



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

Dell Engineering  
May 2016

## 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
May 2016	Updated with ISCSI VTL support and instructions

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2016 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, 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. IBM®, Tivoli, and Storage Manager are trademarks or registered trademarks of International Business Machines Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

# Table of contents

1	Installing and configuring the DR Series system .....	5
1.1	Creating a container (NFS/CIFS).....	8
1.2	Creating a VTL container with an iSCSI connection .....	10
2	Configuring IBM Tivoli Storage Manager for CIFS & NFS target containers .....	13
2.1	Configuring the device class for CIFS & NFS protocols .....	13
2.2	Configuring the storage pool for CIFS & NFS protocols.....	16
2.3	Creating a policy domain for the backup job .....	19
2.4	Creating client node and backup sets.....	23
3	Creating and configuring iSCSI target container(s) for TSM .....	25
3.1	Configuring the iSCSI initiator.....	25
3.1.1	Configuring iSCSI initiator for Windows.....	25
3.1.2	Configuring the iSCSI initiator – Linux.....	29
3.2	Configuring DR Series system VTL for Windows and Linux TSM servers .....	30
3.2.1	Configuring the DR Series system VTL for Windows .....	30
3.2.2	Configuring the DR Series system VTL for Linux.....	31
3.3	Configuring the device class for iSCSI VTL.....	32
3.4	Configuring the storage pool for iSCSI VTL .....	33
3.4.1	Adding volumes to a library .....	35
3.4.2	Adding volumes to a storage pool.....	39
3.5	Creating the policy domain for iSCSI VTL.....	41
3.6	Creating the client node for iSCSI VTL .....	41
4	Using the Backup & Archive GUI .....	42
5	Setting up the DR Series system cleaner .....	43
6	Monitoring deduplication, compression, and performance .....	44
A	Configuring CIFS authentication .....	45
B	Best practices/considerations .....	47
B.1	Deduplication .....	47
B.2	Compression.....	47
B.3	Encryption .....	47
B.4	Space reclamation.....	47
C	Configuring the tape library devices on Linux .....	48



## Executive summary

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

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

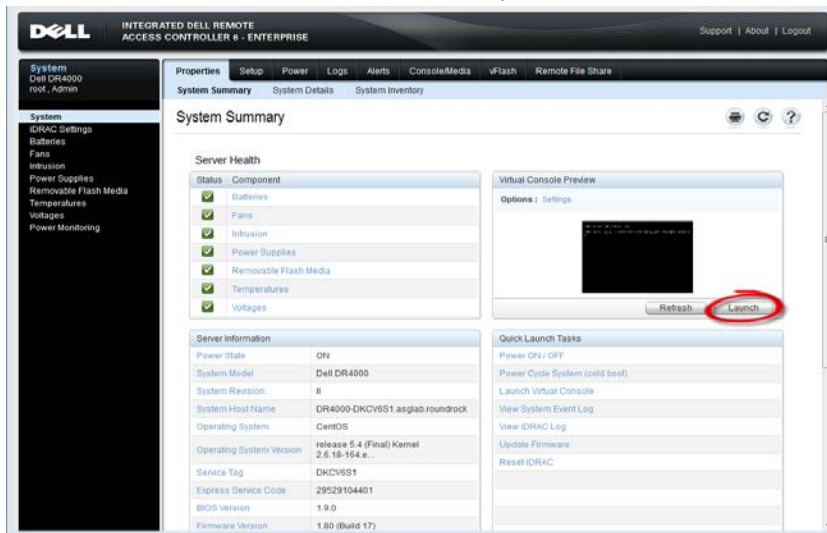
<http://www.dell.com/support/home>

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



# 1 Installing and configuring the DR Series system

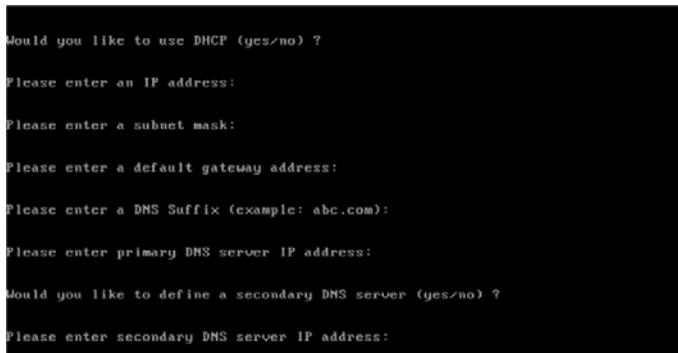
1. Rack and cable the DR Series system, and power it on.  
In the *Dell DR Series System Administrator Guide*, refer to the sections “iDRAC Connection”, “Logging in and Initializing the DR Series System”, and “Accessing iDRAC6/Idrac7 Using RACADM” for information about using the iDRAC connection and 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.

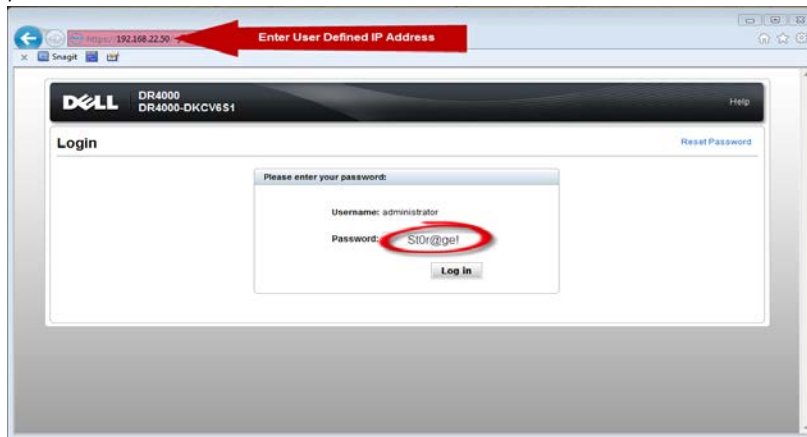


5. View the summary of preferences and confirm that it is correct.

```
=====
                          Set Static IP Address
IP Address      : 10.10.86.108
Network Mask   : 255.255.255.128
Default Gateway : 10.10.86.126
DNS Suffix     : idmdemo.local
Primary DNS Server : 10.10.86.101
Secondary DNS Server : 143.166.216.237
Host Name      : DR4000-5

Are the above settings correct (yes/no) ? _
```

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.



DELL DR4000 administrator (Log out) | Help

swws-49.ocarina.local

Global View

Dashboard

Alerts

Events

Health

Usage

Container Statistics

Replication Statistics

Storage

Containers

Replication

Encryption

Clients

Schedules

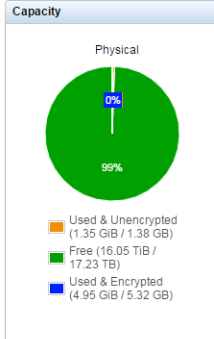
System Configuration

Support

### Dashboard

System State: optimal HW State: optimal Number of Alerts: 0 Number of Events: 157

#### Capacity



Physical

- Used & Unencrypted (1.35 GiB / 1.38 GB)
- Free (16.05 TiB / 17.23 TB)
- Used & Encrypted (4.95 GiB / 5.32 GB)

#### Storage Savings



Zoom: 1h 1d 1w 1m 1y

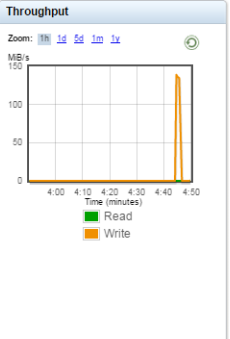
Savings (%)

Time (minutes)

Total Savings

Current Savings = 48.02% / 1.9X

#### Throughput



Zoom: 1h 1d 1w 1m 1y

MB/s

Time (minutes)

Read

Write

#### System Information

Product Name: DR4000	Total Number of Files in All Containers: 1096
System Name: swws-49	Number of Containers: 2
Software Version: 3.2.0194.0	Number of Containers Replicated: 0
Current Date/Time: Fri Apr 24 04:50:15 2015	Active Bytes: 9.5 GiB
Current Time Zone: US/Central	Advanced Data Protection: Idle
Cleaner Status: Pending	Encryption Status: Pending
Total Savings: 47.96%	

Copyright © 2011 - 2015 Dell Inc. All rights reserved.

b. Enter your Active Directory credentials.

DELL DR4100 administrator (Log out) | Help

swws-241.testad.ocarina.local

Global View

Dashboard

Alerts

Events

Health

Usage

Container Statistics

Replication Statistics

Storage

Schedules

System Configuration

Networking

Active Directory

Local Workgroup Users

Email Alerts

Admin Contact Info

Password

Email Relay Host

Date and Time

Support

### Active Directory

Join

Settings

The Active Directory settings have not been configured. Click on the 'Join' link to configure them.

CIFS Share

#### Active Directory Configuration

**Note:** By joining the Active Directory, you will lose the current URL and session connectivity to the system. The browser will re-direct to a new URL and you will need to log back into the system again.

\* = fields are required.

Domain Name (FQDN):

Username:

Password:

Org Unit:

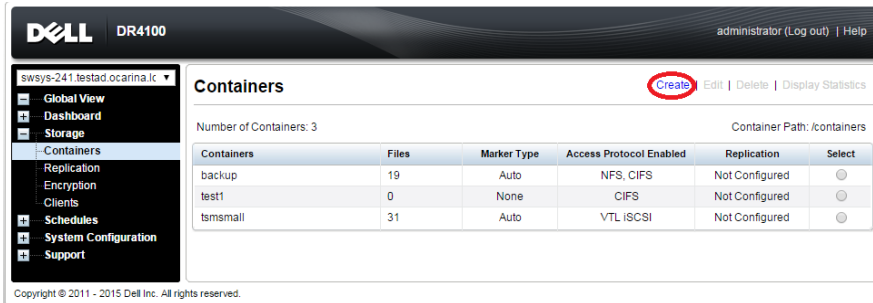
Cancel Join Domain

Copyright © 2011 - 2015 Dell Inc. All rights reserved.



## 1.1 Creating a container (NFS/CIFS)

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



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

The screenshot shows the 'Container Wizard - Create New Container' step. The 'Container Name' field is highlighted with a red box and contains the text 'My\_Container\_Backup'. A note above the field states: 'Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter.' Below the field is a checkbox for 'Virtual Tape Library (VTL):' which is unchecked. At the bottom right, the 'Next >' button is highlighted with a red box, and the 'Cancel' button is also visible.

3. Select the storage access protocol as **NAS**, and then click **Next**.

The screenshot shows the 'Container Wizard - Create New Container' step for selecting the storage access protocol. The 'Select Access Protocols' section has three radio buttons: 'Dell Rapid Data Storage (RDS)', 'Symantec OpenStorage (OST)', and 'NAS (NFS, CIFS)'. The 'NAS (NFS, CIFS)' option is selected and circled in red. To the right, the 'Container Name and Type' section shows 'My\_container\_backup'. At the bottom, the 'Next >' button is highlighted with a red box, and the '< Back' and 'Cancel' buttons are also visible.



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

**Container Wizard - Create New Container** \* = required fields

Configure NAS Access

Enable Access Protocols:  NFS (Use NFS to backup UNIX or LINUX clients)  CIFS (Use CIFS to backup MS Windows clients)

Marker Type\*:  None  Auto  Networker  Unix Dump  BridgeHead  Time Navigator

Container Name and Type: My\_container\_backup

Access Protocols: NAS (NFS, CIFS)

< Back Cancel Next >

- Configure access by doing one of the following:
  - For NFS, select the preferred client access credentials, and click **Next**.

**Container Wizard - Create New Container** \* = required fields

Configure NFS Access

NFS Options\*:  Read Write Access  Read Only Access  Insecure

Map root to: -select-

Client Access:  Open (allow all clients)  Create Client Access List

Client FQDN or IP:  Add

allow access client(s):  Remove

Container Name and Type: My\_container\_backup

Access Protocols: NAS (NFS, CIFS) Auto

< Back Cancel Next >

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

**Container Wizard - Create New Container** \* = required fields

Configure CIFS Client Access

Client Access:  Open (allow all clients)  Create Client Access List

Client FQDN or IP:  Add

allow access client(s):  Remove

Container Name and Type: My\_container\_backup

Access Protocols: NAS (NFS, CIFS) Auto

NFS Access: Read Write Access secure Open (allow all clients)

< Back Cancel Next >



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

Container Wizard - Create New Container \* = required fields

Configuration Summary

<p><b>Container Name and Type</b> Container Name: My_container_backup</p> <p><b>Access Protocols</b> Access Protocol: NAS (NFS, CIFS) Marker Type: Auto</p>	<p><b>NFS Access</b> Access Option: Read Write Access Insecure: No Open (allow all clients):</p> <p><b>CIFS Access</b> Open (allow all clients):</p>
---	--

## 1.2 Creating a VTL container with an iSCSI connection

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

The screenshot shows the Dell DR4100 web interface. The left navigation pane has 'Containers' selected. The main content area shows a 'Containers' table with 3 containers listed. The 'Create' button at the top right of the table is circled in red.

Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
backup	19	Auto	NFS, CIFS	Not Configured	<input type="radio"/>
test1	0	None	CIFS	Not Configured	<input type="radio"/>
tmsmall	31	Auto	VTL iSCSI	Not Configured	<input type="radio"/>

2. Enter a container name, select the **VTL** option, and then click **Next**.

Container Wizard - Create New Container \* = required fields

Container Name \* = required fields

Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter.

Container Name\*:

Virtual Tape Library (VTL):



3. Select the required tape size, the access protocol as **iSCSI**, and the marker type. Also, enter the initiator details as appropriate. Click **Next**.

**Edit Container: TSM-iscsi** \* = required fields

Configure Virtual Tape Library

Is OEM:

Tape Size:  800GB  400GB  200GB  
 100GB  50GB  10GB

Access Protocol:  NDMP  iSCSI  No Access

Access Control (initiator):

Add Tapes (no. of tapes):  ?

