Quest™

Setting Up the DR Series System as a CIFS, NFS and iSCSI-VTL Target on Tivoli Storage Manager (TSM) v7.1

Technical White Paper

Quest Engineering

October 2017

Patents

Trademarks

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Setting Up the DR Series System as a CIFS, NFS and iSCSI-VTL Target on Tivoli Storage Manager v7.1

Updated – December 22, 2017

Contents

Revisions

Date	Description
January 2014	Initial release
November 2016	Updated the guide with new DR-4.0 GUI screens
October 2017	Updated with Quest-branded DR Series GUI screenshots (v4.0.3)

Executive Summary

This paper provides information about how to set up the DR Series system as a backup 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://support.quest.com/DR-Series

For more information about Tivoli Storage Manager, refer to the IBM documentation at:

https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.2/tsm/welcome.html

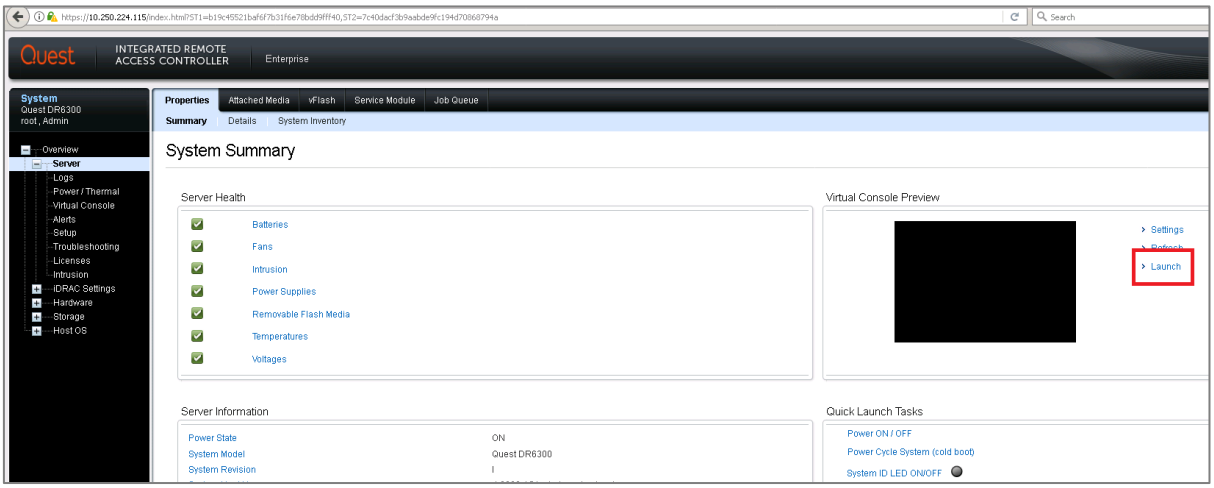
NOTE: The DR Series system/TSM build version and screenshots used in this document might vary slightly, depending on the version of the DR Series system/TSM Software version you are using.

Installing and configuring the DR Series system

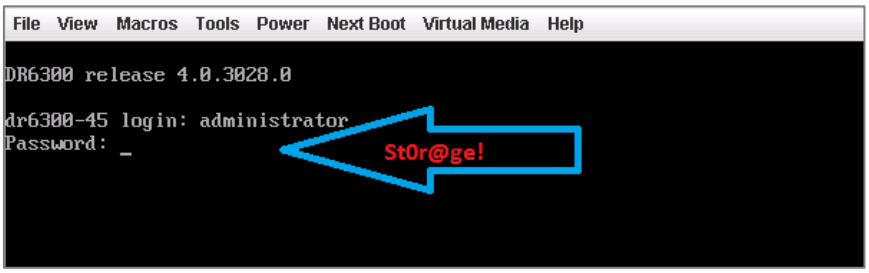
1 Rack and cable the DR Series system, and power it on. In the Dell DR Series System Administrator Guide, refer to the sections “iDRAC Connection”, “Logging in and Initializing the DR Series System”, and “Accessing IDRAC6/Idrac7 Using RACADM” for information about using the iDRAC connection and initializing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

2 Log on to iDRAC at 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.

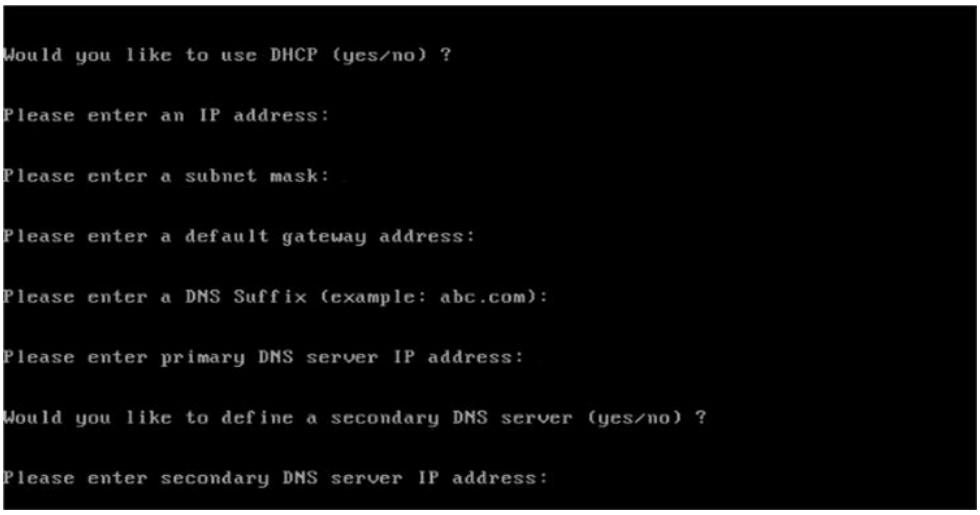
3 Launch the virtual console.



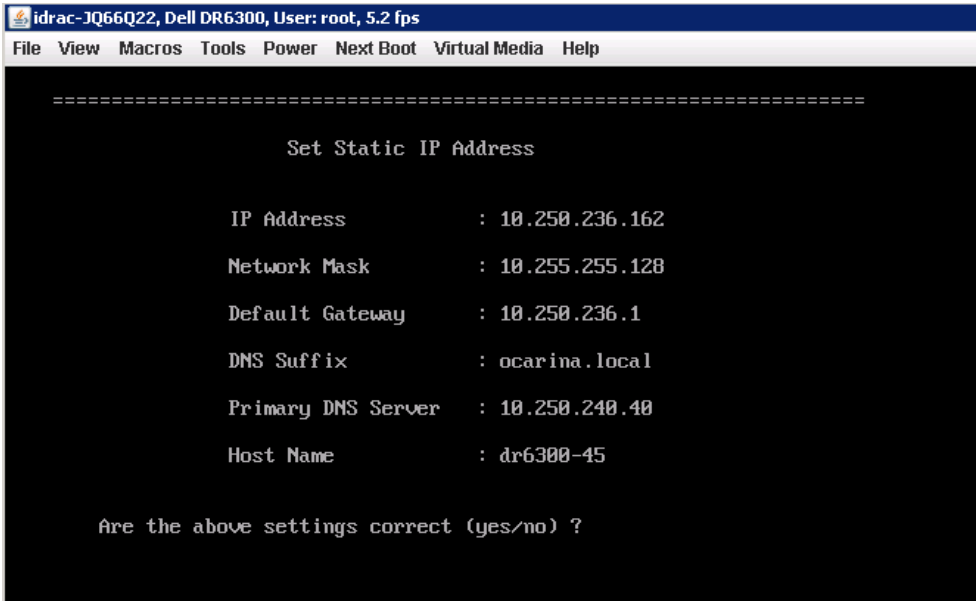
4 After the virtual console is open, log on to the system as the user **administrator** with the password **St0r@ge!** (The “0” in the password is the numeral zero).



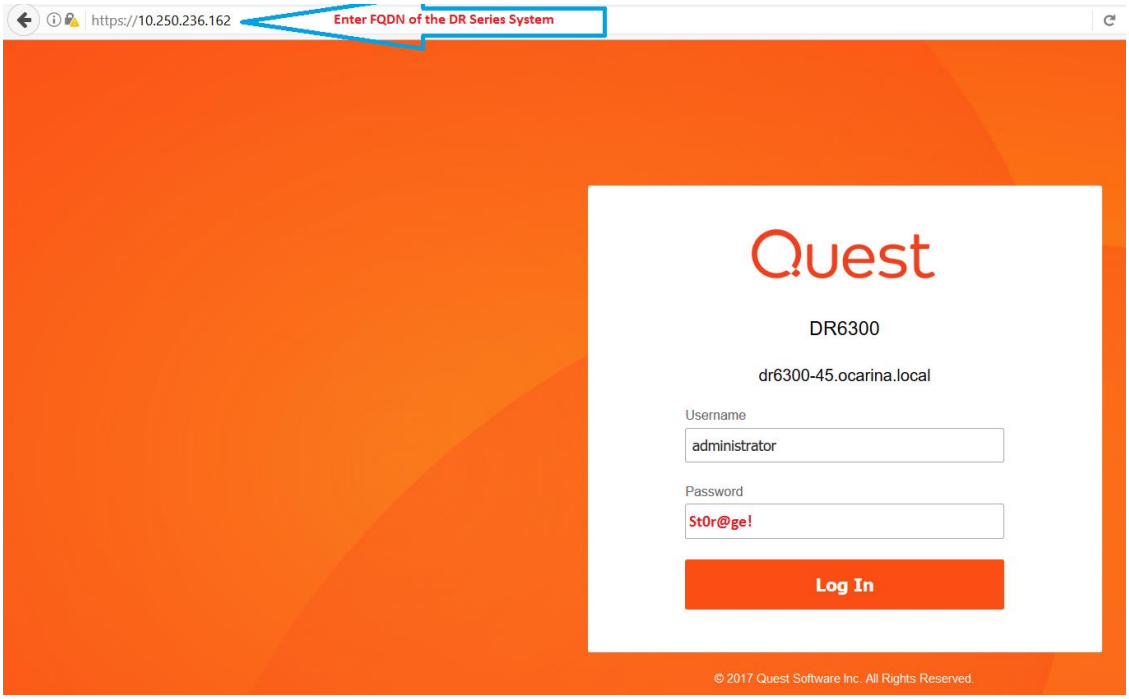
5 Set the user-defined networking preferences.



