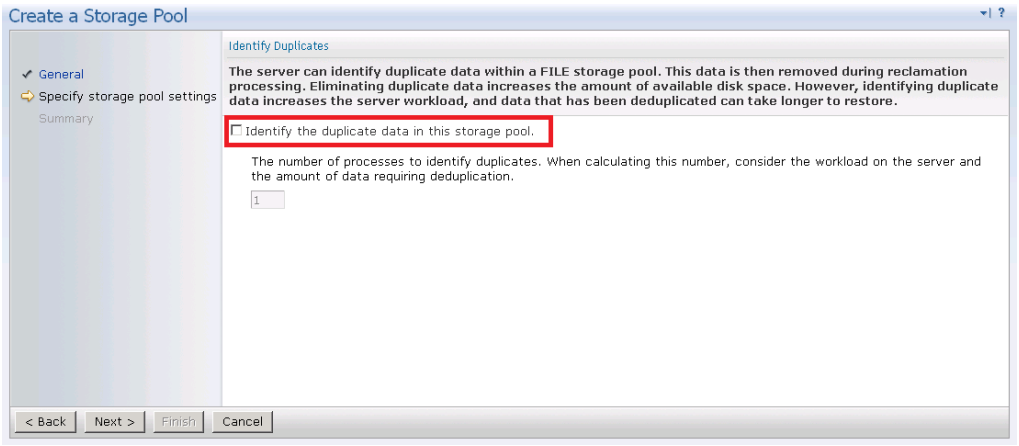
- **Storage Pool Name**: Enter a descriptive name for the DR Series system pool.
- **Storage Pool Description**: Enter a description for the DR Series system pool.
- **Storage Pool Type**: Select **Sequential Access** as the DR Series system is integrated as a FILE type device.

11. Enter the required information for the device class, and click **Next**.



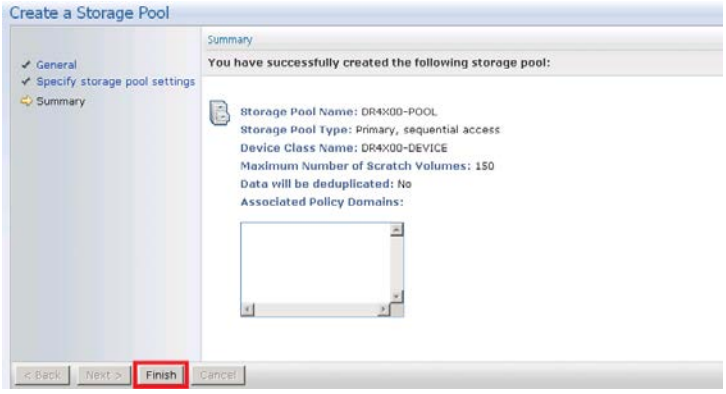
- **Device Class Name:** Select the name of the DR Series system device class (created previously).
- **Maximum Number of Scratch Volumes:** Set the number of scratch volumes in the system. (Setting the value between 100 to 200 scratch volumes is recommended.)

12. For Identifying Duplicates, accept the defaults selections, and click **Next**.

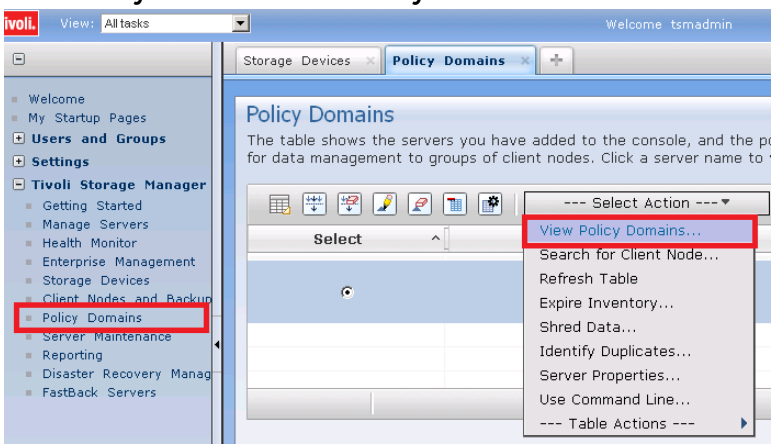


Keep the **Identify the duplicate data in the storage pool** check box clear as the DR Series system uses inline deduplication and already identifies and removes duplicate data.