Marker Type:  Unix Dump  Networker  BridgeHead  
 None  Auto  Time Navigator

Container Name and Type  
TSM-iscsi  
VTL

**Cancel** **Next >**

4. Click **Create a New Container**.

**Container Wizard - Create New Container** \* = required fields

Configuration Summary

Container Name and Type	Virtual Tape Library
Container Name: TSM-iscsi	OEM: no
Connection Type: VTL	Tape Size: 800gb
	Access Protocol: iSCSI
	Access Control: 10.250.209.35
	Marker Type: Auto

**< Back** **Cancel** **Create a New Container**



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

The screenshot shows the Dell DR4000 web interface. The top navigation bar includes the Dell logo, 'DR4000', and user information 'root (Log out) | Help'. A left sidebar contains a navigation menu with categories like Global View, Dashboard, Alerts, Events, Health, Usage, Container Statistics, Replication Statistics, Storage, Replication, Encryption, Clients, Schedules, System Configuration, and Support. The main content area is titled 'Containers' and includes a 'Message' box with a green checkmark and two bullet points: 'Successfully added container "TSM-iscsi".' and 'Successfully enabled container "TSM-iscsi" with the following marker(s) "Auto".'. Below the message, it states 'Number of Containers: 15' and 'Container Path: /containers'. A table lists the containers with columns for Container Name, Files, Marker Type, Access Protocol Enabled, Replication, and Select. The 'TSM-iscsi' container is highlighted with a red border.

Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
back_cifs	0	Auto	CIFS	Not Configured	<input type="radio"/>
backis	31	Auto	VTL ISCSI	Not Configured	<input type="radio"/>
backup	19	Auto	NFS, CIFS	Not Configured	<input type="radio"/>
Backup1	0	None	CIFS	Not Configured	<input type="radio"/>
data	2258	None	CIFS	Not Configured	<input type="radio"/>
esh-bkup	8	None	CIFS	Not Configured	<input type="radio"/>
hpdata	14	None	CIFS	Not Configured	<input type="radio"/>
largedata	31	Auto	VTL ISCSI	Not Configured	<input type="radio"/>
sav2	2	HP_DataProtector	NFS	Not Configured	<input type="radio"/>
savings	0	None	CIFS	Not Configured	<input type="radio"/>
source	0	None	CIFS	Not Configured	<input type="radio"/>
source1	0	None	CIFS	Not Configured	<input type="radio"/>
target	0	None	CIFS	Online	<input type="radio"/>
target1	1	None	CIFS	Not Configured	<input type="radio"/>
TSM-iscsi	0	Auto	VTL	Not Configured	<input type="radio"/>

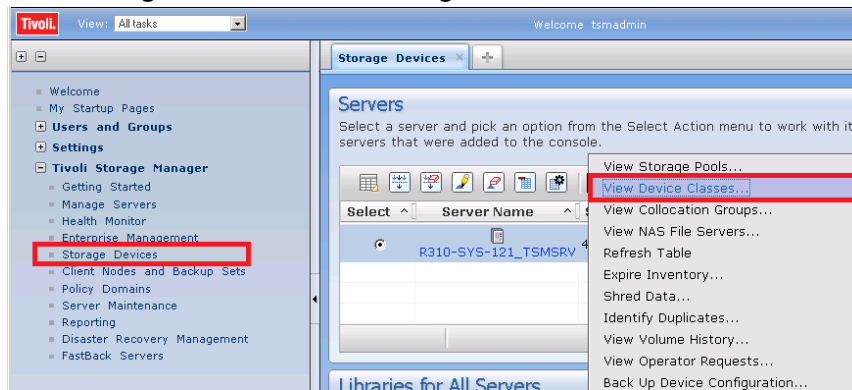


## 2 Configuring IBM Tivoli Storage Manager for CIFS & NFS target containers

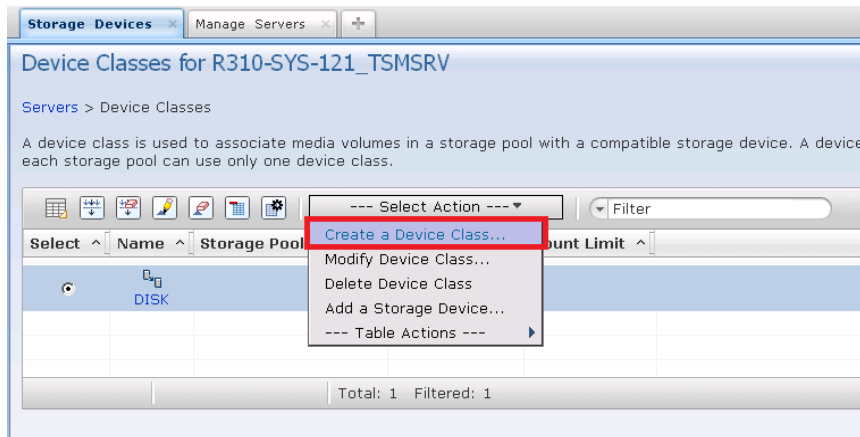
### 2.1 Configuring the device class for CIFS & NFS protocols

The following instructions describe a basic configuration for connecting a DR Series system to the Windows version of IBM Tivoli Storage Manager (TSM) version 7.1.4.

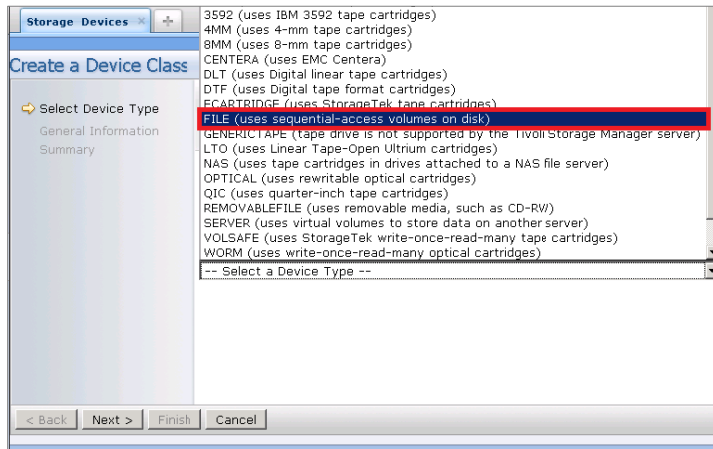
1. Open the IBM Tivoli Storage Manger Administration Center.
2. Click **Storage Devices > View Storage Classes**.



3. Click **Create a Device Class**.



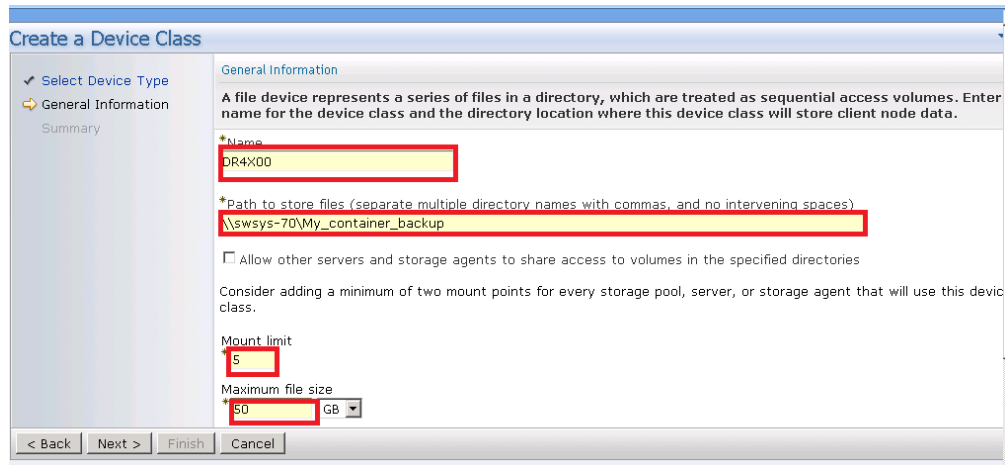
- Select the **FILE** device type, and click **Next**. (This device type is optimized for writing to disk-based storage.)



- Under General Information, enter the following 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 system export for NFS.
  - Mount Limit** – Set the mount 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 file size. The DR Series system supports very large files, such as 1TB.

**Note:** The service account for TSM needs to have the correct permission to connect 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.

An example for the CIFS Container Path follows.



An example for the NFS container path follows.

The screenshot shows the 'Create a Device Class' wizard in the 'General Information' step. The left sidebar has 'Select Device Type' checked and 'General Information' selected. The main area contains the following fields and options:

- Name:** TSM-iscsi
- Path to store files:** //mnt/TSM-iscsi
- Allow other servers and storage agents to share access to volumes in the specified directories
- Mount limit:** 20
- Maximum file size:** 2 GB

At the bottom, the 'Next >' button is highlighted with a red box.

6. Click **Finish**.

The screenshot shows the 'Create a Device Class' wizard in the 'Summary' step. The left sidebar has 'Select Device Type' and 'General Information' checked, and 'Summary' selected. The main area displays a success message:

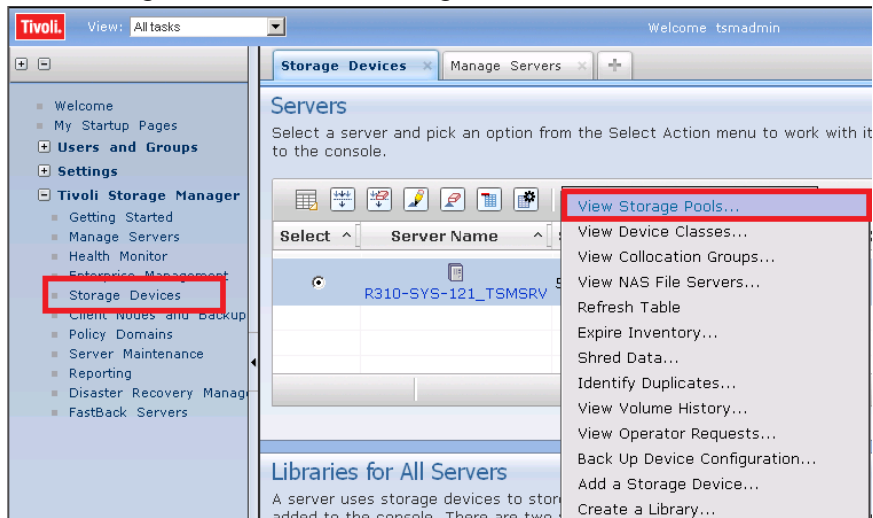
These storage objects have been successfully defined.

Device class DR4X00-Device has been created.

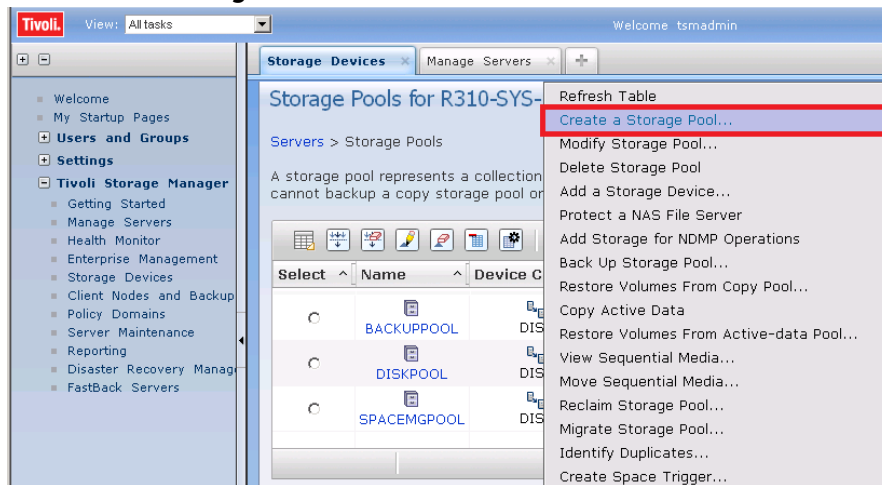
At the bottom, the 'Finish' button is highlighted with a red box.