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



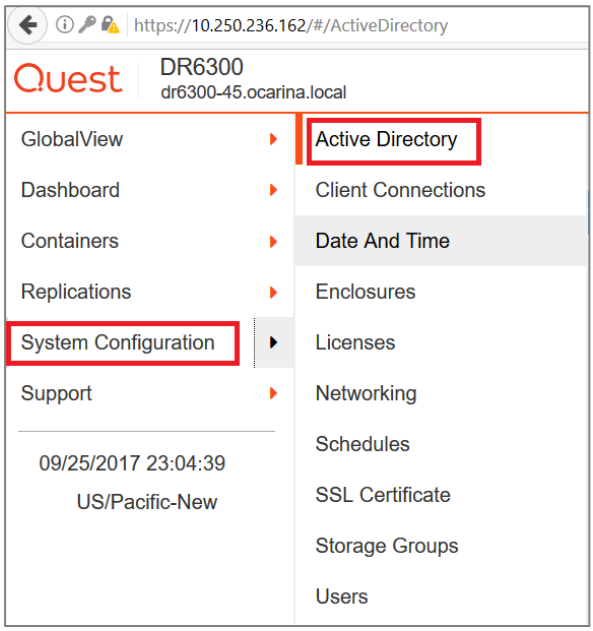
7 Log on to the DR Series system administrator console with the Hostname or the IP address you just provided for the DR Series system with the username: **administrator** and password: **St0r@ge!** (The “0” in the password is the numeral zero.).



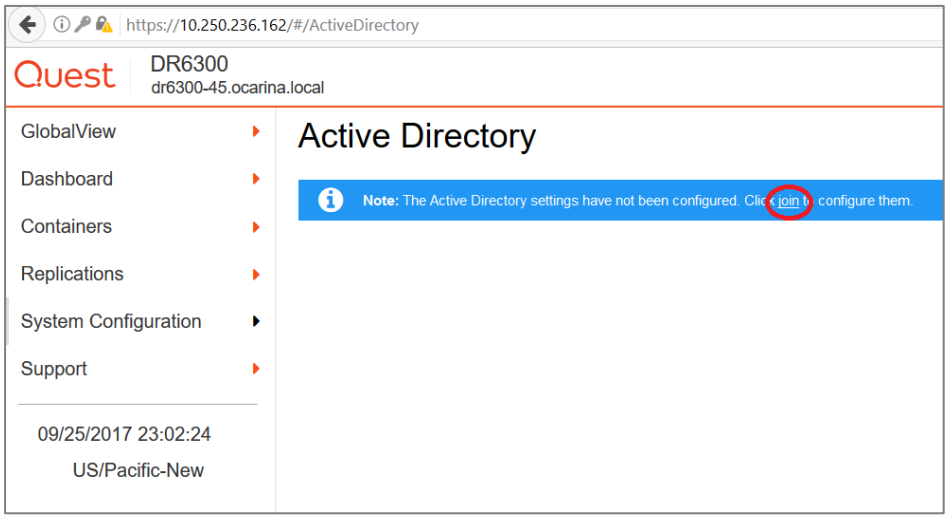
NOTE if you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

8 Join the DR Series system into the Active Directory domain.

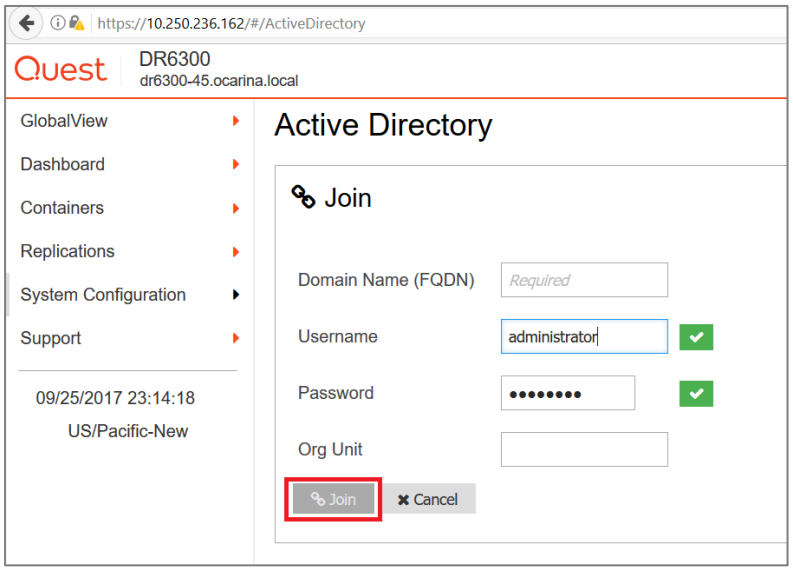
a Select **System Configuration** > **Active Directory** from the left navigation area of the DR Series system GUI.



b Click the **Join** link.



c Enter valid credentials, and then click the **Join** button.

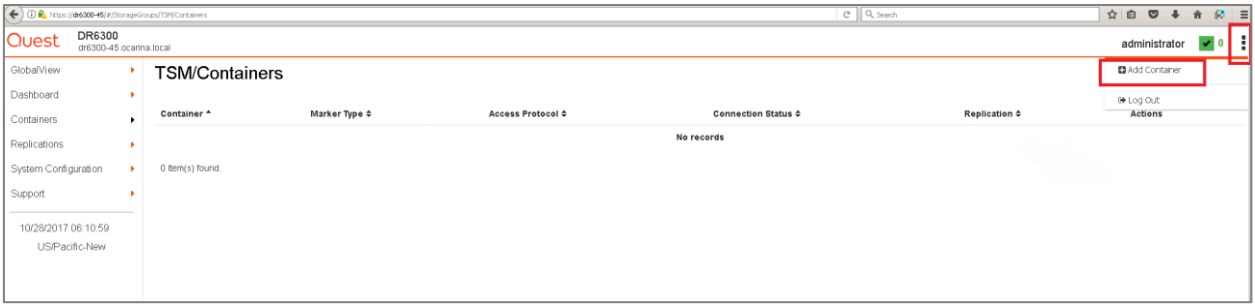


Creating a container with an NFS or CIFS connection

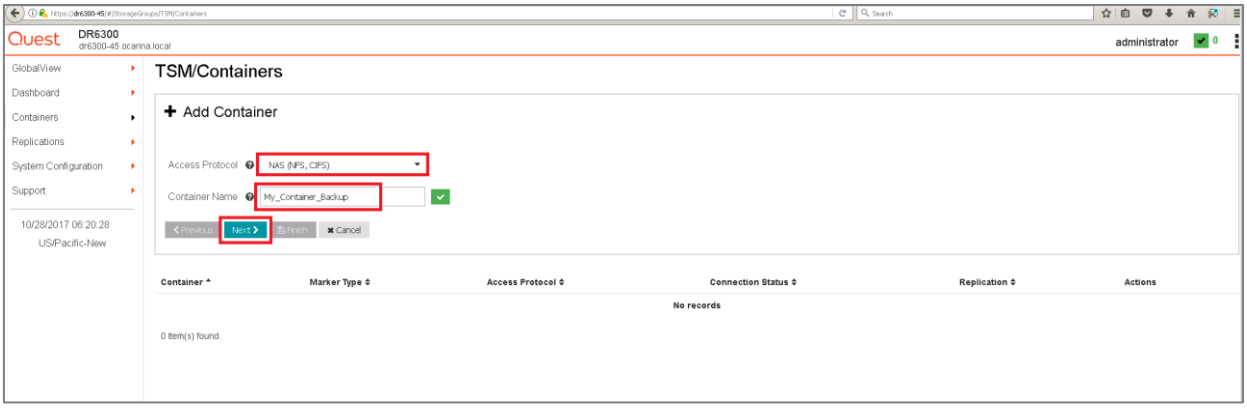
1 Create a container by selecting **Containers** in the left navigation area, and then selecting the required **Storage Group**.

NOTE: For more information about storage groups in the DR Series system, see the *DR Series System Admininstrator's Guide.*

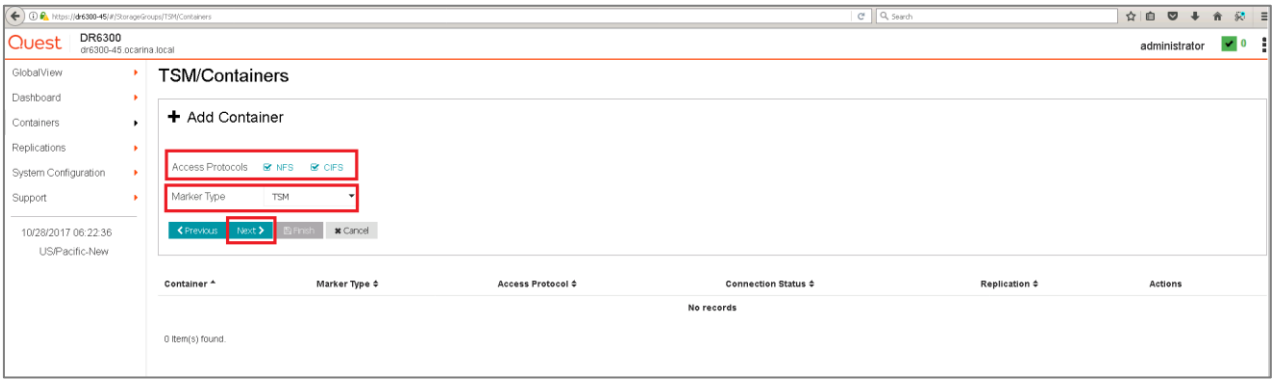
2 On the Action Menu in the upper right corner of the page, click **Add Container**.



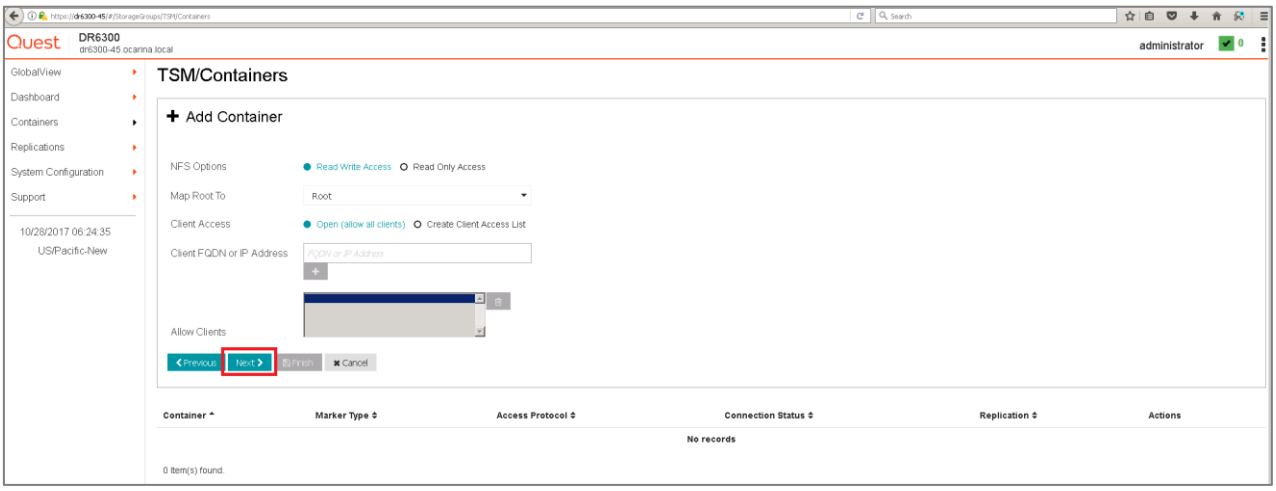
3 Enter a container name, select the access protocol as **NAS (NFS, CIFS)**, and click **Next**.