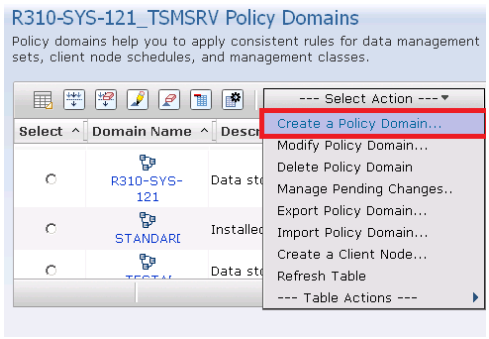
13. Review the settings and click **Finish**.



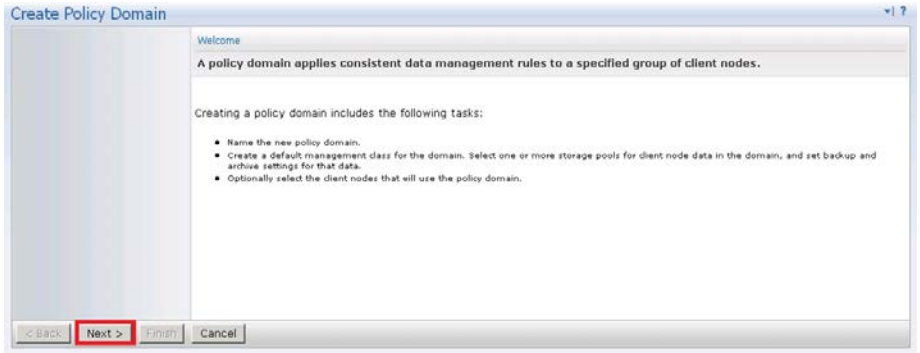
14. Click **Policy Domain** > **View Policy Domain**.



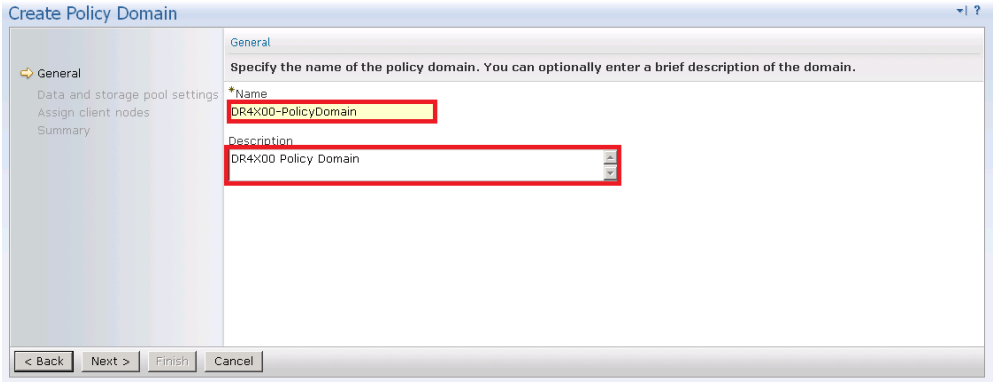
15. Click **Create a Policy Domain**.