## 2.2 Configuring the storage pool for CIFS & NFS protocols

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

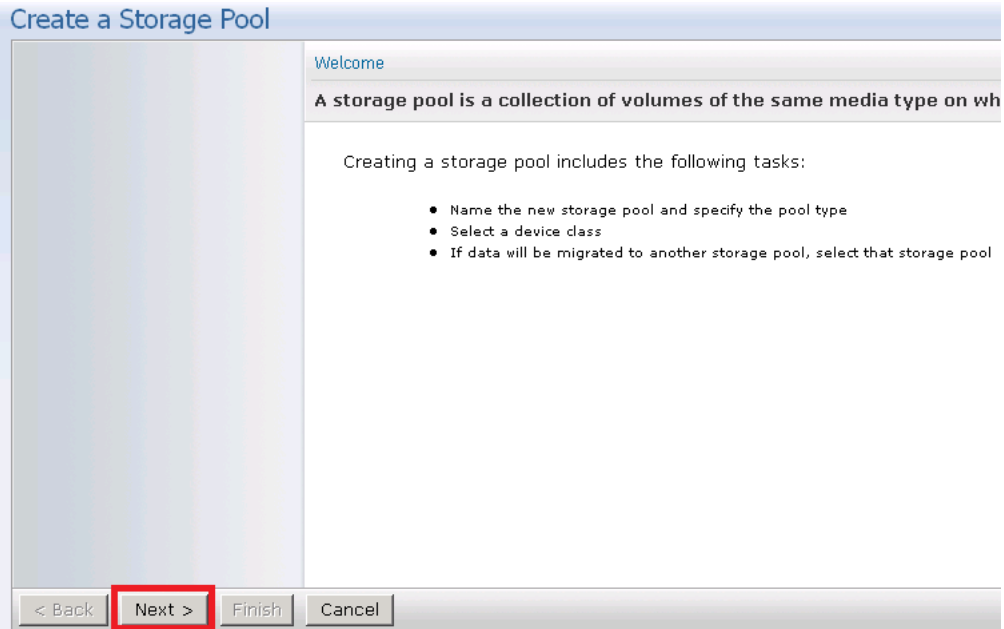


2. Click **Create Storage Pools**.

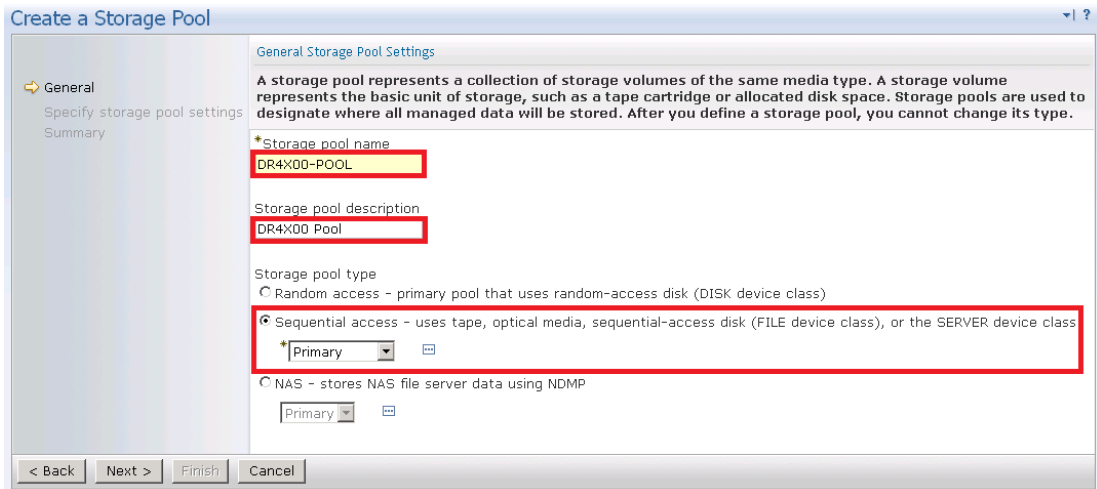




3. Click **Next**.



4. Enter the following 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.



5. 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.)

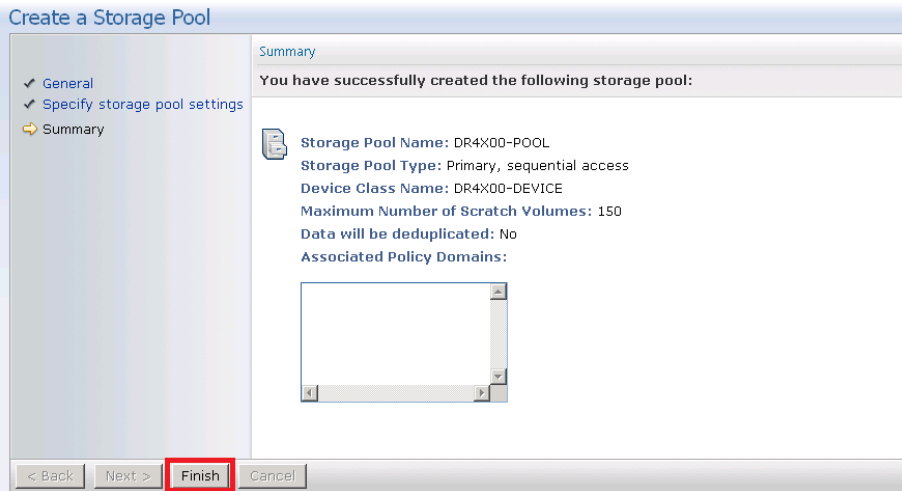
The screenshot shows the 'Create a Storage Pool' wizard window. The left sidebar has 'General' selected. The main area is titled 'Select a Device Class' and contains the following text: 'A device class represents a set of similar storage devices. A device class is used to associate storage pool volumes with a compatible storage device.' Below this, there are two fields: '\*Device class name' with a dropdown menu showing 'DR4X00-DEVICE' (highlighted with a red box), and '\*Maximum number of scratch volumes' with a text input field containing '150' (highlighted with a red box). At the bottom, there is a 'Next storage pool' dropdown menu set to '-- None --'. Navigation buttons '< Back', 'Next >', 'Finish', and 'Cancel' are at the bottom.

6. For Identifying Duplicates, accept the defaults selections, and click **Next**. (Ensure that the **Identify the duplicate data in the storage pool** check box is not selected as the DR Series system uses inline deduplication and already identifies and removes duplicate data.)

The screenshot shows the 'Create a Storage Pool' wizard window, now on the 'Identify Duplicates' step. The left sidebar has 'General' selected. The main area is titled 'Identify Duplicates' and contains the following text: 'The server can identify duplicate data within a FILE storage pool. This data is then removed during reclamation processing. Eliminating duplicate data increases the amount of available disk space. However, identifying duplicate data increases the server workload, and data that has been deduplicated can take longer to restore.' Below this, there is a checkbox labeled 'Identify the duplicate data in this storage pool.' which is unchecked (highlighted with a red box). Underneath, there is a text input field for the number of processes, containing the value '1'. Navigation buttons '< Back', 'Next >', 'Finish', and 'Cancel' are at the bottom.

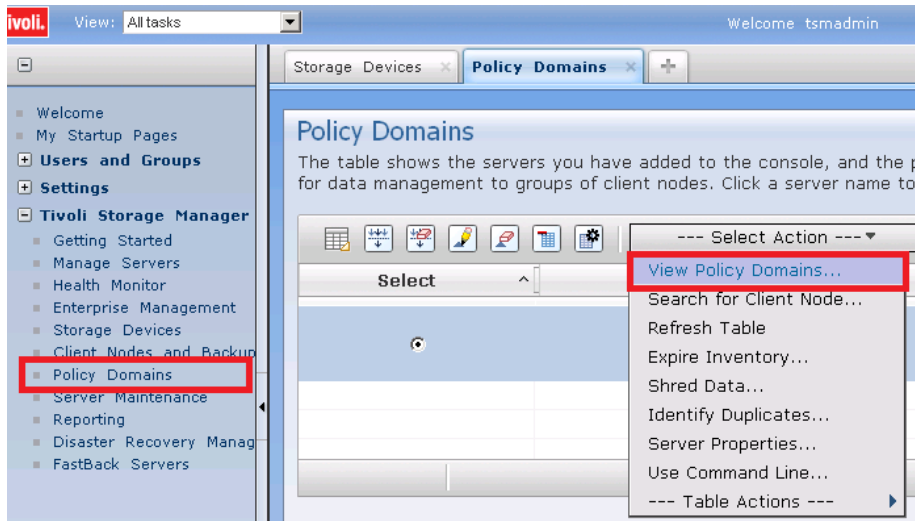


7. Review the settings and click **Finish**.

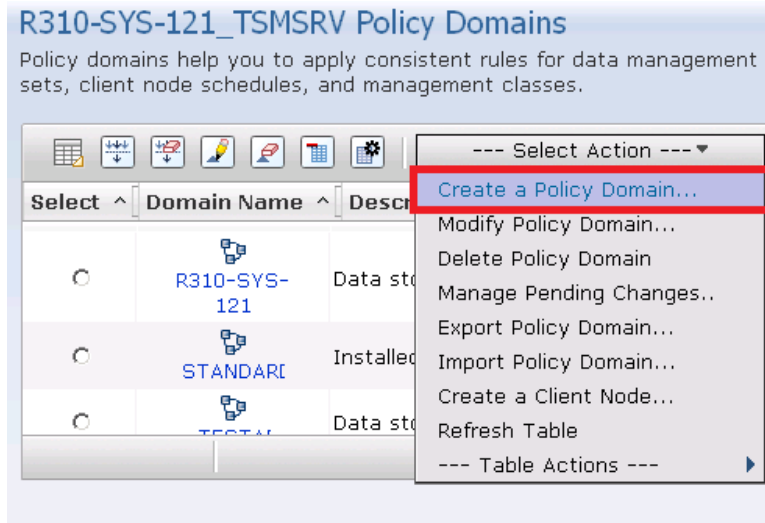


## 2.3 Creating a policy domain for the backup job

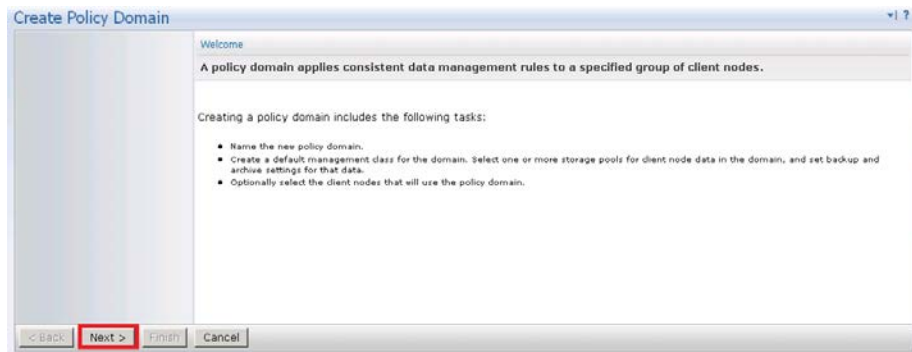
1. Click **Policy Domains > View Policy Domains**.



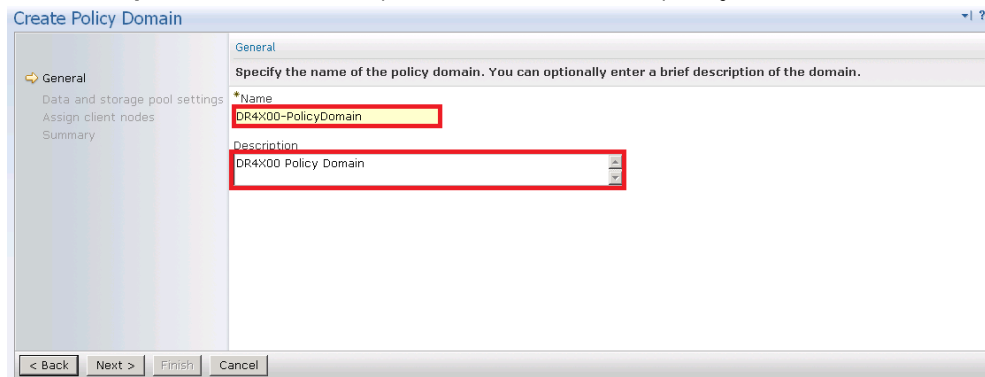
2. Click **Create a Policy Domain**.



3. Click **Next**.



4. Enter the following 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.



5. 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.

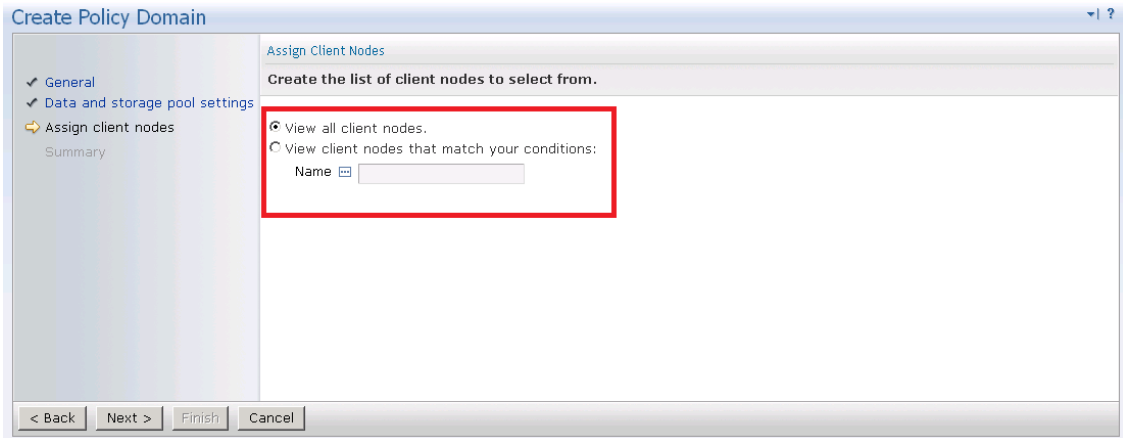
**Note:** File versions and inactive versions are set based on company policies.

The screenshot shows the 'Create Policy Domain' wizard with the 'Data and storage pool settings' step selected. The left sidebar shows 'General', 'Data and storage pool settings', 'Assign client nodes', and 'Summary'. The main content area has a title 'Data and storage pool settings' and a description: 'The default management class is used for all client node data that are not bound to a different management class. Select the default management class storage pools, specify backup and archive settings, and specify if active-data pools can be used.' Below this is a note: 'Select a storage pool for at least one of these data types. If you do not select storage pools for both data types, backup or archive operations can fail.' There are two sections: 'Specify default management class settings for backup data:' and 'Specify default management class settings for archive data:'. The backup data section is checked and contains a dropdown menu for 'Storage pool for backup data' with 'DR4X00-POOL' selected, a text input for 'Number of file versions to keep' with the value '2', and a text input for 'Number of days to keep inactive versions' with the value '30'. The archive data section is unchecked and contains a dropdown menu for 'Storage pool for archive data' with 'DR4X00-POOL' selected.