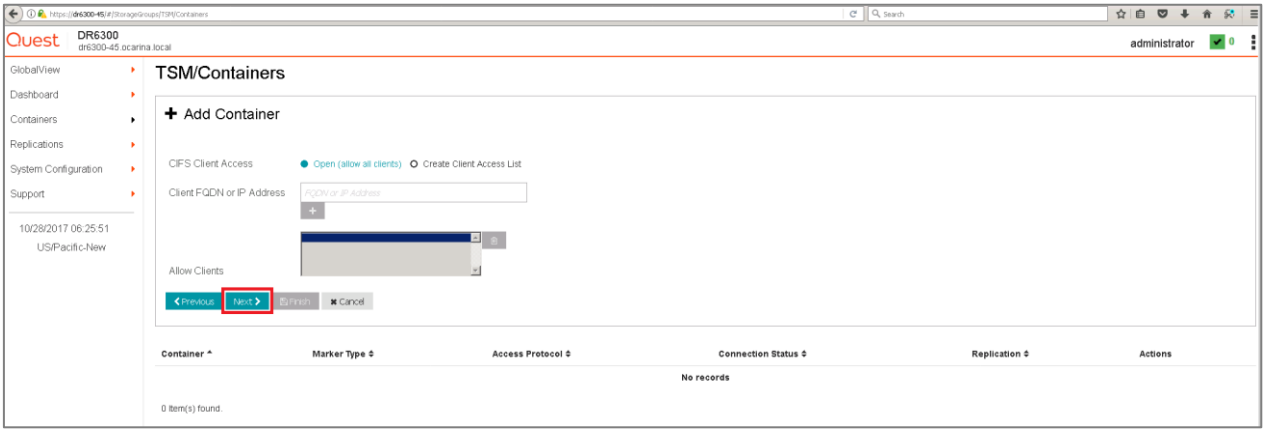
4 Select the storage access protocol you want to use, set the marker type as **AUTO/TSM** and then click **Next**.



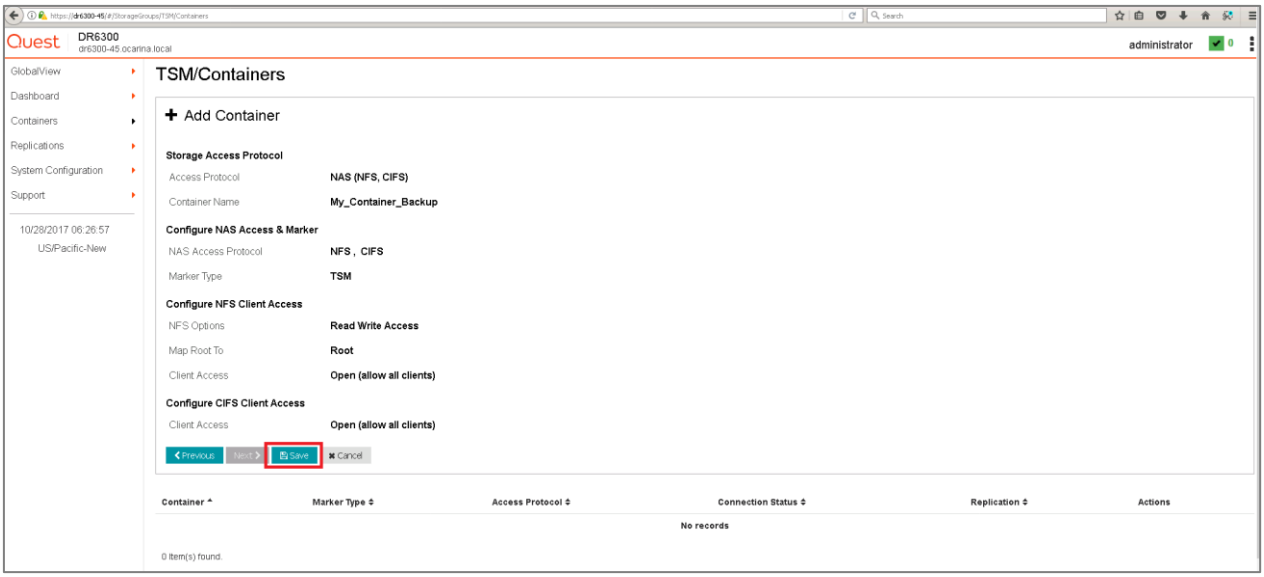
5 For NFS, select the preferred client access credentials, and click **Next**.



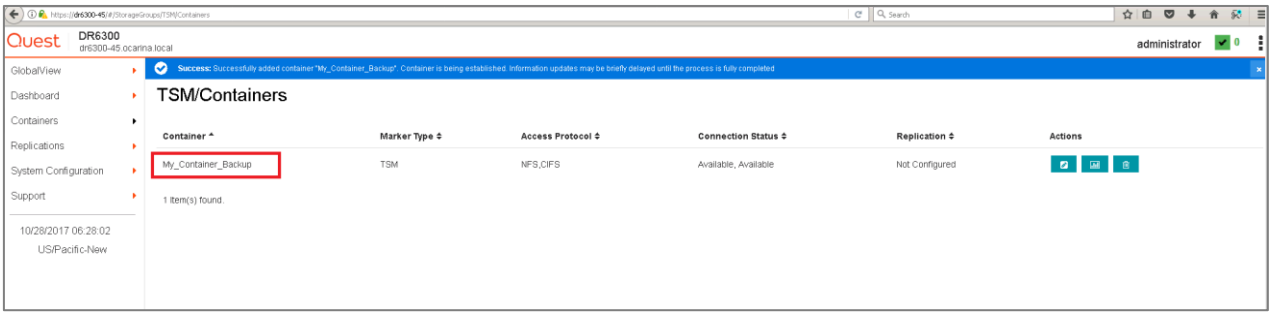
6 For CIFS, select the preferred client access credentials, and click **Next**.



7 Review the summary and then click **Save** to add the container.

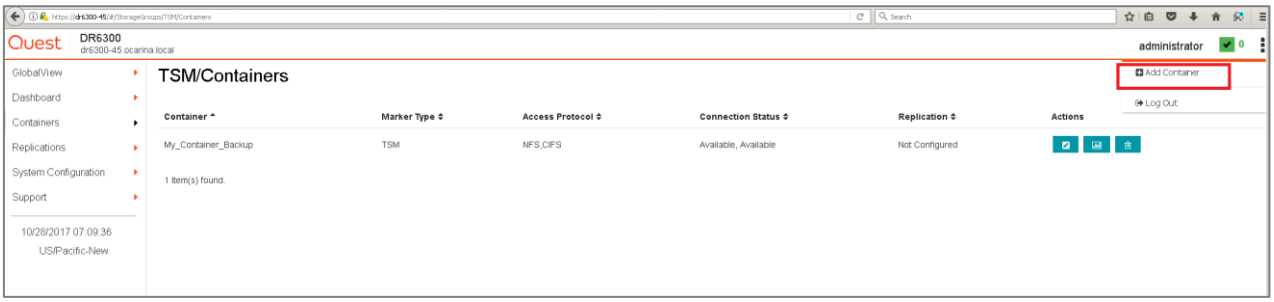


8 Confirm that the Container has been added.

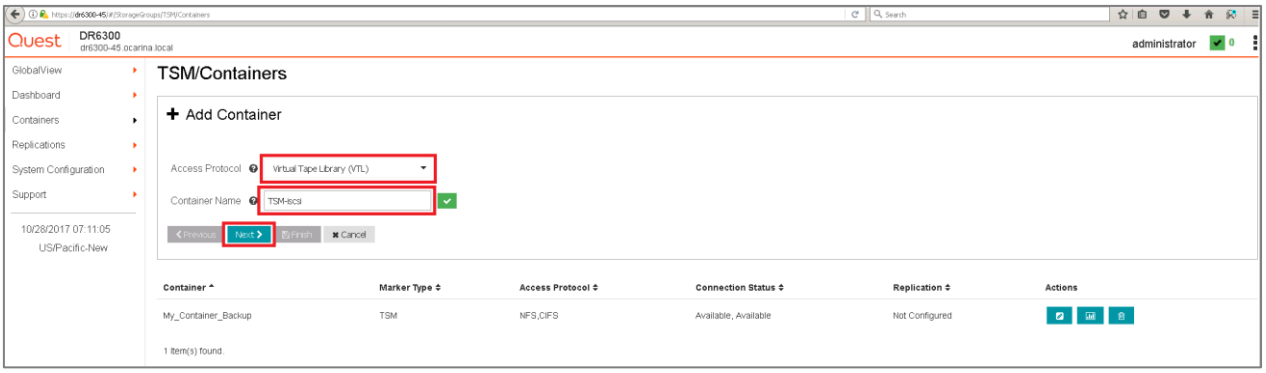


Creating a VTL container with an iSCSI connection

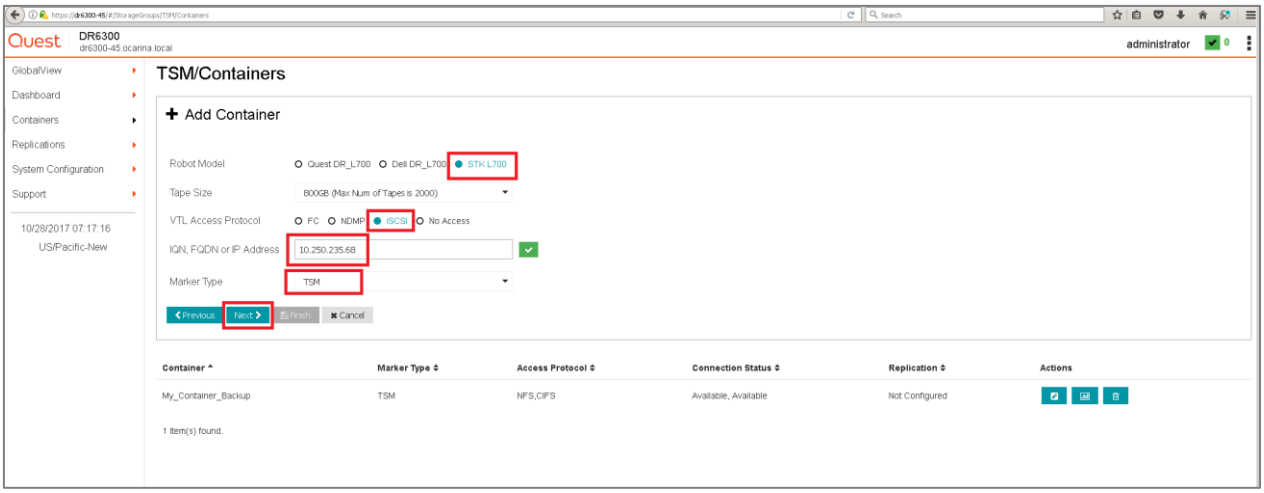
1 Select **Containers** in the left navigation area, and, on the **Action Menu** in the upper right corner of the page, select **Add Container**.