16. Click **Next**.

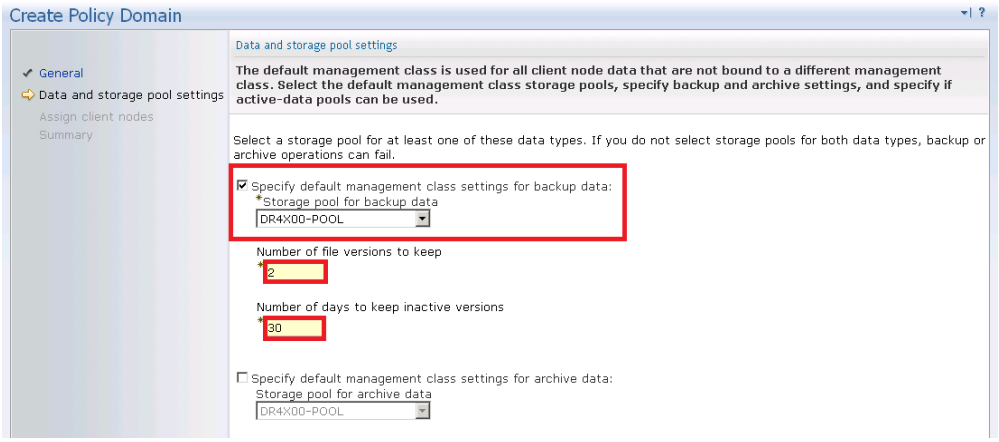


17. Enter the required information and then click **Next**.



Name: Enter a descriptive name for the DR Series system policy domain.
Description: Enter a description for the DR Series policy domain.

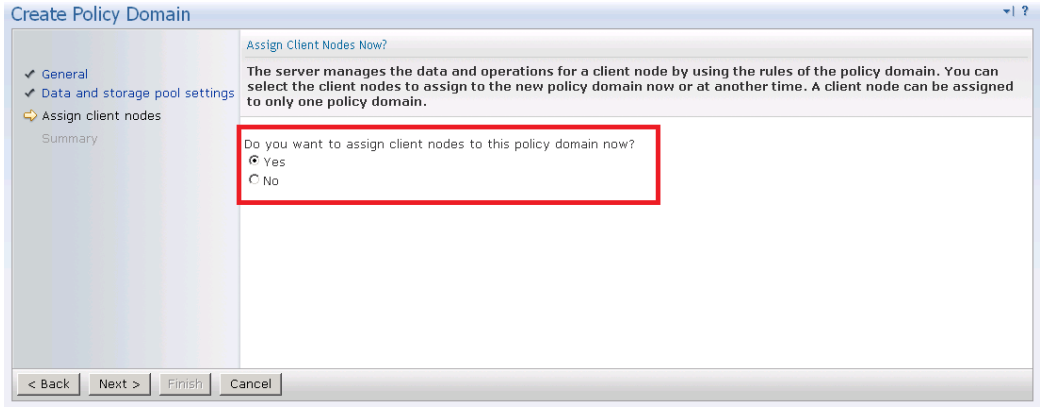
18. Enter the required information for data and storage pool settings, and then click **Next**.



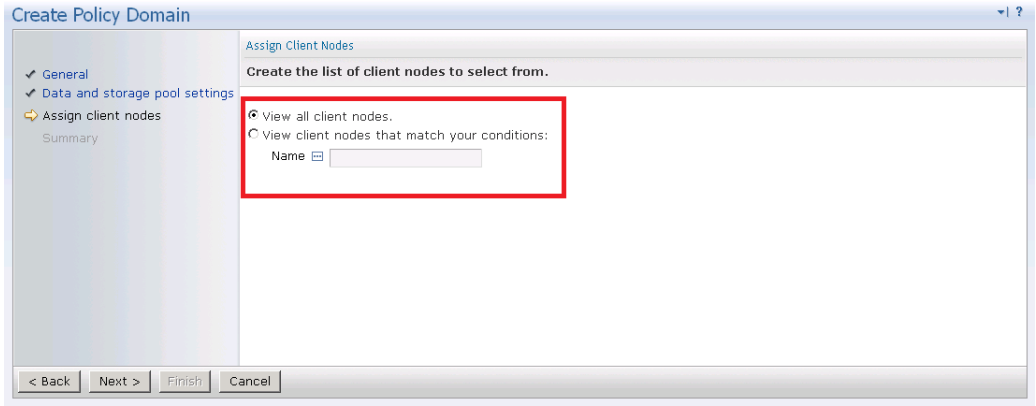
Specify default management class: Select the DR Series system pool that was set up previously.
Number of file versions to Keep: Specify how many versions of a file to keep.
Number of days to keep inactive versions: Specify how many days to retain data after it falls out of policy.

Note: File versions and inactive versions are set based on company policies.