6. Select **Yes** to assign this policy domain to clients, and click **Next**.

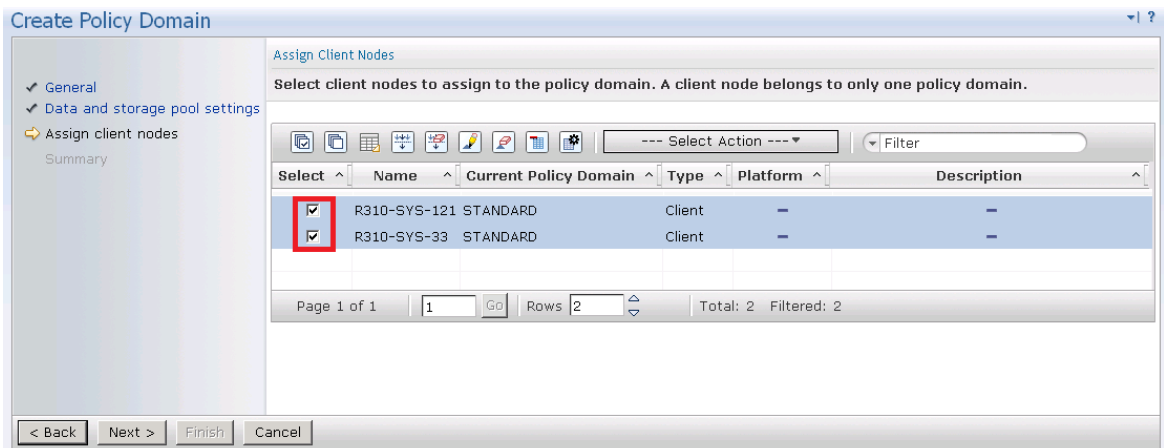
The screenshot shows the 'Create Policy Domain' wizard with the 'Assign Client Nodes Now?' step selected. The left sidebar shows 'General', 'Data and storage pool settings', 'Assign client nodes', and 'Summary'. The main content area has a title 'Assign Client Nodes Now?' and a description: 'The server manages the data and operations for a client node by using the rules of the policy domain. You can select the client nodes to assign to the new policy domain now or at another time. A client node can be assigned to only one policy domain.' Below this is a question: 'Do you want to assign client nodes to this policy domain now?' with two radio button options: 'Yes' (selected) and 'No'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

7. Select **View all client nodes** to display the set of clients to move to the DR Series system, and click **Next**.

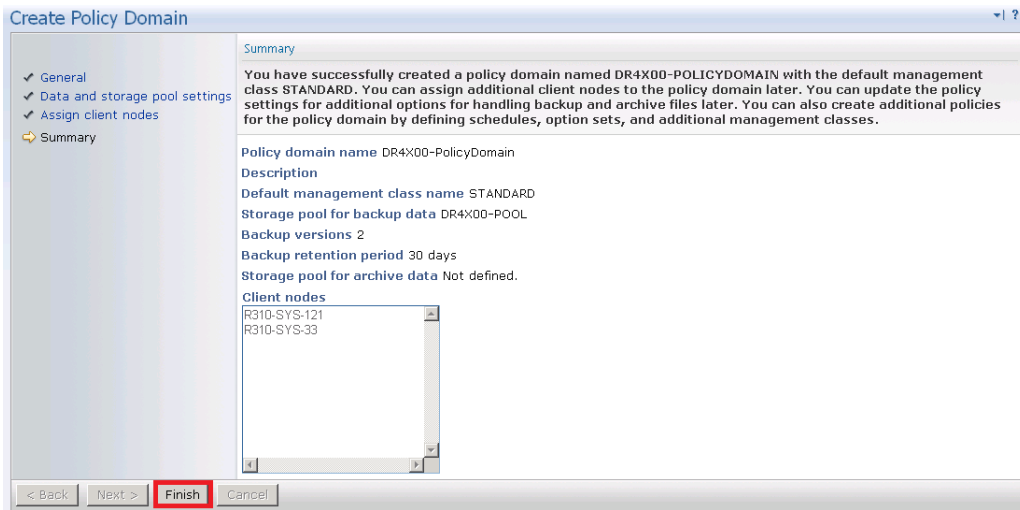


**Note:** You can choose to limit if you have a lot of client computers.

8. Select the check boxes next to the clients you want to back up to the DR Series system, and click **Next**.

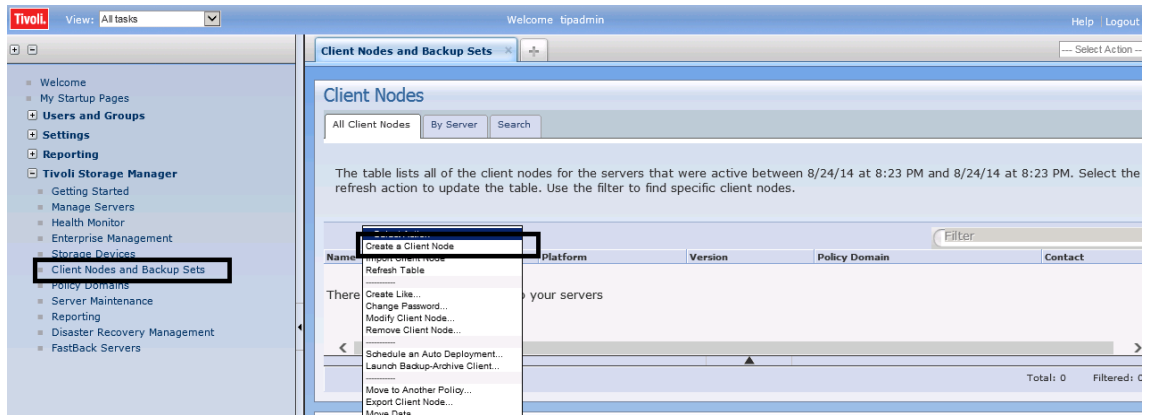


9. Click **Finish**.



## 2.4 Creating client node and backup sets

1. Open the client sets and backup sets from TSM to register the client machine.



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



3. Confirm that the client node is successfully registered.



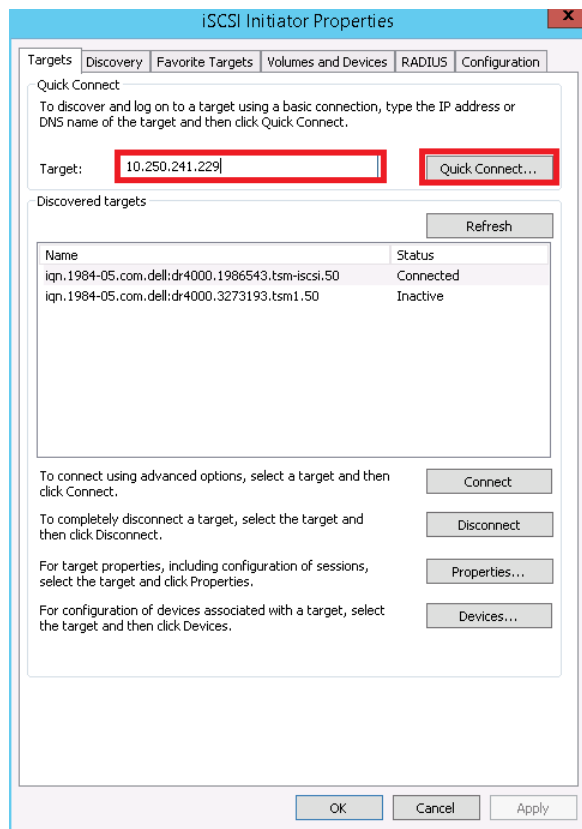


## 3 Creating and configuring iSCSI target container(s) for TSM

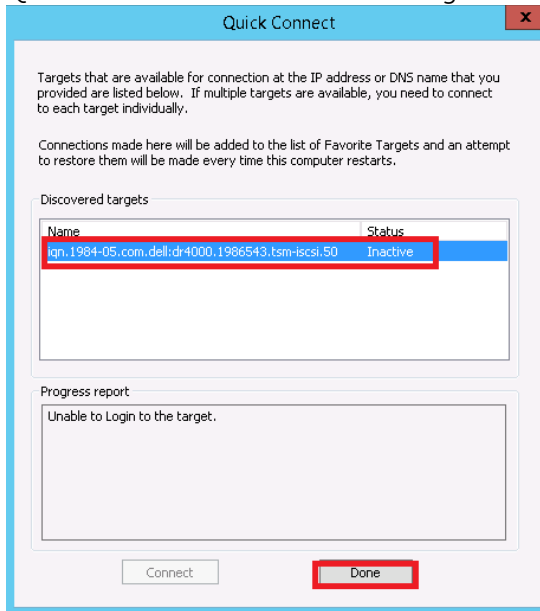
### 3.1 Configuring the iSCSI initiator

#### 3.1.1 Configuring iSCSI initiator for Windows

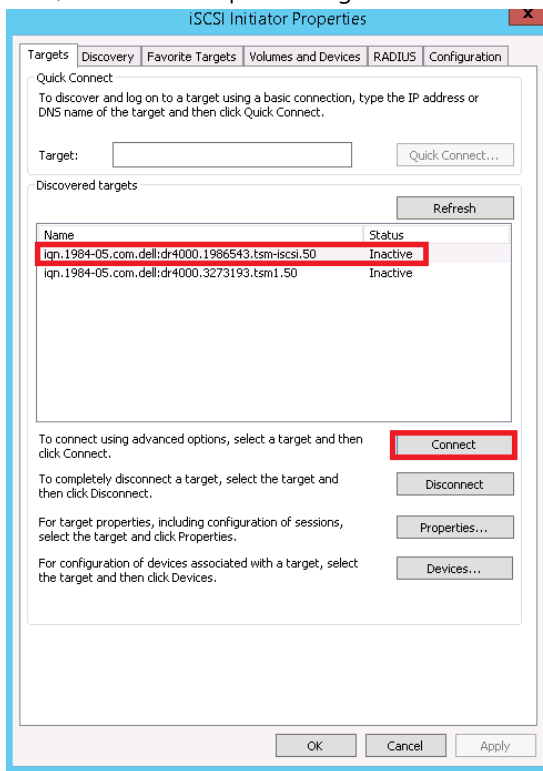
1. In the Windows TSM Server, open iSCSI initiator software, and then enter the DR IP/Hostname as target. Click **Quick Connect**.



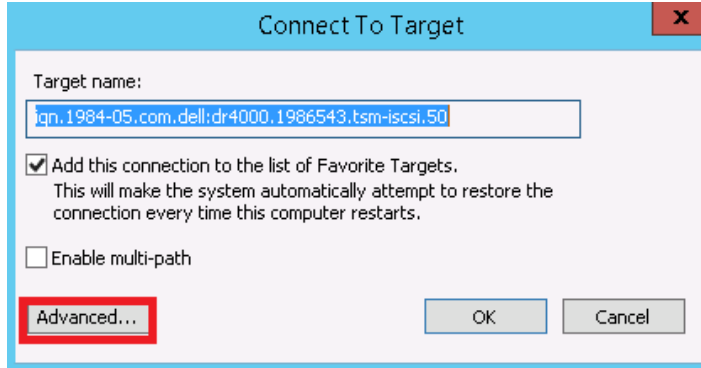
Quick connect will discover the targets.



2. Click **Done**.
3. Then, select the required targets and click **Connect**.

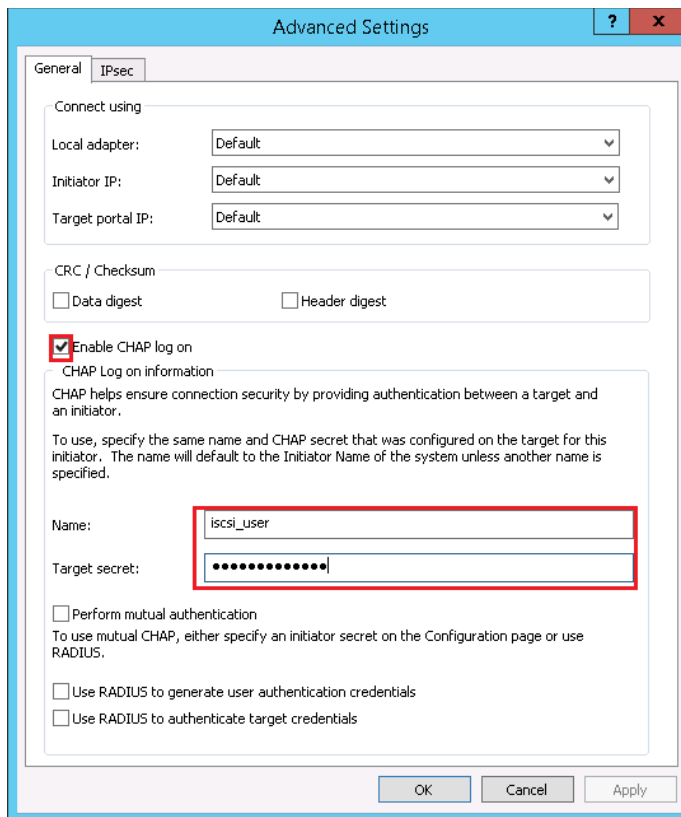


4. Click **Advanced**.

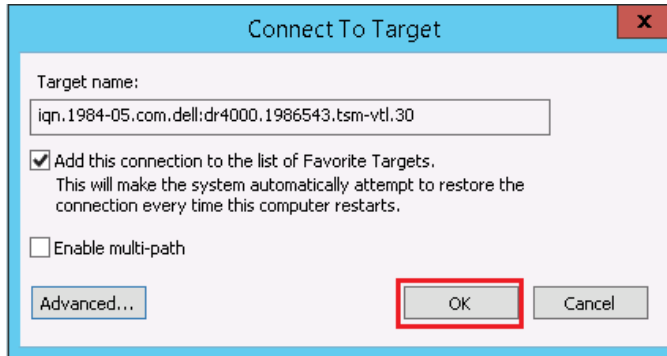


5. Select the option, **Enable CHAP log on**, enter the following credentials, and click **OK**:
  - Name: iscsi\_user
  - Password: St0r@geliscsi

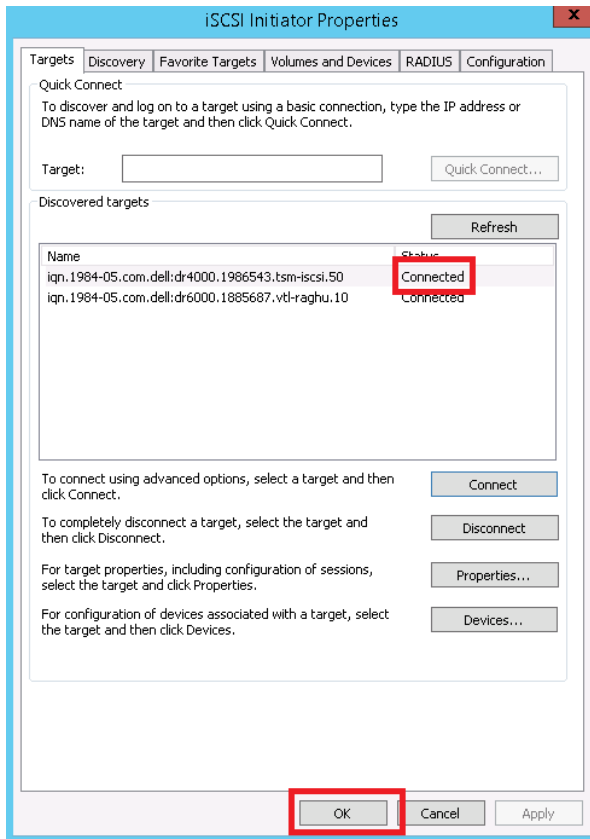
**Note:** The iSCSI user name can be found by entering the following command on the DR Series system:  
**# iscsi --show --user**



6. Click **OK**.



7. Verify that the Status shows as "Connected," and click **OK**.



### 3.1.2 Configuring the iSCSI initiator – Linux

Before you begin this procedure, ensure that the iSCSI initiator is installed (iscsi-initiator-utils). For example, enter the following command:

```
yum install iscsi-initiator-utils ; /etc/init.d/iscsi start
```

To configure the iSCSI target for Linux, follow these steps.