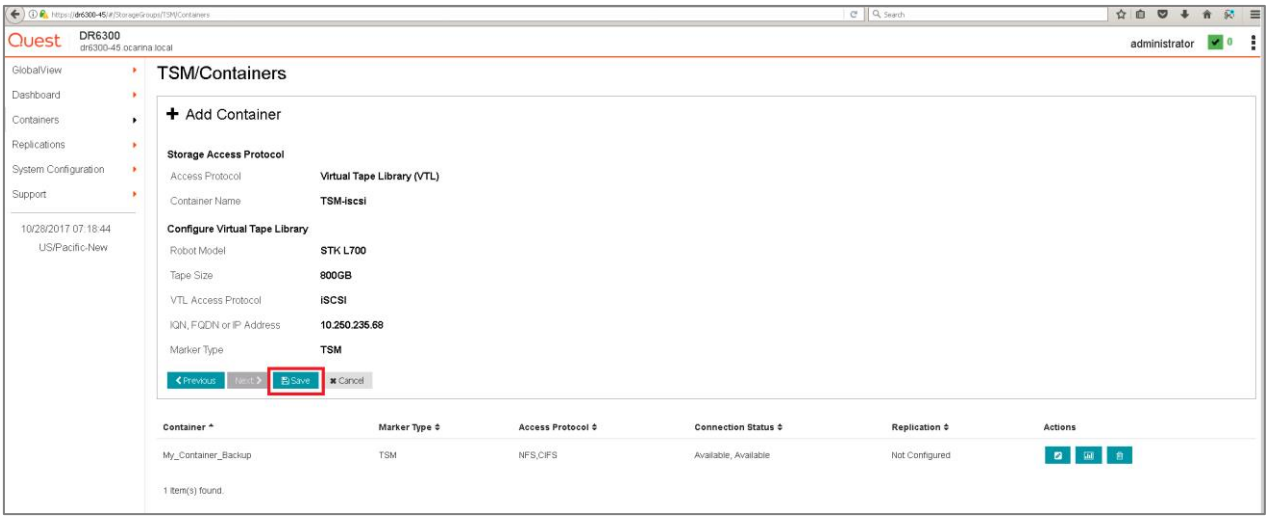
2 Enter the name of the container, select **Virtual Tape Library (VTL)** as the access protocol, and click **Next**.



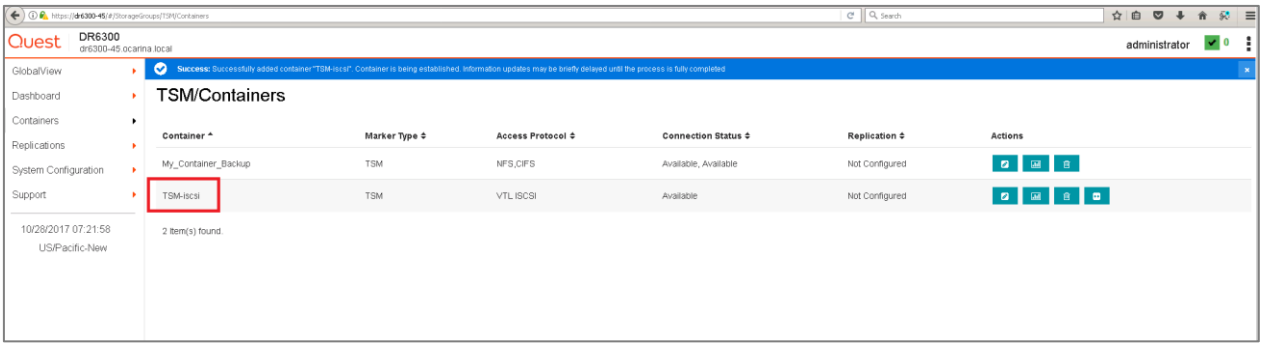
3 Select the required tape size, access protocol, marker type, and initiator details, and click **Next**.



4 Review the summary and then click **Save** to add the container.



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



2

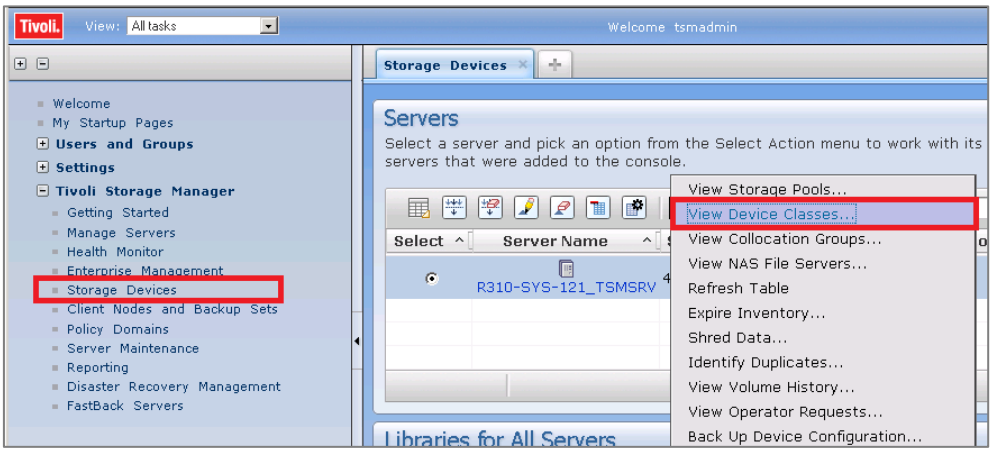
Configuring TSM for CIFS and NFS targets

Configuring the device class for CIFS and NFS protocols

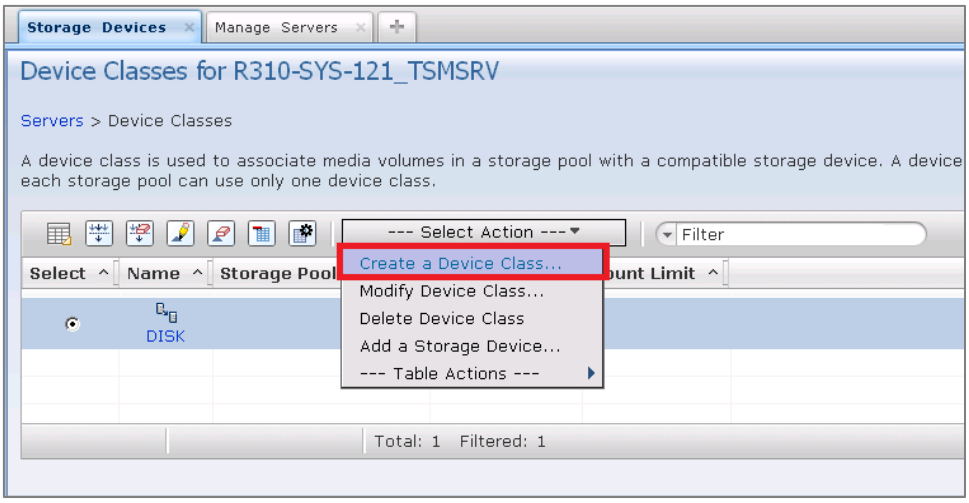
These instructions walk you through a basic configuration for connecting a DR Series system appliance with the Windows version of Tivoli Storage Manager (v7.1.4).

1 Open the IBM Tivoli Storage Manger Administration Center.

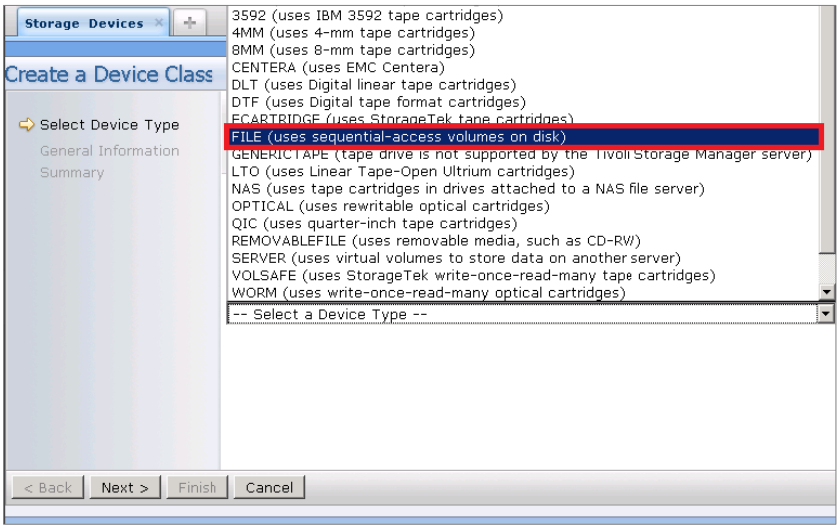
2 Click **Storage Devices** > **View Storage Classes**.