19. Select to assign policy domain to clients, and click **Next**.

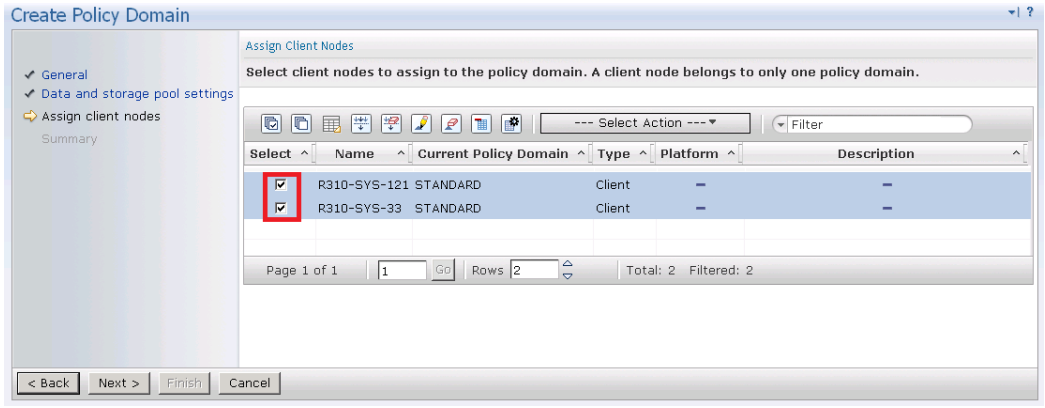


20. Select to display the set of clients to move to the DR Series system, and click **Next**.

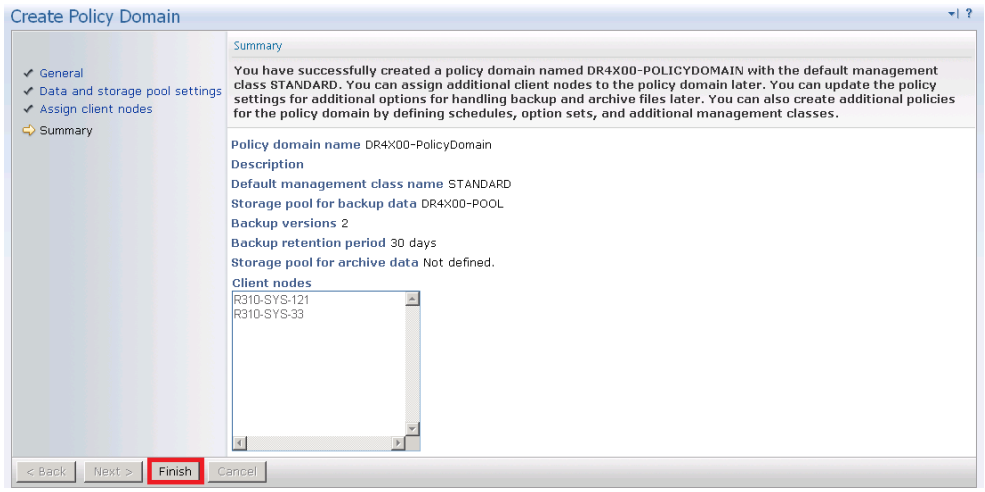


Note: Choose to limit if you have a lot of client computers.

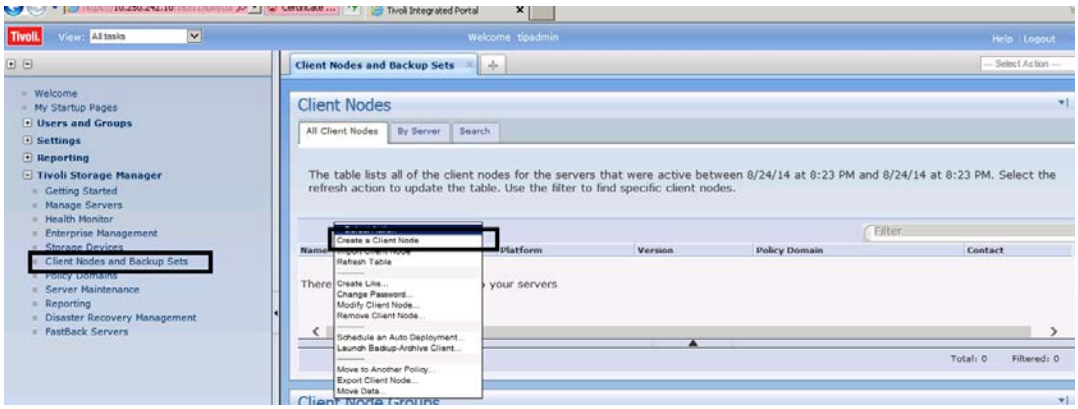
21. Select the checkbox next to the clients you want to back up to the DR Series system, and click **Next**.