1. Add the CHAP Authentication details for the DR Series system on the Linux Initiator as follows:
  - a. Edit /etc/iscsi/iscsid.conf and un-comment the following line:

```
node.session.auth.authmethod = CHAP
```

- b. Modify the following lines:

```
# To set a CHAP username and password for initiator
```

```
# authentication by the target(s), uncomment the following lines:
```

```
node.session.auth.username = iscsi_user
```

```
node.session.auth.password = St0r@ge!iscsi
```

2. Set the Discovery Target Node(s) by using this command:

```
iscsiadm -m discovery -t st -p <IP or IQN of DR>
```

For example:

```
iscsiadm -m discovery -t st -p 10.8.230.108
```

3. Enable logon to the DR Series system iSCSI VTL target(s) by using the following command:

```
iscsiadm -m node --portal <IP or IQN of DR:PORT> --login
```

For example:

```
iscsiadm -m node --portal "10.8.230.108:3260" --login
```

4. Display the open session(s) with DR VTL(s) by using the following command:

```
iscsiadm -m session
```

For example:

```
iscsiadm -m session = tcp: [8] 10.8.230.108:3260,1 iqn.1984-05.com.dell:dr4000.3071067.interoprhel52n1.30
```

5. Review dmesg or /var/log/messages for details about the tape devices created upon adding the DR Series system iSCSI VTL.

6. Run the "cat /proc/scsi/scsi" command to see the LUN and HOST details



## 3.2 Configuring DR Series system VTL for Windows and Linux TSM servers

**Note:** Refer to the following instructions for viewing the tape devices and IDs, which you will need to configure the DR Series system VTL.

**For Windows:** To see the Tape Library device IDs, use the command “tsmdlst.” For example:

```
cd C:\program files\Tivoli\TSM\Server\Tsmdiag
.\tsmdlst.exe
```

**For Linux:** For discovering the tape devices and their IDs, refer to Appendix C later in this document.

### 3.2.1 Configuring the DR Series system VTL for Windows

#### 3.2.1.1 Define library

```
# define library TSM-iscsi libtype=scsi shared=yes autolabel=yes
```

(TSM-iscsi is user defined name for the library)

#### 3.2.1.2 Define library path

```
# define path WIN-8B1A4SA50SR TSM-iscsi srct=server autodetect=yes destt=library
device=lb0.1.0.3
```

Where:

- WIN-8B1A4SA50SR = TSM server hostname
- Device = Device ID for medium changer listed by “tsmdlst” command.

#### 3.2.1.3 Define drive

```
# define drive TSM-iscsi drive01 online=yes
```

Where:

- TSM-iscsi = Library name defined in earlier command
- Drive01 = User defined drive name

#### 3.2.1.4 Define drive path

```
# define path WIN-8B1A4SA50SR drive01 srct=server destt=drive library=TSM-iscsi
device=mt0.2.0.3 online=yes
```

#### 3.2.1.5 Audit the library

```
# audit library TSM-iscsi checklabel=barcode
```



### 3.2.1.6 Check in the library volumes

```
# checkin libvolume TSM-iscsi search=yes checklabel=barcode status=scratch
```

## 3.2.2 Configuring the DR Series system VTL for Linux

### 3.2.2.1 Define library

```
# define library TSM-iscsi libtype=scsi shared=yes autolabel=yes
```

### 3.2.2.2 Define library path

```
# define path RHEL-TSM-SERVER TSM-iscsi srct=server autodetect=yes destt=library  
device=/dev/tsm SCSI/lb0
```

### 3.2.2.3 Define drive

```
# define drive TSM-iscsi drive01 online=yes (define all drives 0-9, drive01 is  
defined by user)
```

### 3.2.2.4 Define drive path

```
# define path RHEL-TSM-SERVER drive01 srct=server destt=drive library=TSM-iscsi  
device=/dev/IBMtape0 online=yes
```

### 3.2.2.5 Audit the library

```
# Audit library TSM-iscsi checklabel=barcode
```

### 3.2.2.6 Checkin the library volumes

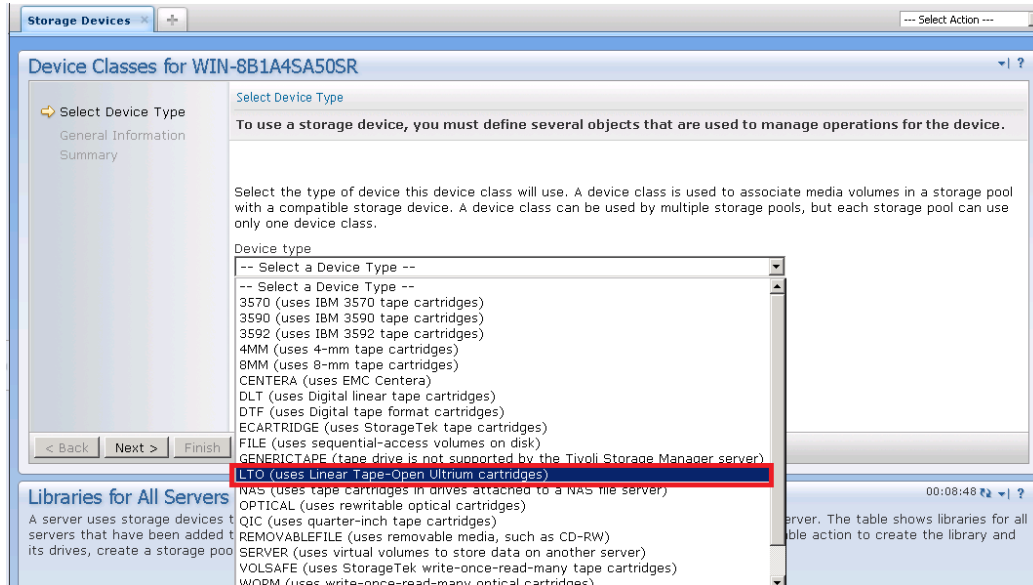
```
# checkin libvolume TSM-iscsi search=yes checklabel=barcode status=scratch
```



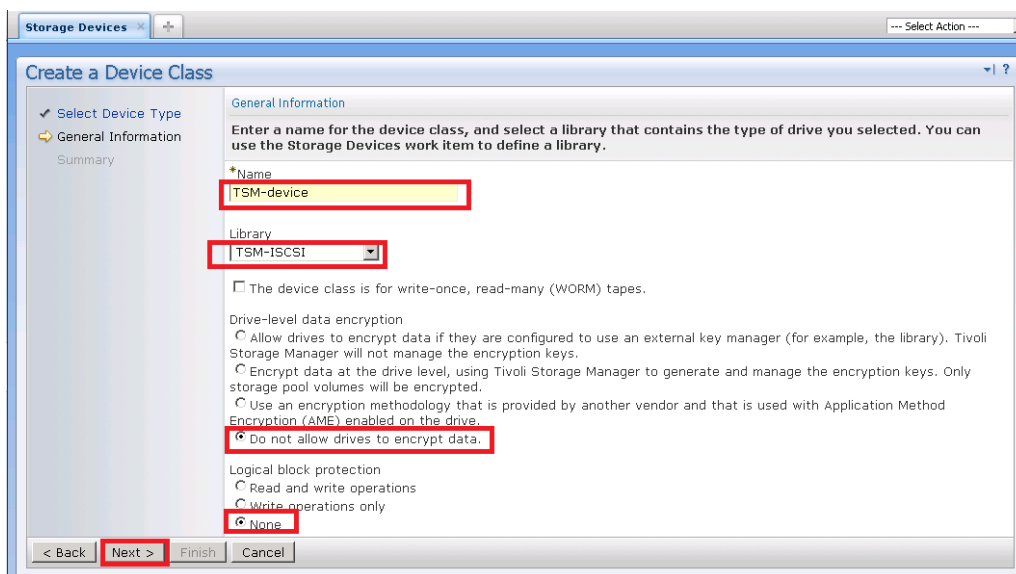
### 3.3 Configuring the device class for iSCSI VTL

Follow Steps 1, 2, and 3 earlier in the Device Class creation section 2.1.

1. Select the Device Type as LTO for iSCSI VTL.

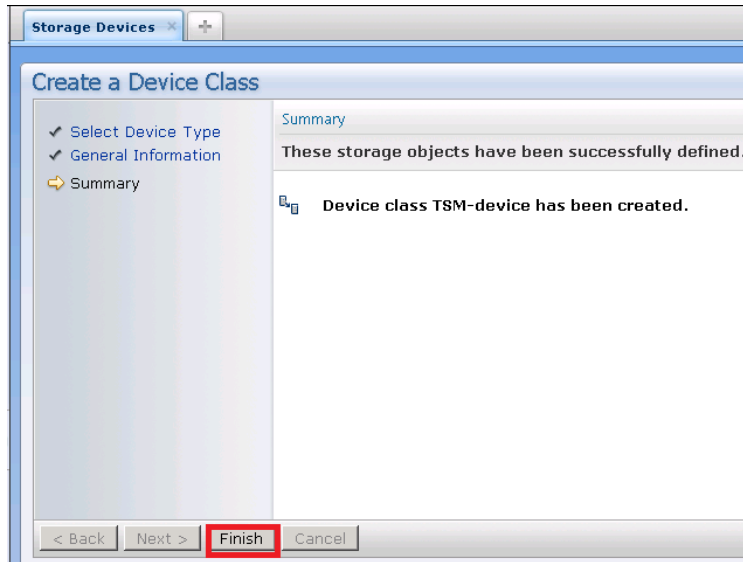


2. Under General Information, provide the name and select the library configured. Under Drive-level data encryption, select the **Do not allow drives to encrypt data** option, and under Logical block protection, click **None**.