3 Click **Create a Device Class**.

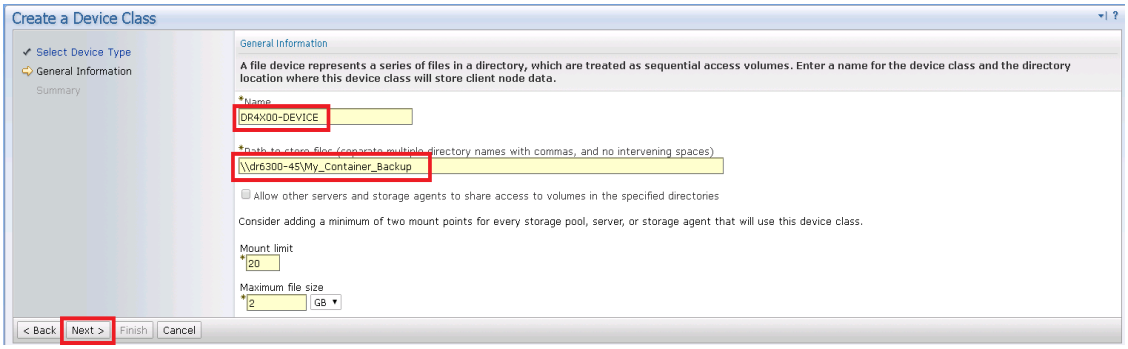


4 Select the **FILE** device type and click **Next**. (This device type is optimized for writing to disk-based storage.)

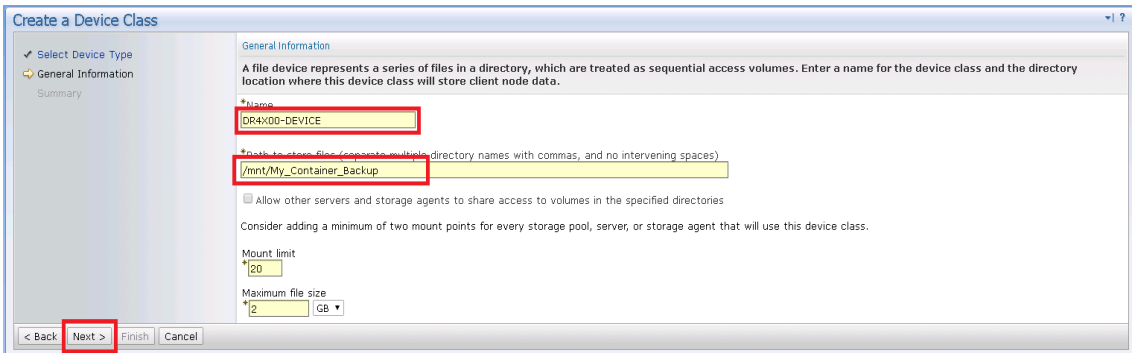


5 Enter the appropriate information under General Information and click **Next**.

6 For a CIFS Container Path:



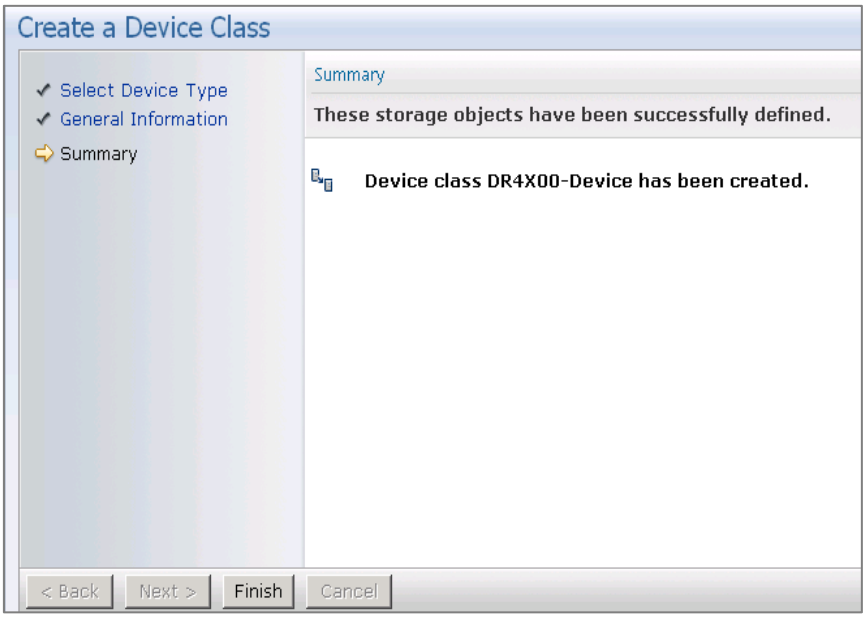
7 For an NFS container path:



- **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 connection limit. Please consult the DR Series Interoperability Guide for your systems maximum 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.

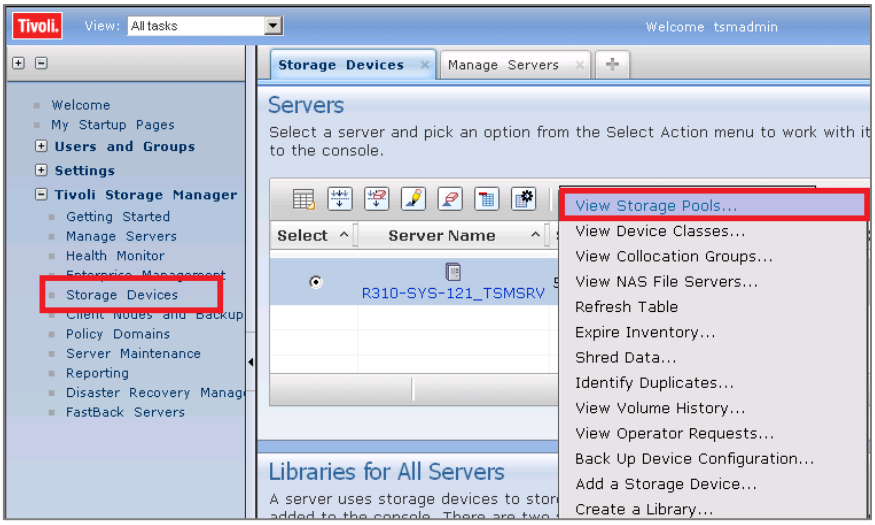
NOTE: The service account for Tivoli Storage Manager needs to have the correct permission to the DR Series system CIFS share for this step to complete successfully. Before providing the information, see Appendix A for information about setting up the TSM service account correctly.

8 Click **Finish**.

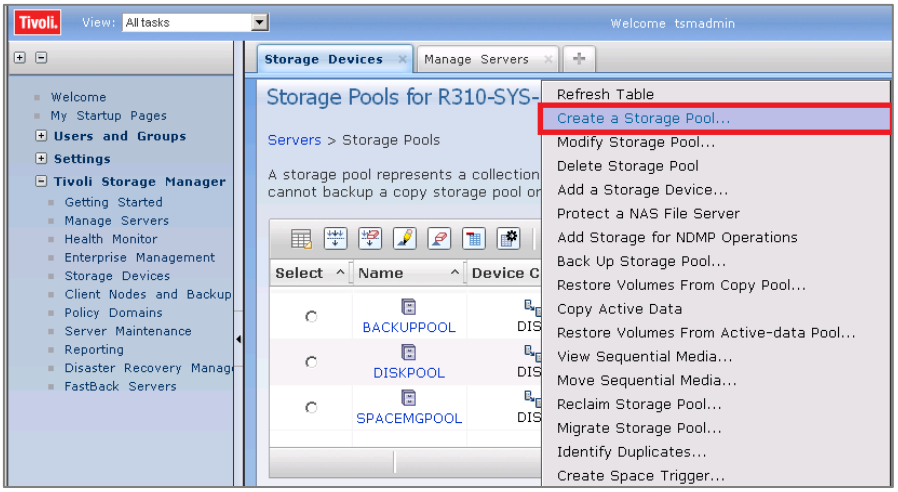


Configuring a storage pool for the CIFS and NFS protocols

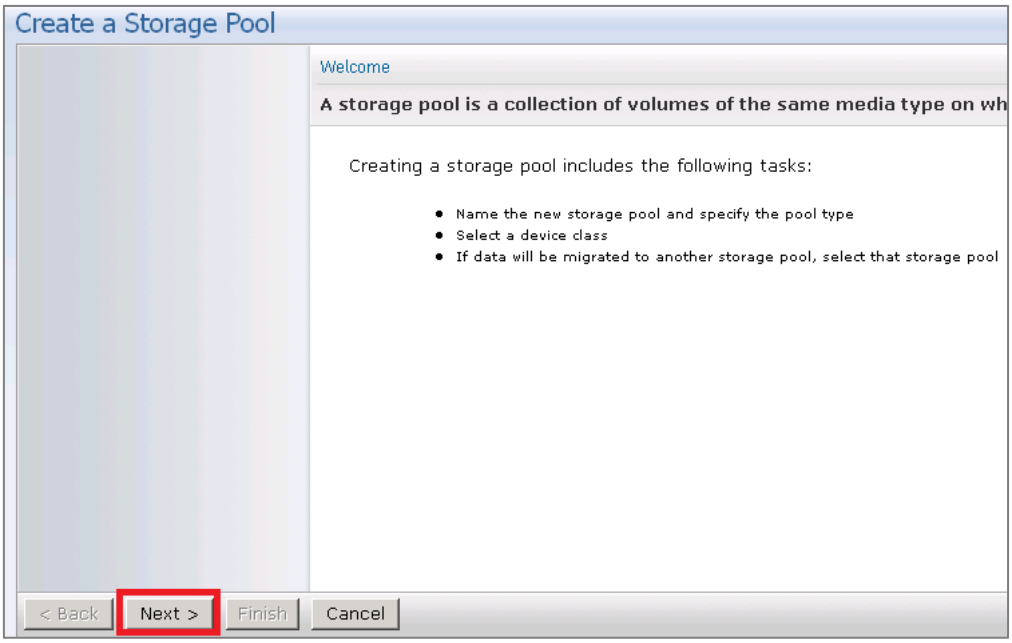
1 Click **Storage Devices > View Storage Pools.**



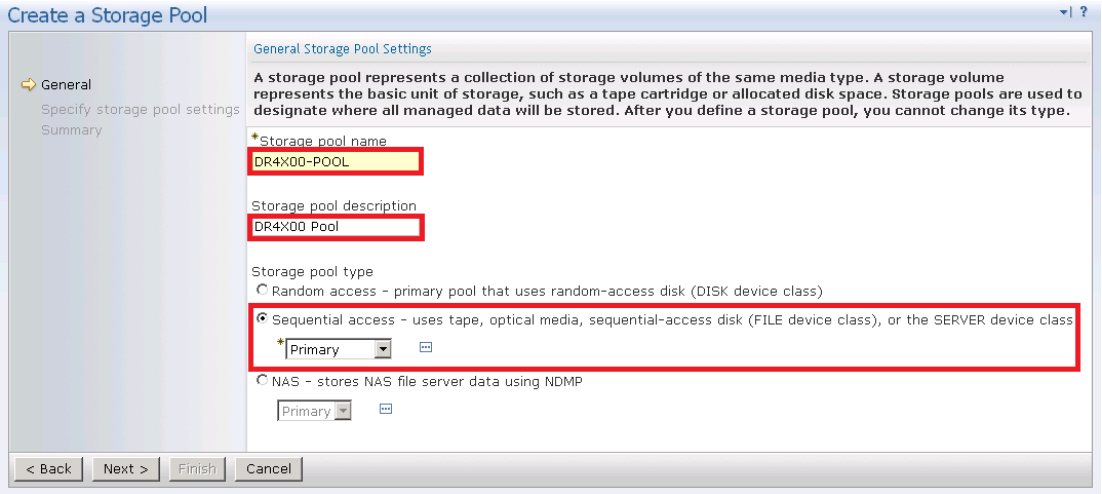
2 Click **Create Storage Pools**.