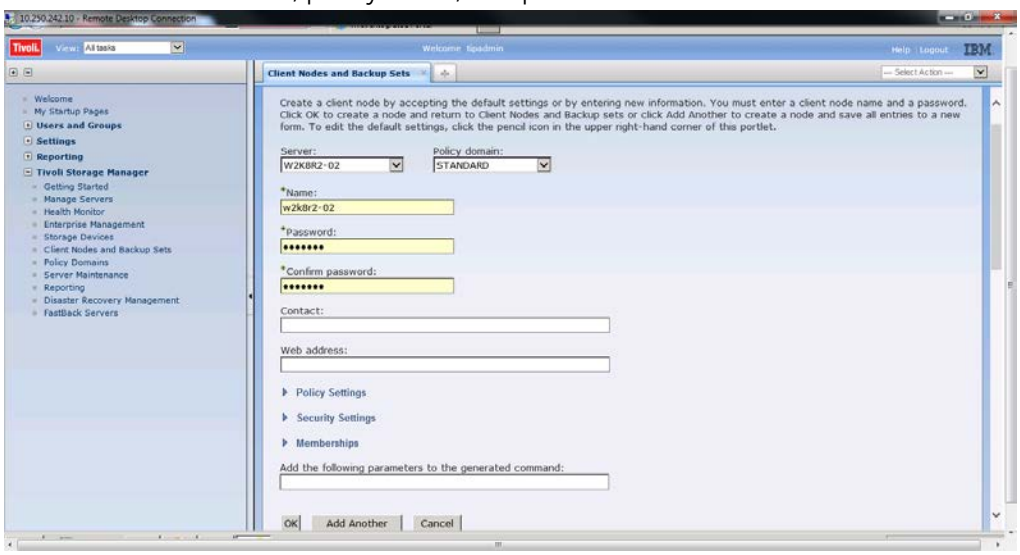
22. Click **Finish**.



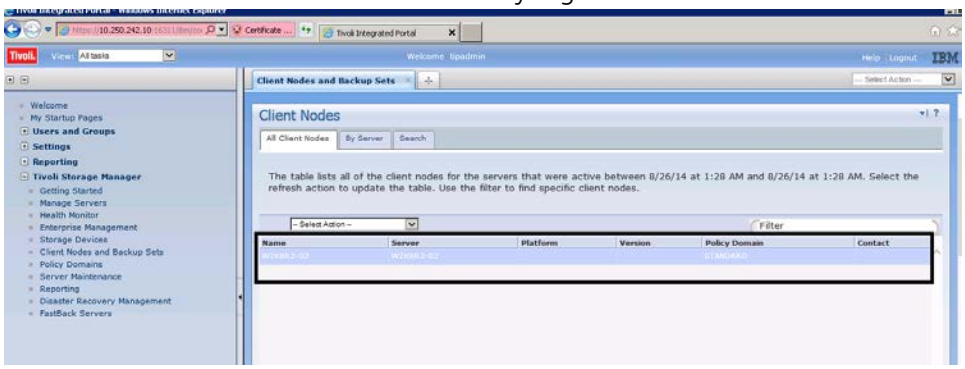
23. Open the client nodes and backup sets from Tivoli Storage Manager to register the client machine.



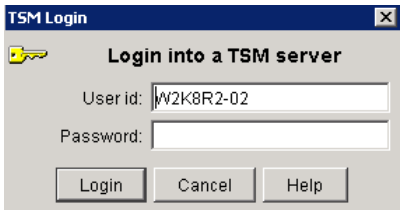
24. Provide the client name, policy name, and password to connect.