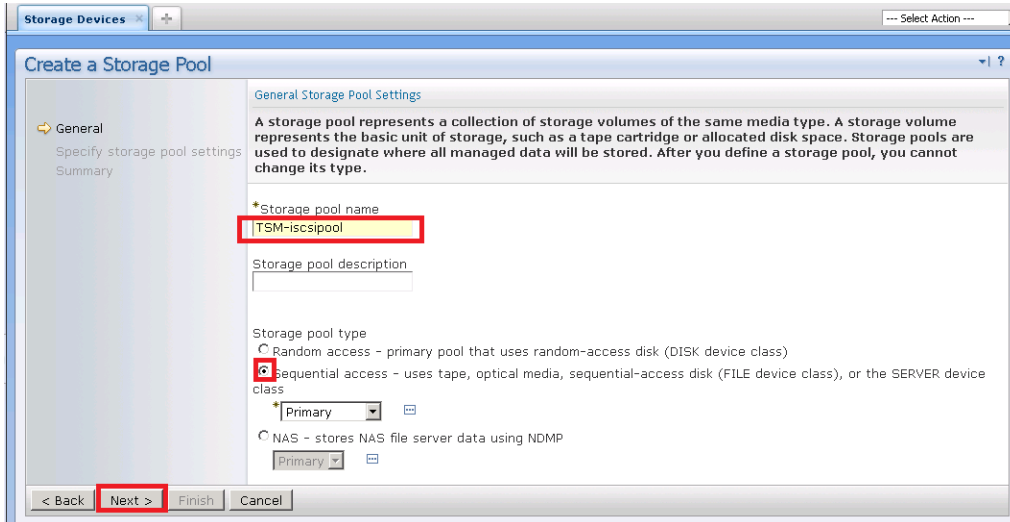


3. Click **Next** and then click **Finish**.

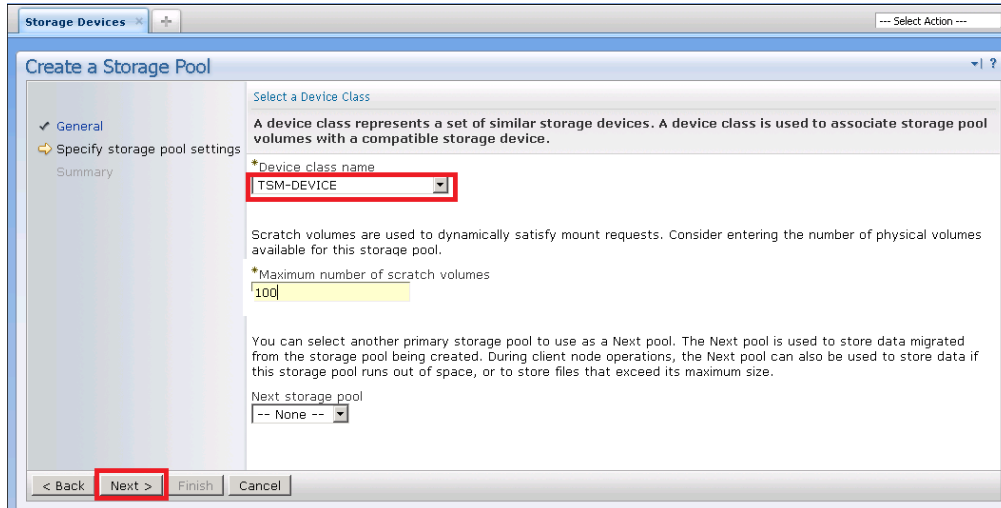


## 3.4 Configuring the storage pool for iSCSI VTL

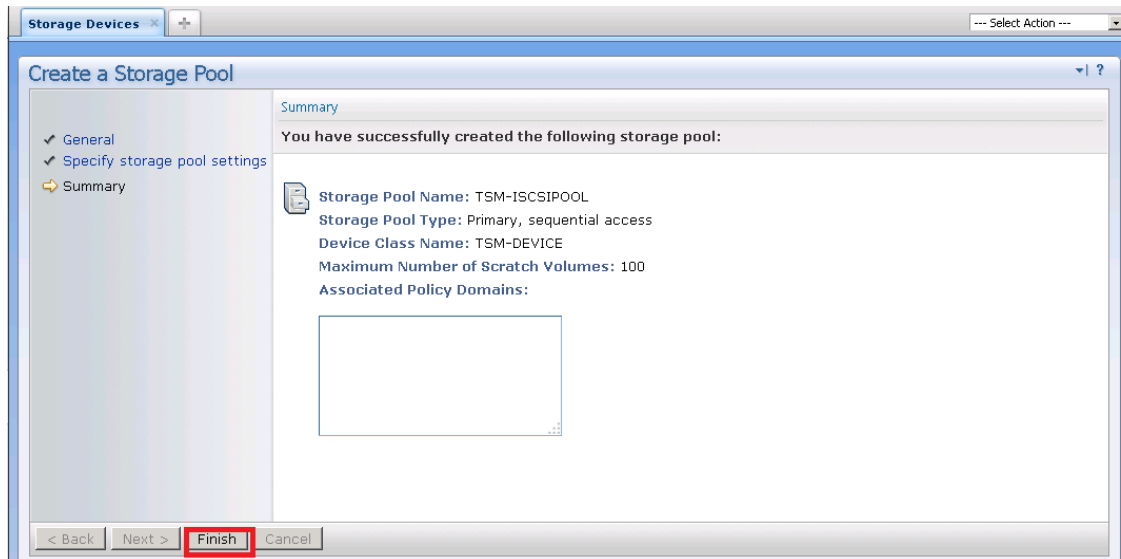
1. Follow Steps 8,9 and 10 from the previous Storage Pool creation section 2.2
2. Under General storage pool settings, provide the pool name and type, and then click **Next**.



4. Provide the necessary Device name and maximum number of Scratch volumes and click **Next**.

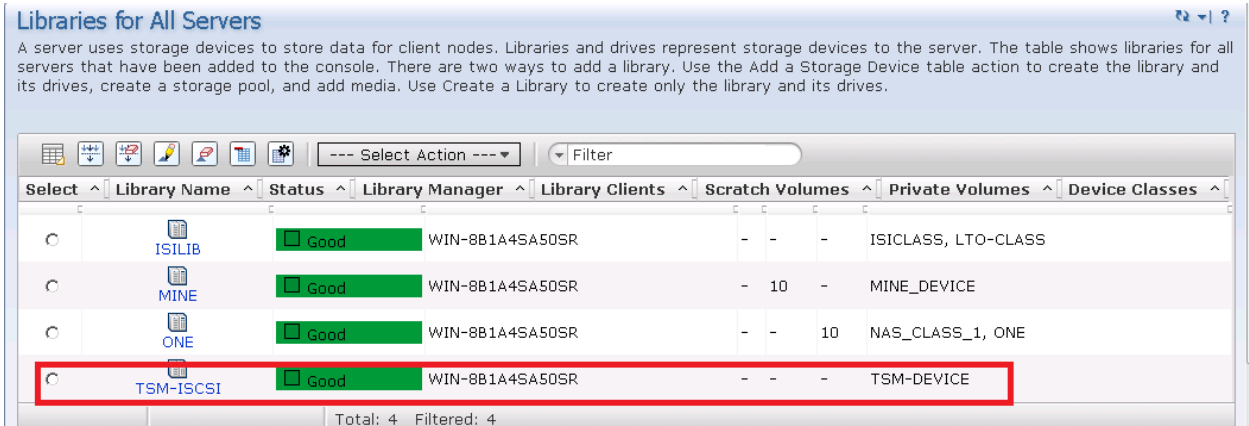


5. Click **Finish**.

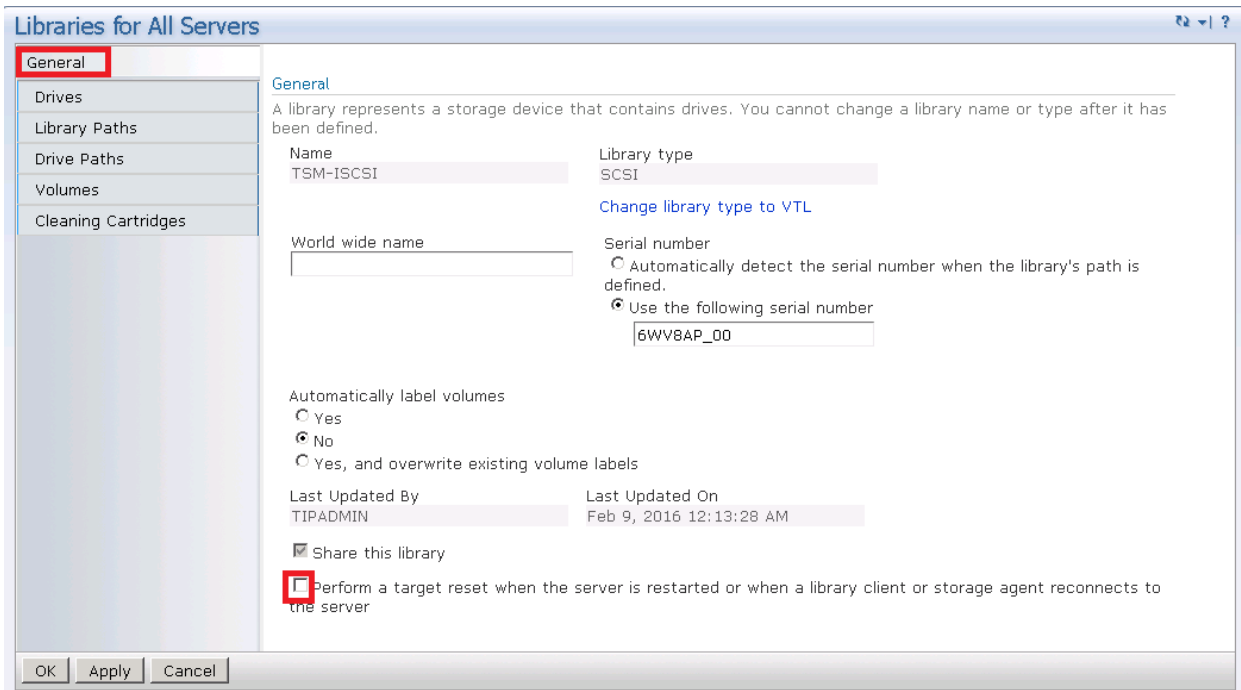


### 3.4.1 Adding volumes to a library

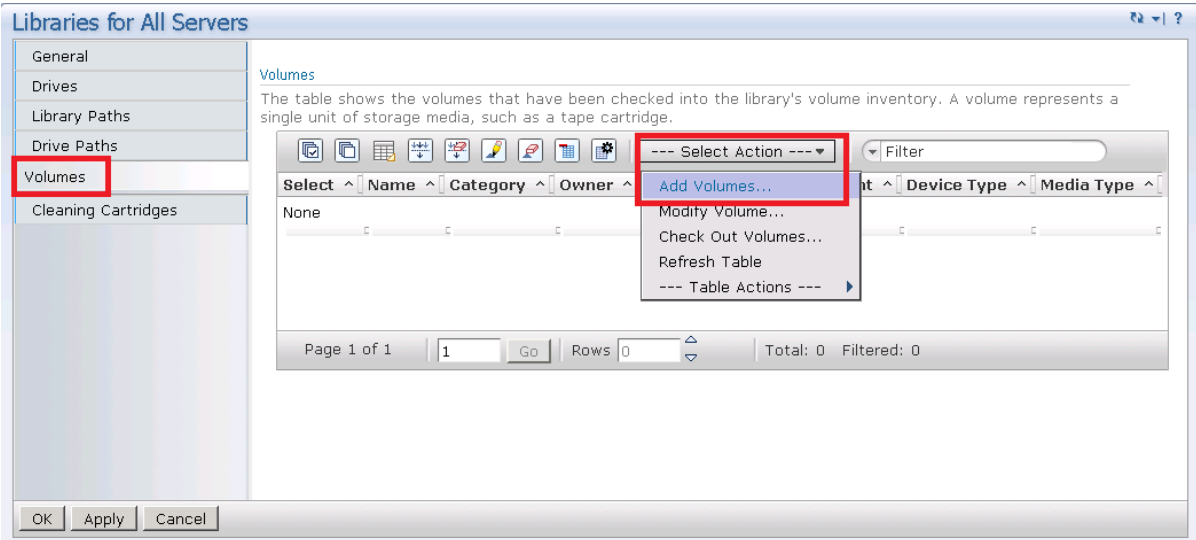
1. After creating a storage pool, click Storage Devices in the Left Pane, and then select the library that was configured earlier.



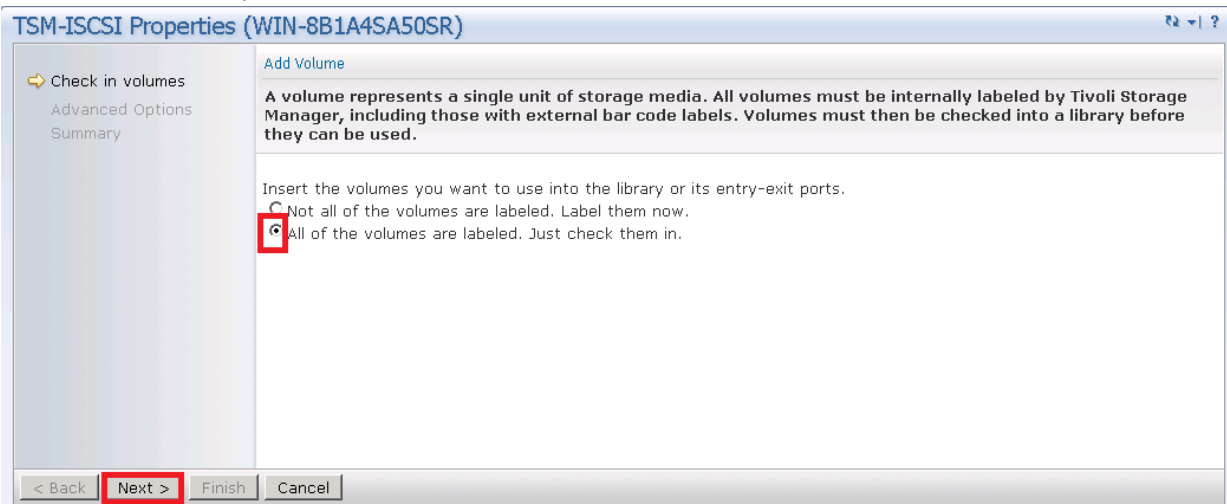
2. Select the column (which was default earlier) and disable the target reset option when the server is restarted.



3. In the Volumes section, click **Add Volumes**.



4. Select the option, **All of the volumes are labeled. Just check them in**. Click **Next**.



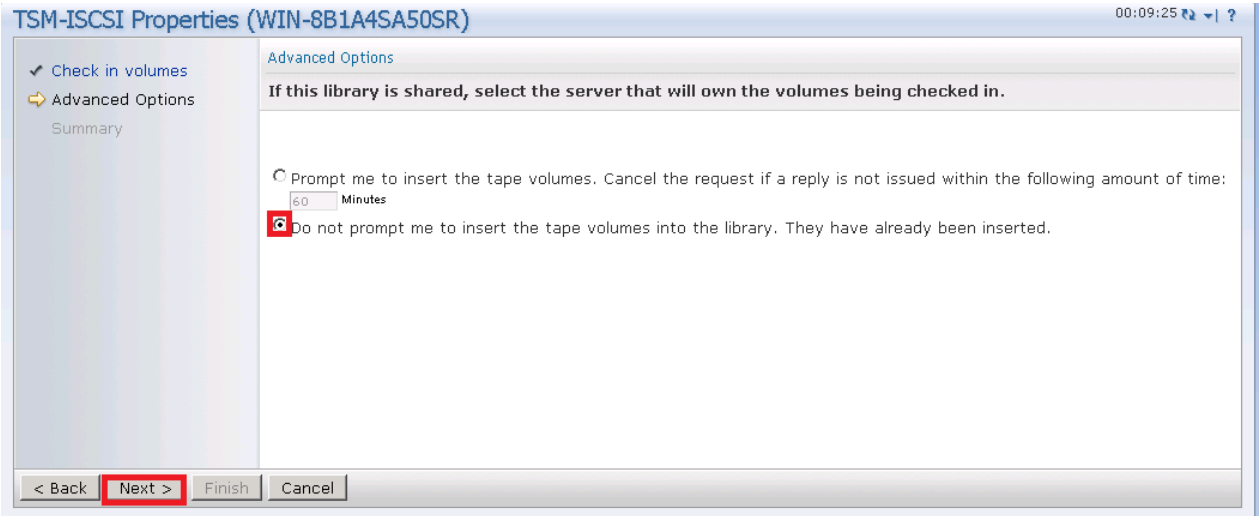
6. Select the option, **Search for all eligible volumes in the library's regular slots**. Click **Next**.