3 Click **Next**.

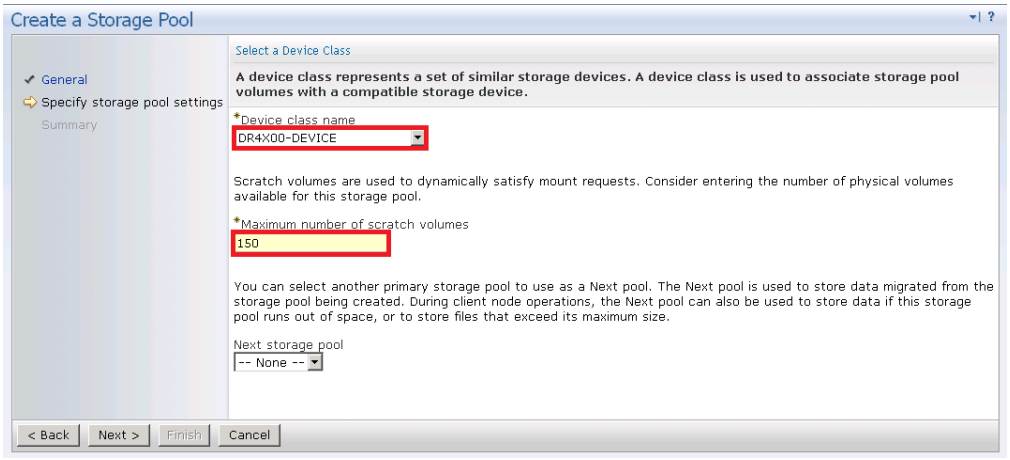


4 Enter the information for the General Storage Pool Settings and then click **Next**.



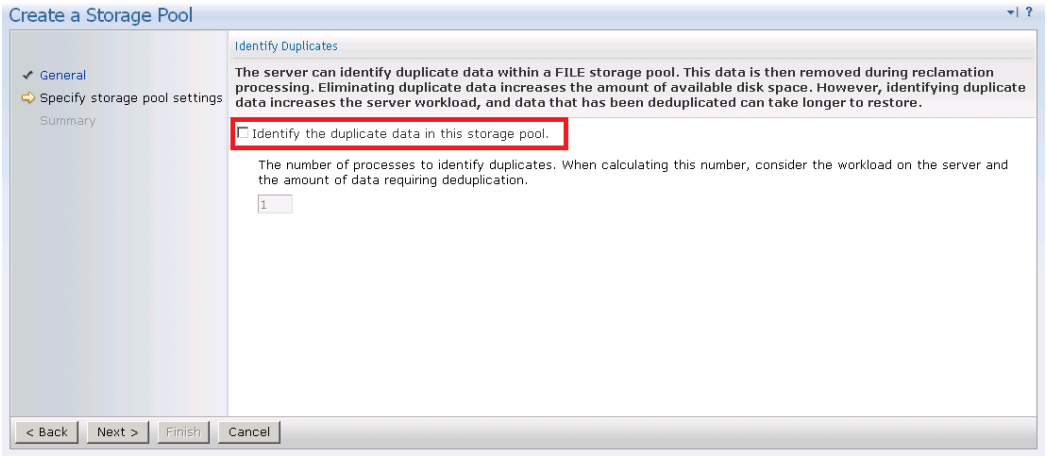
- **Storage Pool Name:** Enter a descriptive name for the DR Series system pool.
- **Storage Pool Description:** Enter a description for the DR Series system pool.
- **Storage Pool Type**: Select **Sequential Access** as the DR Series system is integrated as a FILE type device.

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



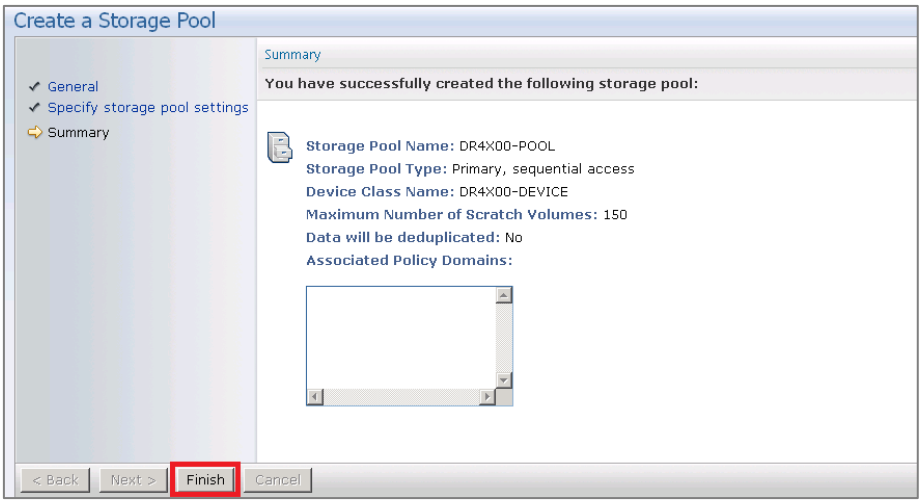
- **Device Class Name:** Select the name of the DR Series system device class (created previously).
- **Maximum Number of Scratch Volumes:** Set the number of scratch volumes in the system. (Setting the value between 100 to 200 scratch volumes is recommended.)

6 For Identifying Duplicates, accept the default selections, and click **Next**.



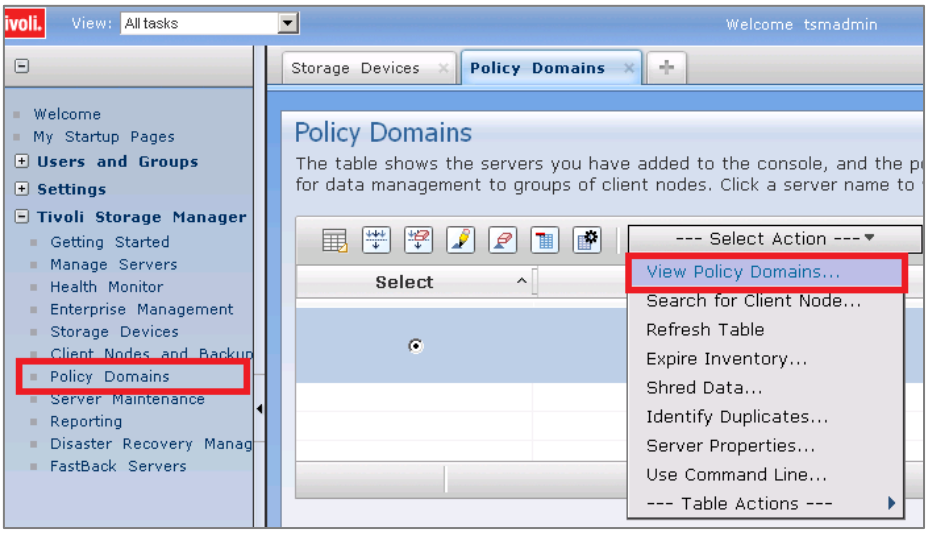
- Keep the **Identify the duplicate data in the storage pool** check box clear as the DR Series system uses inline deduplication and already identifies and removes duplicate data.

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

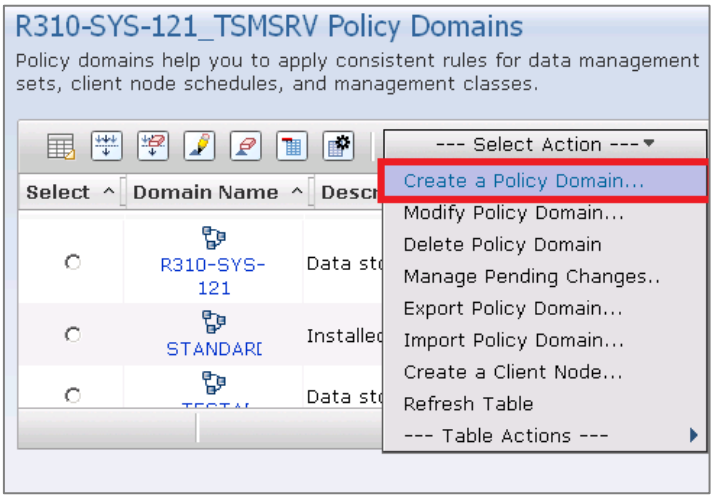


Creating a policy domain for the job

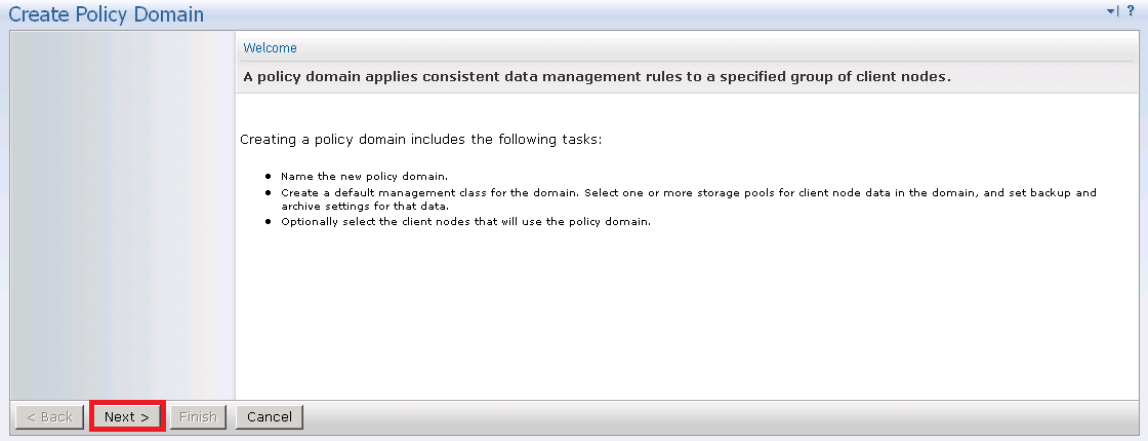
1 Click **Policy Domain > View Policy Domain**.



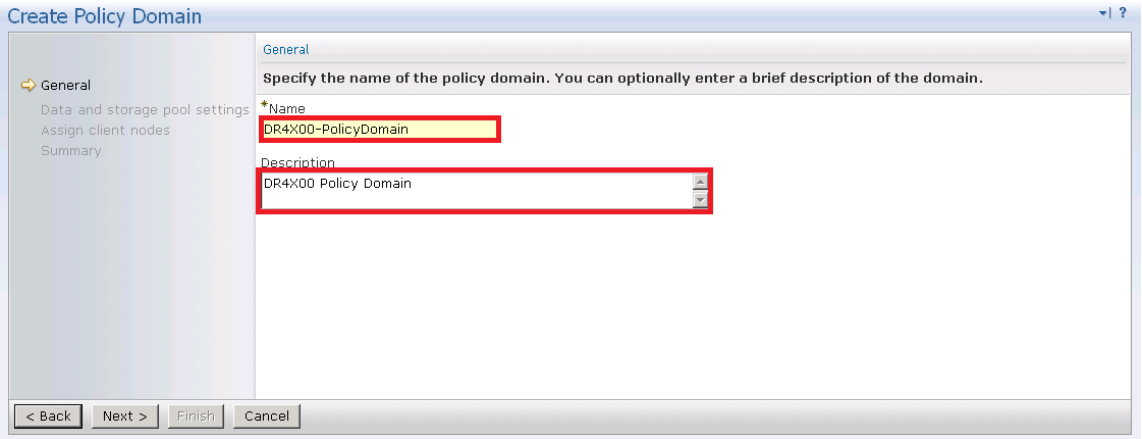
2 Click **Create a Policy Domain**.