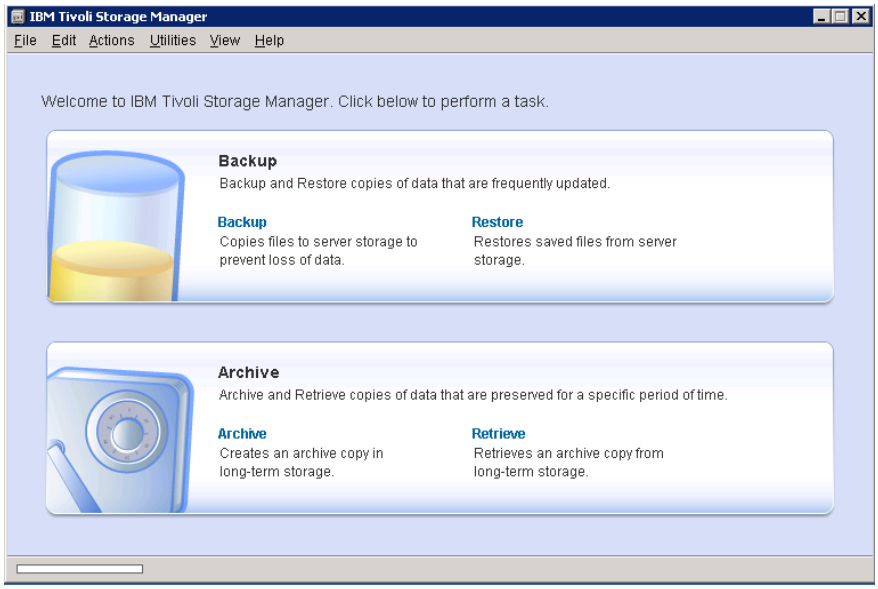
25. Confirm that the client node is successfully registered.



26. On a client machine, open the Backup-Archive GUI. Provide the user ID and password details that were described previously.



When you have logged on, the Backup button will be enabled.



When you have successfully completed the steps above, you have configured the DR Series system for Tivoli Storage Manager. The next time the client is scheduled to back up it will back up to the DR Series system(s).

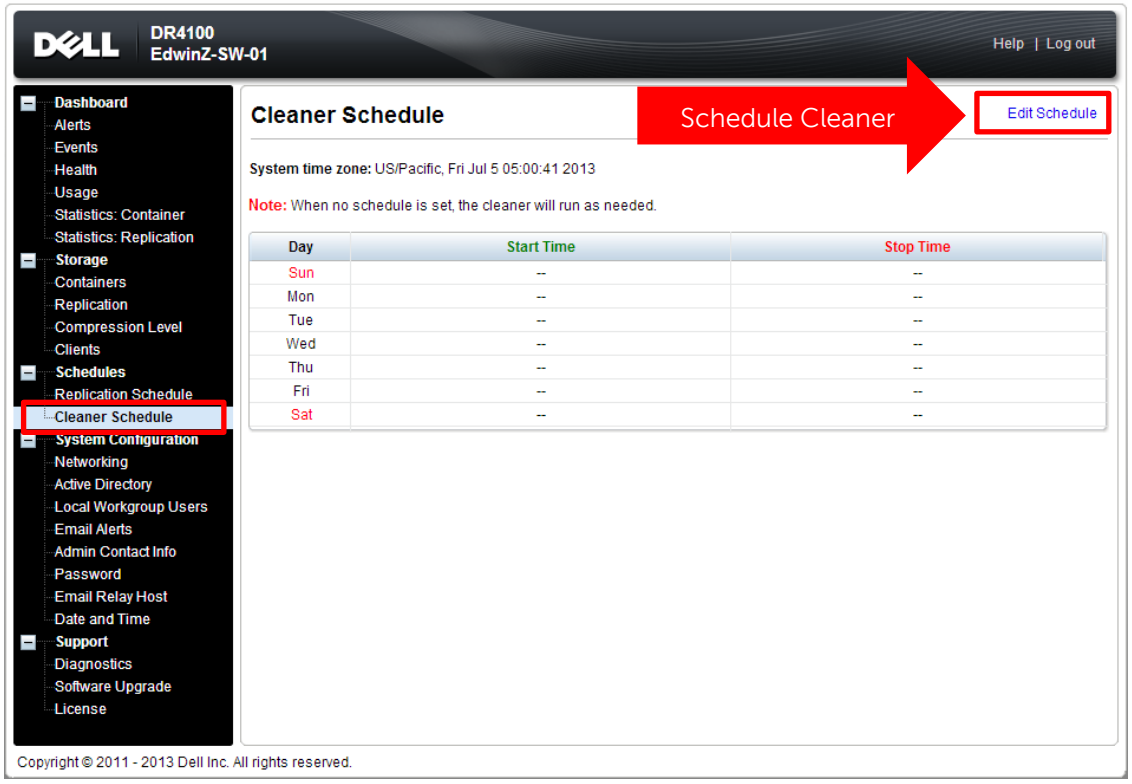
See Appendix B for additional best practices.