The screenshot shows the 'Volume Search Options' dialog box within the 'TSM-SCSI Properties (WIN-8B1A4SA50SR)' window. The left sidebar contains 'Check in volumes', 'Advanced Options', and 'Summary'. The main area has a title bar 'Volume Search Options' and a description: 'Select whether to search for volumes that are not currently checked in. For a single volume, the server will issue a mount request. Use the View Operator Requests table action in the Libraries table to reply to the mount request.' Below this are three radio button options: 'Search for all eligible volumes in the library's entry-exit ports', 'Search for all eligible volumes in the library's regular slots' (which is selected and highlighted with a red box), and 'Request only this volume'. A 'Volume name' text box is present below the options. At the bottom, there are four buttons: '< Back', 'Next >' (highlighted with a red box), 'Finish', and 'Cancel'.

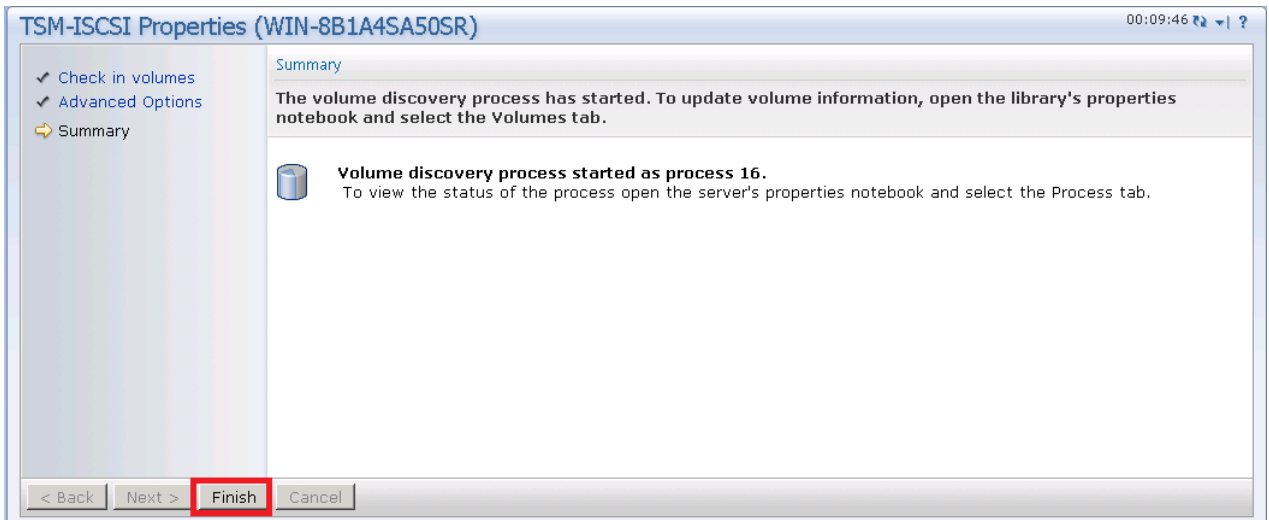
7. On the Check in Volumes page, do the following:
- Select the option, **Read bar codes and check in all eligible volumes**.
  - Select **Scratch** as the pool to check in volumes to the scratch pool.
  - Click **Next**.

The screenshot shows the 'Check In Volumes' dialog box within the 'TSM-SCSI Properties (WIN-8B1A4SA50SR)' window. The left sidebar contains 'Check in volumes', 'Advanced Options', and 'Summary'. The main area has a title bar 'Check In Volumes' and a description: 'The server will search the library to discover volumes that are not currently checked in. Volumes currently defined to the server cannot be checked in as scratch volumes. The check-in process will fail if a drive is not available.' Below this is a section 'Use the following procedure to discover eligible volumes' with three radio button options: 'Read bar codes and check in all eligible volumes.' (selected and highlighted with a red box), 'Read bar codes, but search only these volumes (separate volume names with commas)', and 'Read bar codes, but search only the volumes found in the following file'. There are text boxes for 'Starting volume name' and 'Ending volume name' under the third option. Below this is a radio button option: 'Mount volumes and read their labels (required for WORM tapes, except 3592). Check in all eligible volumes.' At the bottom, there is a section 'Give volumes the following status when checking them in' with two radio button options: 'Scratch - can be used to satisfy any request to mount a scratch volume' (selected and highlighted with a red box) and 'Private - can only be used to satisfy a request to mount the volume by name'. At the bottom of the dialog, there are four buttons: '< Back', 'Next >' (highlighted with a red box), 'Finish', and 'Cancel'.

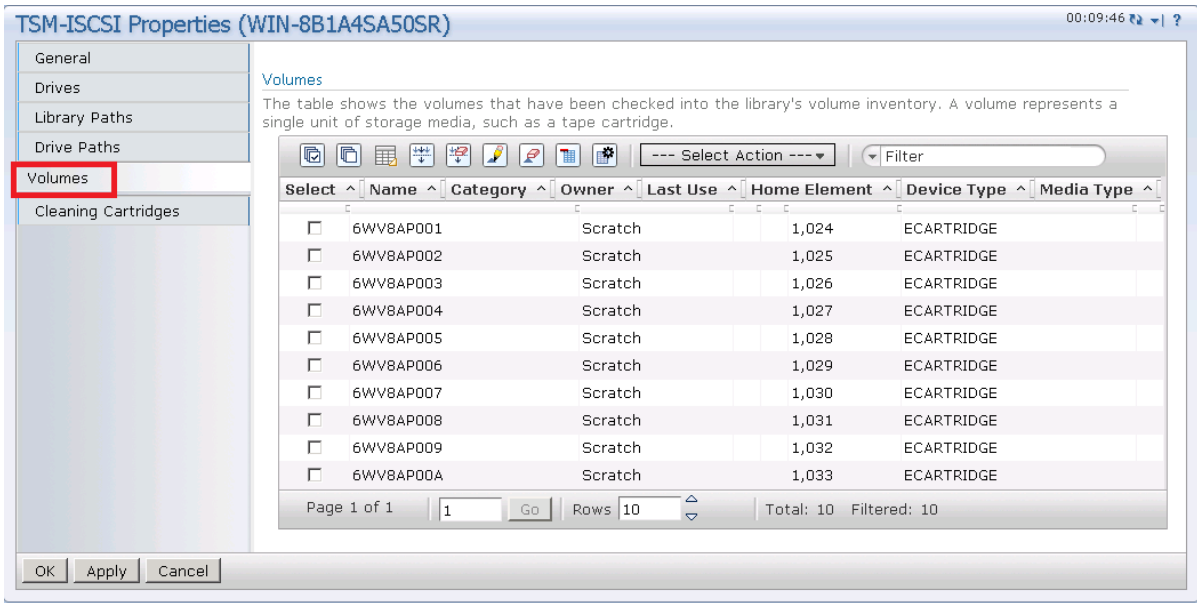
- For Advanced Options, select the option, **Do not prompt me to insert the tape volumes into the library**. Click **Next**.



- Click **Finish**.