3 Click **Next**.

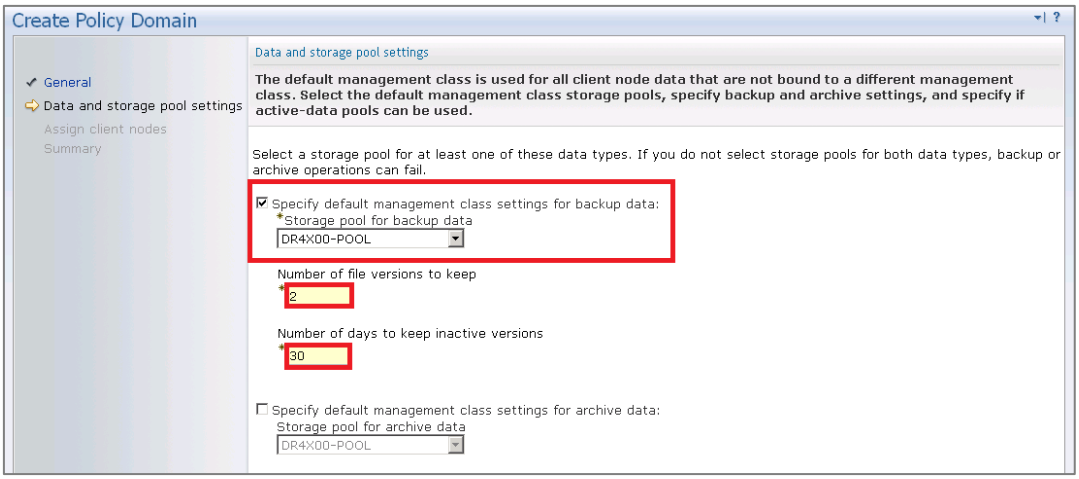


4 Enter the required information, and then click **Next**.



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

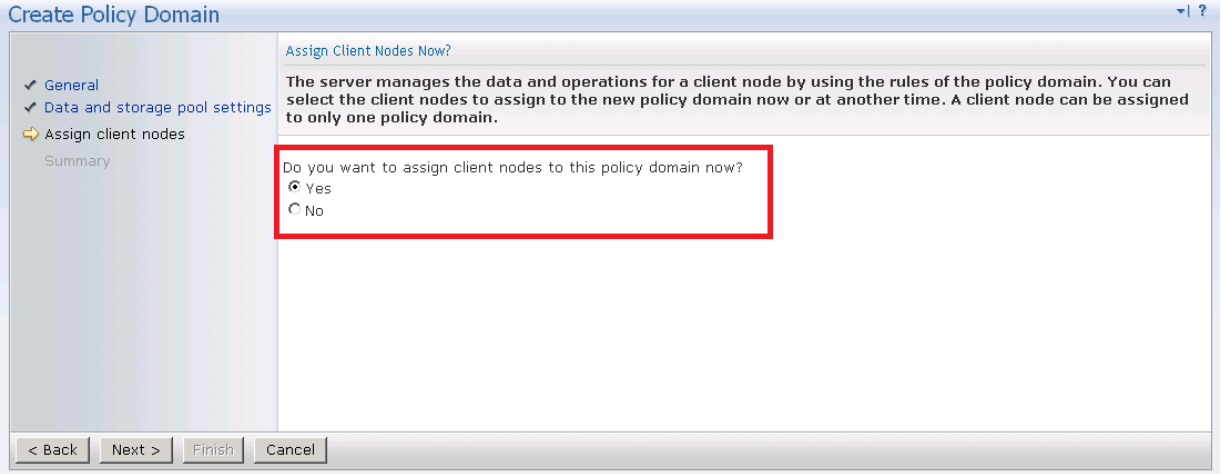
5 Enter the required information for data and storage pool settings, and then click Next.



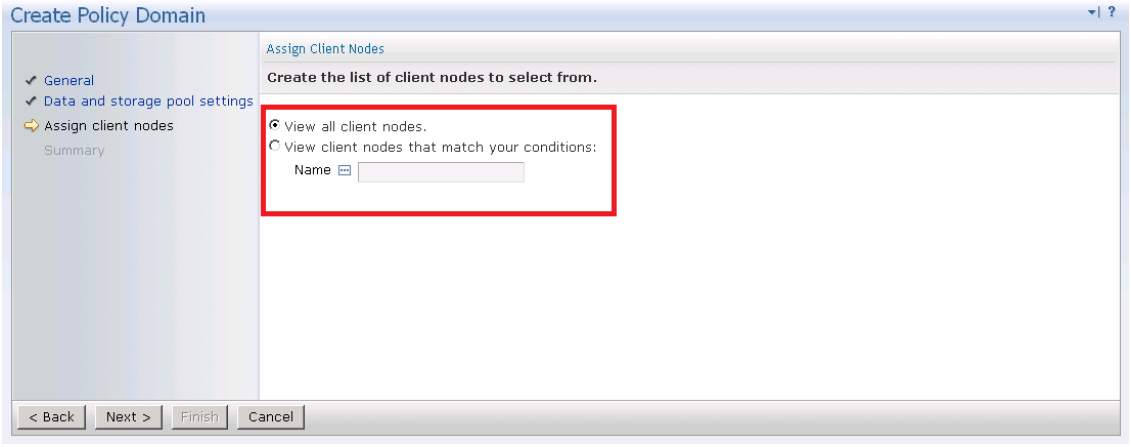
- **Specify default management class:** Select the DR Series system pool that was set up previously.
- **Number of file versions to Keep:** Specify how many versions of a file to keep.
- **Number of days to keep inactive versions**: Specify how many days to retain data after it falls out of policy.

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

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

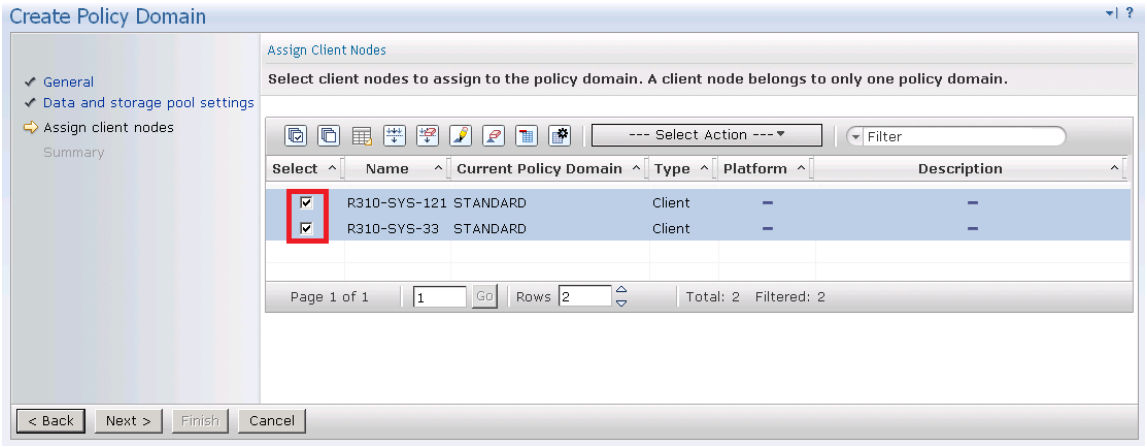


7 Select to display the set of clients to move to the DR Series system, and click **Next**.

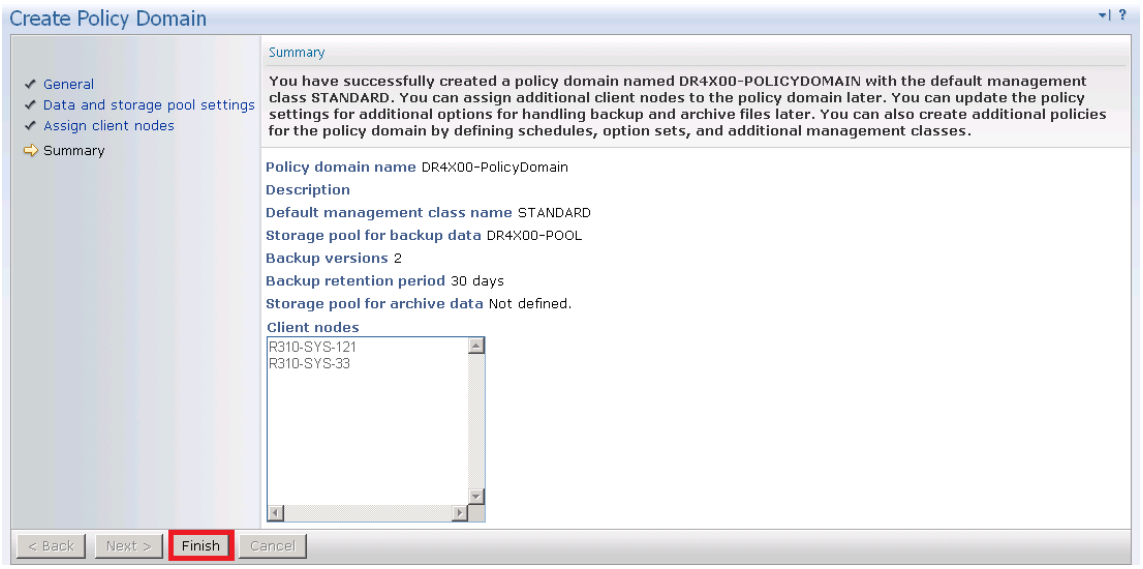


NOTE: Choose to limit if you have a lot of client computers.