3 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 system 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.

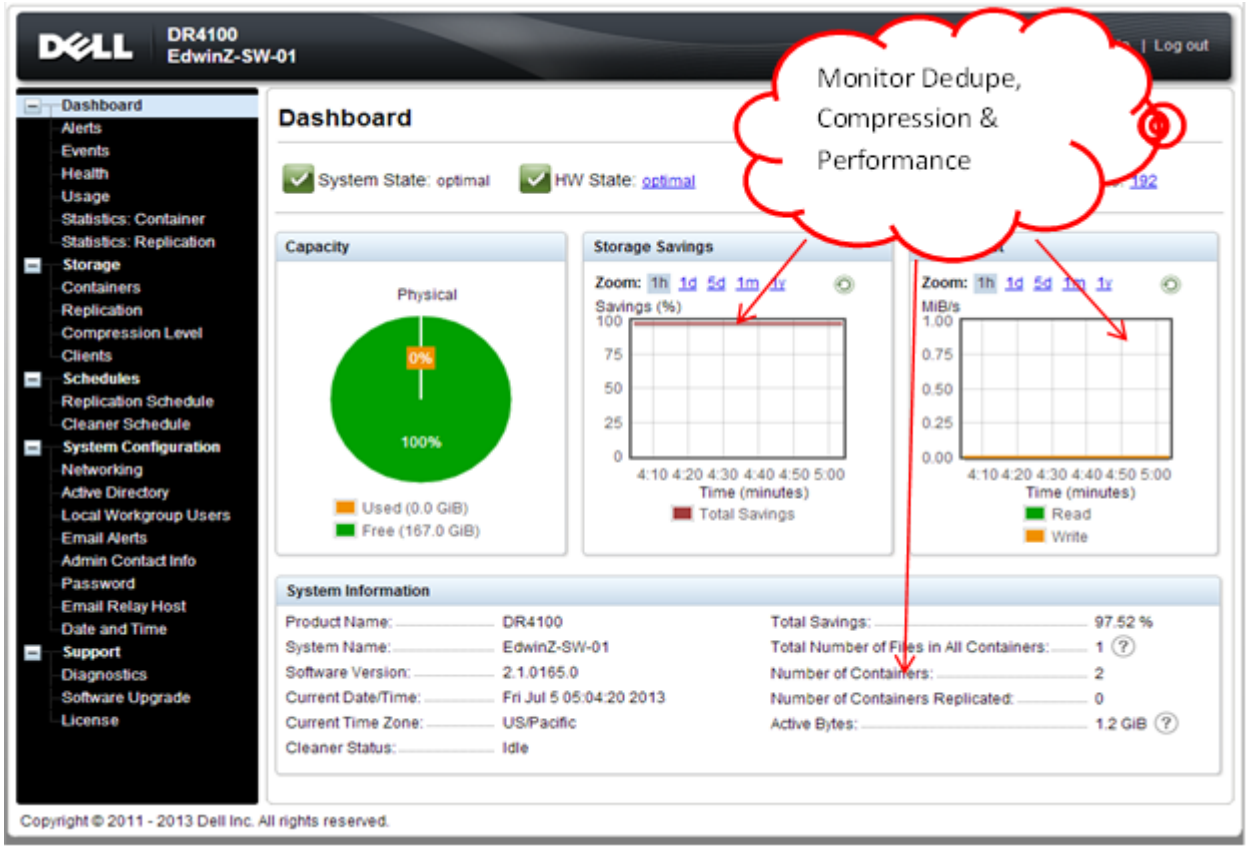
If necessary, you can perform the procedure shown in the following example screenshot to force the cleaner to run. After all of the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place,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



4 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 Configuring CIFS authentication

This appendix describes the steps for sync-ing CIFS authentication between the Tivoli Storage Manager service account and the DR Series system.