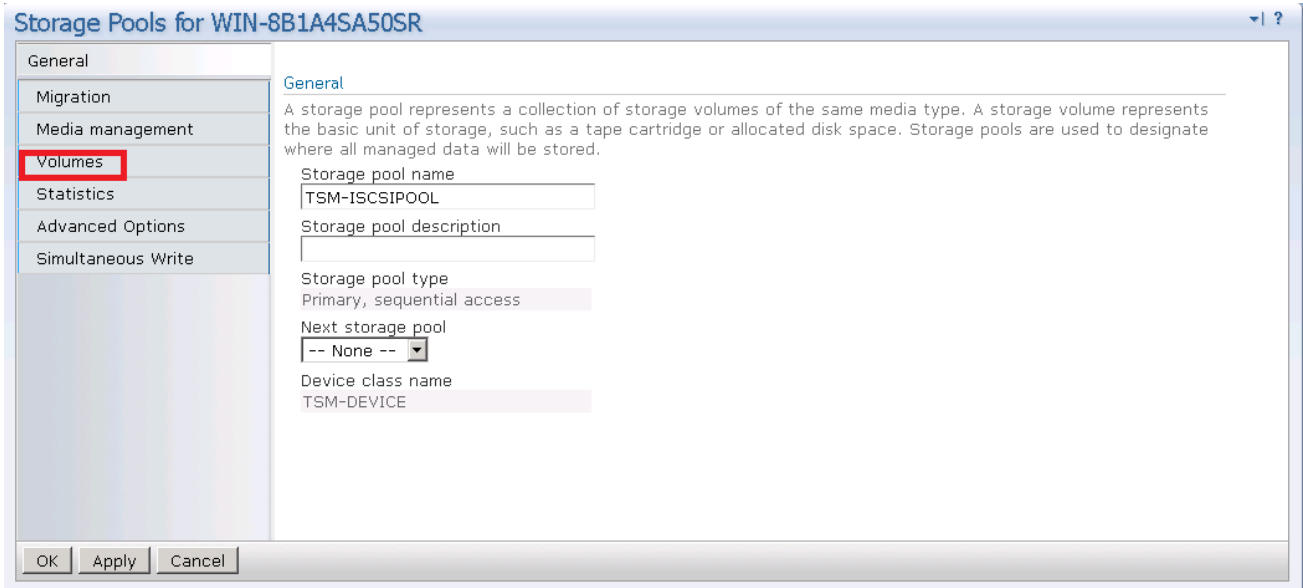


10. Check that all the volumes are created.

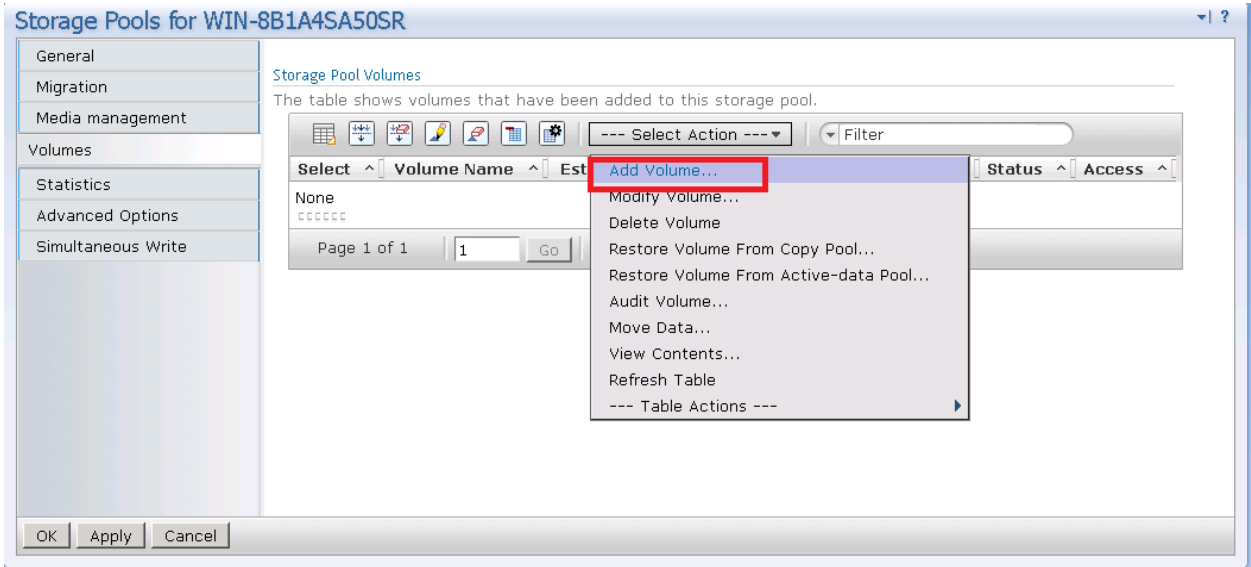


### 3.4.2 Adding volumes to a storage pool

1. Go to the Storage Pool section (which was created earlier for the iSCSI target), and click Volumes.

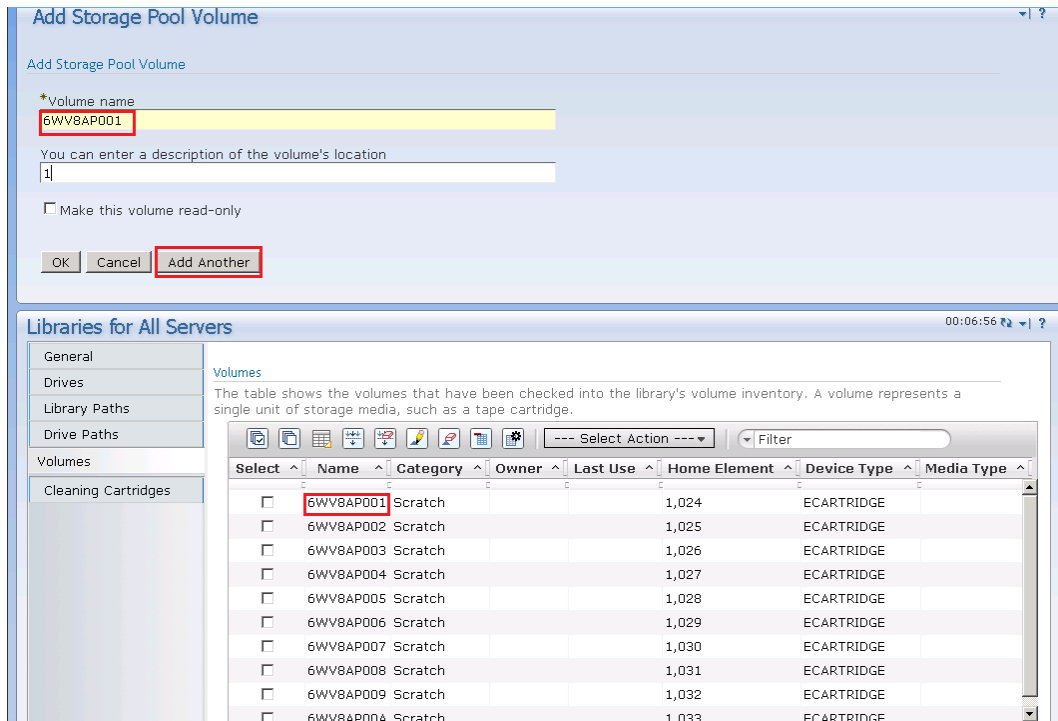


2. In the Volumes section, click **Add Volumes**.



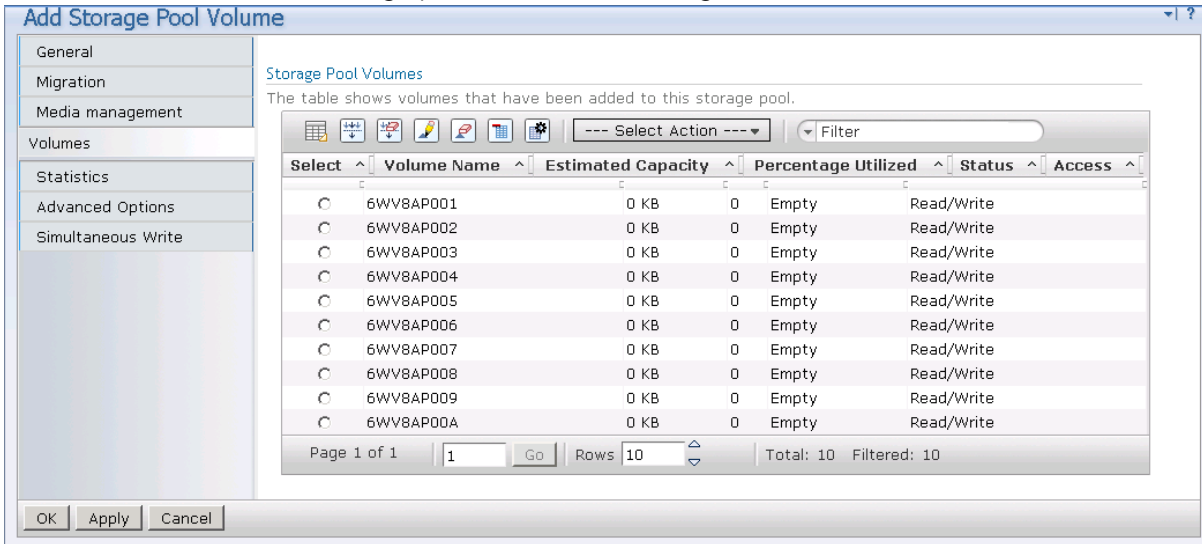
3. Provide the details of the volumes one by one in the volumes name column.

**Note:** Provide exactly the same volume name as present in the LIBRARY for volume name for the storage pool.





4. Check that all the storage pool volumes are configured



### 3.5 Creating the policy domain for iSCSI VTL

Follow the steps described in the earlier section related to Policy Domain creation, Section 2.3.

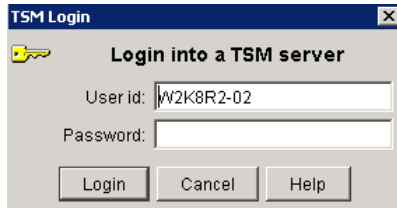
### 3.6 Creating the client node for iSCSI VTL

Follow the steps described earlier in the section for creating a client node, Section 2.4.



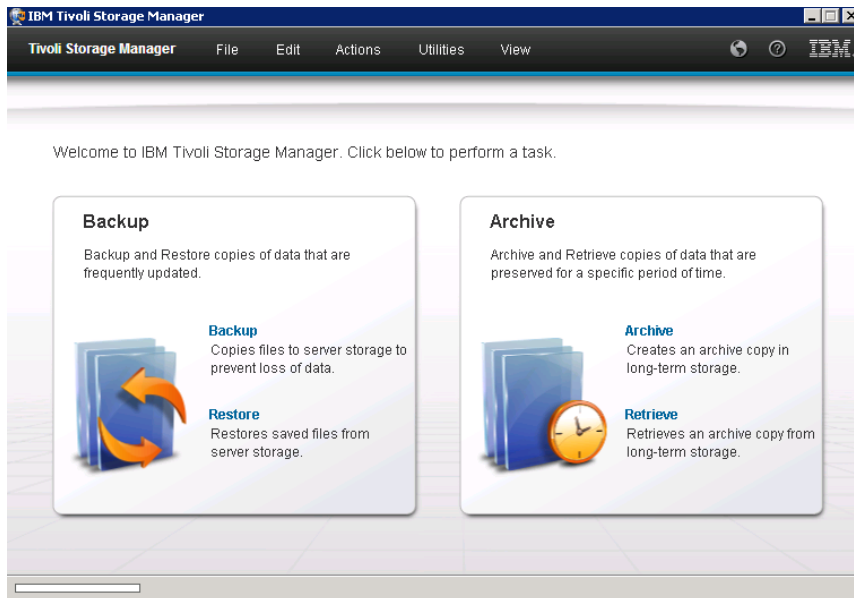
## 4 Using the Backup & Archive GUI

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.

The Backup and Restore Manager is ready to perform.



When you have successfully completed the steps above, you have configured the DR Series system for TSM. 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.

## 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 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.

The screenshot shows the Dell DR Series system cleaner configuration interface. The sidebar menu on the left includes sections for Dashboard, Storage, Schedules, System Configuration, and Support. The 'Cleaner Schedule' option is highlighted in the Schedules section. The main content area displays the 'Cleaner Schedule' configuration page. The page title is 'Cleaner Schedule'. The system time zone is US/Pacific, Fri Jul 5 05:00:41 2013. A note states: 'Note: When no schedule is set, the cleaner will run as needed.' Below the note is a table with columns for Day, Start Time, and Stop Time. The table shows the following data:

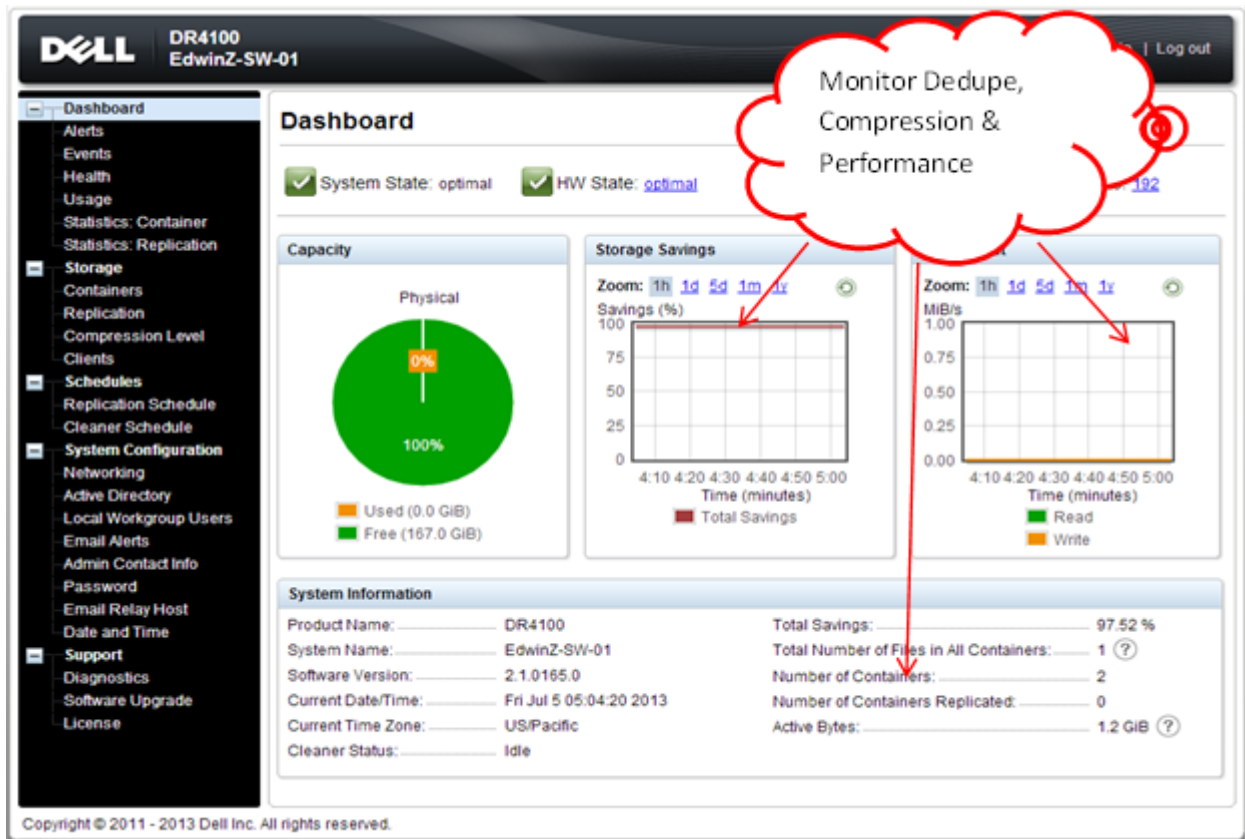
Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--

At the top right of the main content area, there is a red arrow pointing to the 'Schedule Cleaner' button and a red box around the 'Edit Schedule' button. The footer of the page reads: Copyright © 2011 - 2013 Dell Inc. All rights reserved.

## 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 Configuring CIFS authentication

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

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

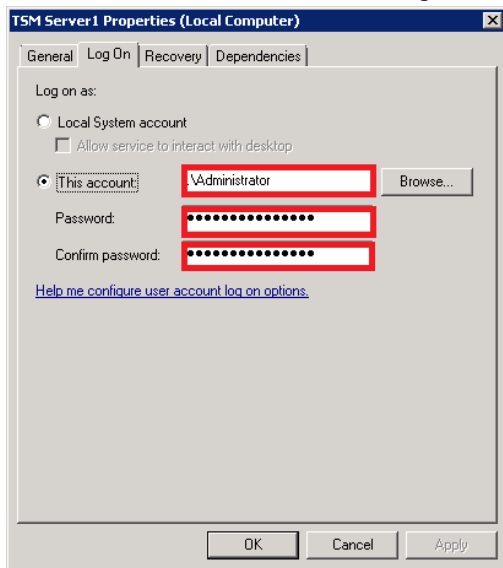
- Integrate the Tivoli Storage Manager Media Server and DR Series system with Active Directory (AD).
  - Ensure the AD user has appropriate ACLs to the DR4X00 Container.
  - Set the TSM Server service to run with <Domain\User>.
- Sync local usernames and passwords between the DR Series system and the TSM 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/StOr@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 TSM 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 TSM backup and space reclamations jobs should be scheduled to happen at different times.

## C Configuring the tape library devices on Linux

After installing the required device drivers for medium changer and drive, we need to configure tape Library with TSM Server. There is need to figure out the device IDs for respective devices so that Library can be defined in TSM.

In Windows server, there is a command utility "tsmdlst," which lists all the devices with their IDs.

The same can be done in Linux TSM server with "Autoconf" utility located at '/opt/tivoli/tsm/devices/bin'.

If "Autoconf" utility is not working, you need to define library manually in the TSM server as described below.

**Note:** Please see following link for more details –

[http://publib.boulder.ibm.com/tividd/td/ITSM/ITSM/GC23-4692-02/en\\_US/HTML/anrlqs52254.htm](http://publib.boulder.ibm.com/tividd/td/ITSM/ITSM/GC23-4692-02/en_US/HTML/anrlqs52254.htm)

To configure the TSM device drivers for selected tape drives and libraries, do the following:

1. Verify that the device is connected to your system, and is powered on and active.
2. Ensure that the TSM device driver package (TIVsm-tsm SCSI-x.x.x-x) is installed for your corresponding architecture.
3. Copy the two sample configuration files that are located in the installation directory from mt.conf.smp and lb.conf.smp to mt.conf and lb.conf, respectively:

For drives:

```
> cp /opt/tivoli/tsm/devices/bin/mt.conf.smp /opt/tivoli/tsm/devices/bin/mt.conf
```

For libraries:

```
> cp /opt/tivoli/tsm/devices/bin/lb.conf.smp /opt/tivoli/tsm/devices/bin/lb.conf
```

4. Edit the mt.conf and lb.conf. Add one stanza (as shown in the example at the top of the file) for each SCSI target ID and LUN combination for which you want the device driver to probe for supported tape drives, and for each autochanger device in the system that you want the server to use.
5. To load the device driver, run the tsm SCSI script from the device driver installation directory.

```
> cd /opt/tivoli/tsm/devices/bin ./tsm SCSI
```

Then all the devices will be listed in following locations:

TSM drives	/dev/tsm SCSI/mt#
IBM drives	/dev/IBMtape#
TSM Library	/dev/tsm SCSI/lb#





6. Change the permissions of the devices to avoid IO error during Library configuration –

```
chmod 777 /dev/tmscsi/*
```

```
chown tsminst1:tsmsrvrs /dev/tmscsi/*
```

```
chmod 777 /dev/IBM*
```

```
chown tsminst1:tsmsrvrs /dev/IBM*
```

**Note:** tsminst1 and tsmsrvrs are the user and group created for TSM installation.