There are two methods for allowing the Tivoli Storage Manager service account to authenticate to a DR Series system.

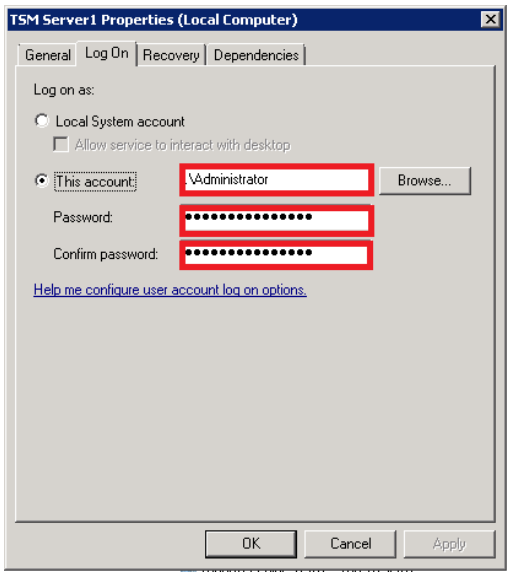
- Integrate the Tivoli Storage Manager Media Server and DR Series system with Active Directory.
  - Ensure the AD user has appropriate ACLs to the DR4X00 Container
  - Set the TSM Server service to run with <Domain\User>
- Sync local usernames and passwords between the DR Series system and the Tivoli Storage Manager media server. To set the password for the local CIFS administrator on the DR Series system, log on to the DR Series system using SSH.
  - Logon with the credentials: administrator/St0r@ge!
  - Run the following command: `authenticate --set --user administrator`

```
administrator@SWSYS-70 > authenticate --set --user administrator
Enter new password for CIFS user administrator:
Re-enter new password for CIFS user administrator:
Changed administrator's password.
```

Note: The CIFS administrator is a different account than the administrator used to administer the DR Series system.

When an authentication method has been selected, set the Tivoli Storage Manager service account to use that account.

1. Launch the Microsoft Services Snap-in. (Start > Run > Services.msc > Enter).
2. Locate the TSM Server Service (Right-click > Properties > Logon tab.)



Note: If you are using local sync'ed accounts instead of an Active Directory account, make sure that there is a ".\"in front of the user name.

3. Click OK.
4. Right-click the TSM Service process, and click Stop/Start to restart the process.

B Best practices/considerations

B.1 Deduplication

The DR Series system has inline deduplication built-in and does not require any additional deduplication to be done ahead of data being written to the DR Series system. The system will remove any redundancies in the data before the data is stored on disk.

Enabling deduplication before the data stream is sent to the DR Series system will cause the data to be obfuscated, not allowing the system to achieve optimal dedupe savings. It is highly recommended that deduplication is not done before the data stream is sent to the DR Series system.

B.2 Compression

The DR Series system has compression built-in and does not require any additional compression to be done ahead of data being written to the DR Series system. The system will remove any redundancies in the data before being stored on disk.

Enabling compression before the data stream is sent to the DR Series system will cause the data to be obfuscated, not allowing the system to achieve optimal savings. It is highly recommended that compression is not done before the data stream is sent to the DR Series system.

B.3 Encryption

The DR Series system supports encryption-at-rest; hence there is no need to enable encryption for the data management application.

Enabling encryption before the data stream is sent to the DR Series system will cause the data to be obfuscated, not allowing the DR series devices to achieve optimal savings. It is highly recommended that encryption is not done before the data stream is sent to the DR Series system. It supports encryption on the wire for transferring data to remote sites using replication.

B.4 Space reclamation

For optimal performance, DR Series system and Tivoli Storage Manager backup and space reclamations jobs should be scheduled to happen at different times.