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

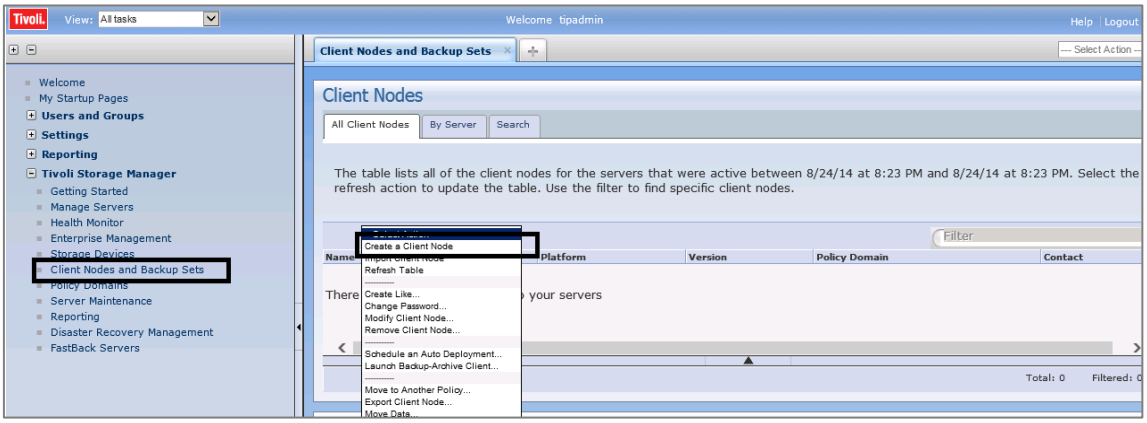


9 Click **Finish**.

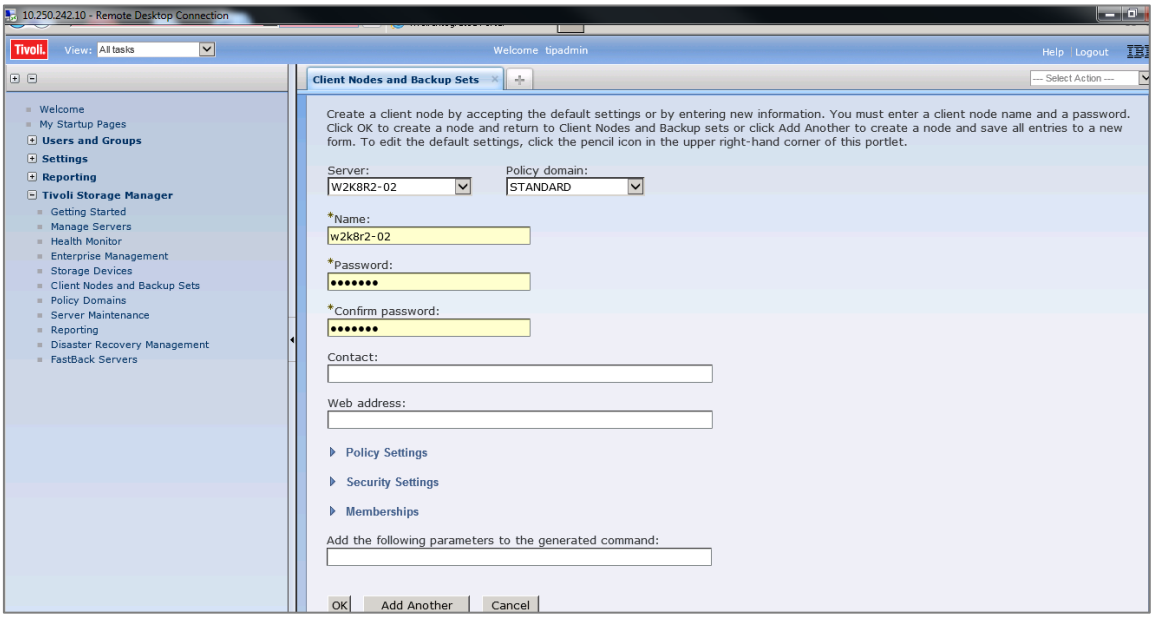


Creating client nodes and backup sets

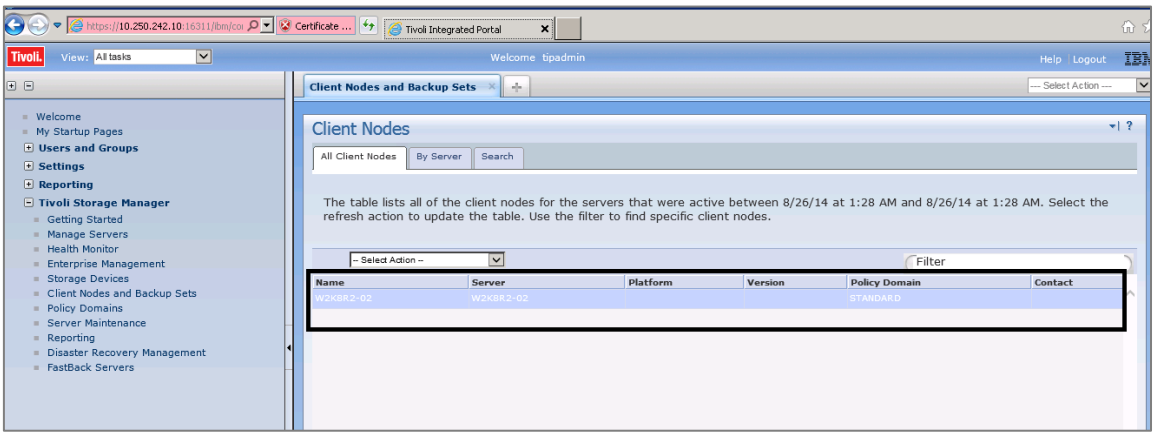
1 Open the client nodes and backup sets from Tivoli Storage Manager to register the client machine.



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



3 Confirm that the client node is successfully registered.

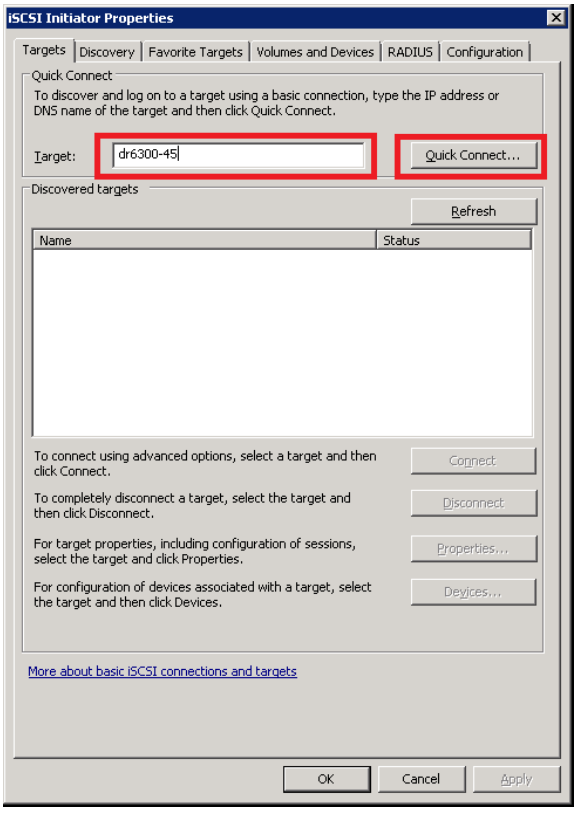


Configuring iSCSI target container(s) for TSM

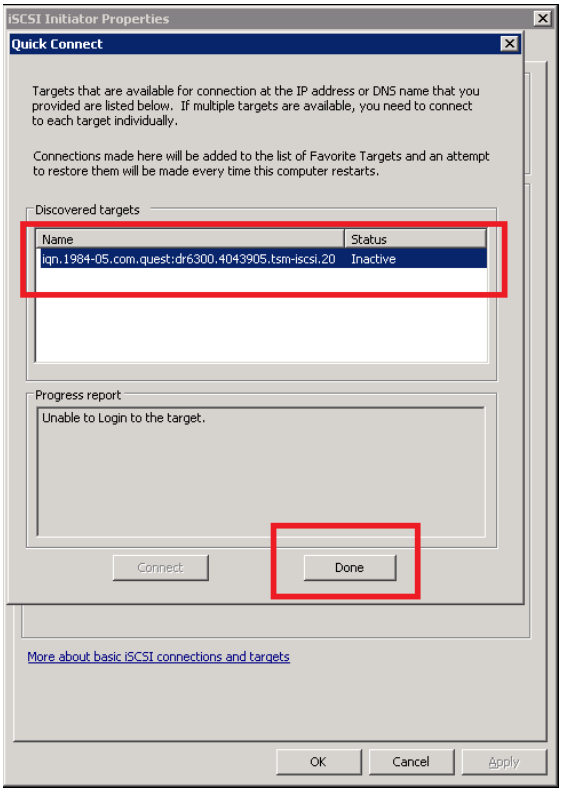
Configuring the iSCSI initiator

Configuring the iSCSI initiator for Windows (TSM Server)

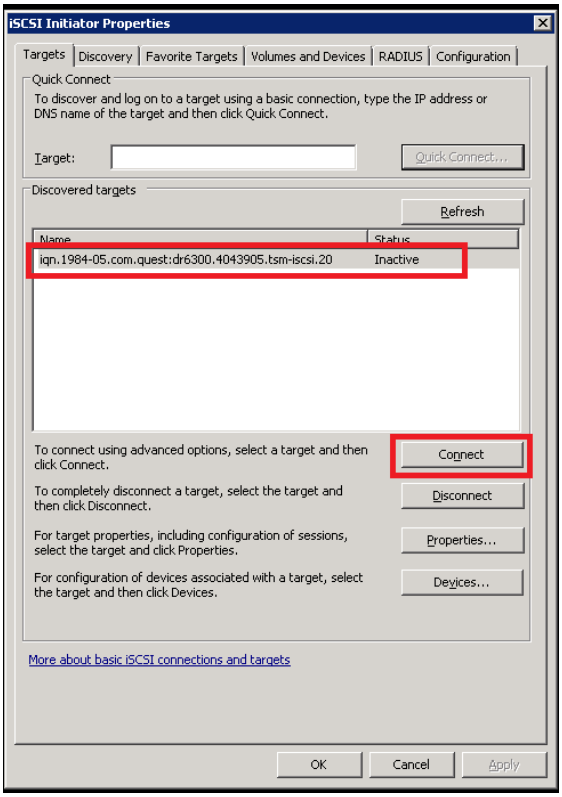
1 In the Windows TSM Server, open your iscsi initiator software, enter the DR Series system IP/Hostname as the target, and click **Quick connect**.



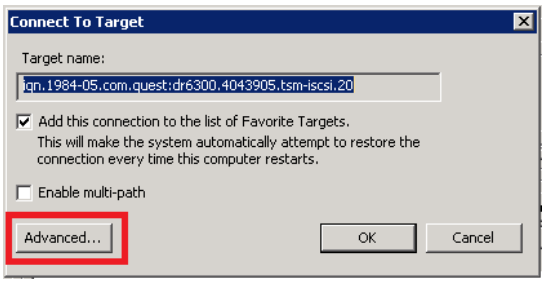
2 Quick connect will discover the targets.Click **Done**.



3 Select the required targets and click **Connect**

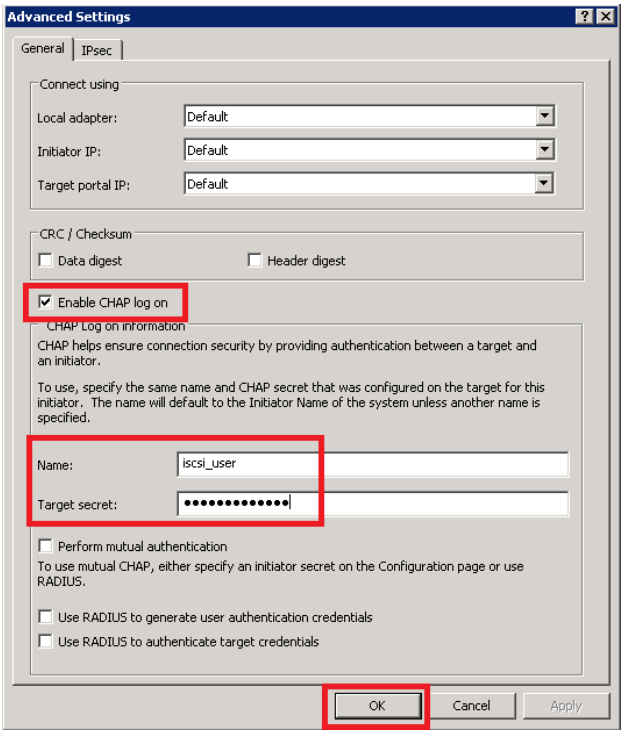


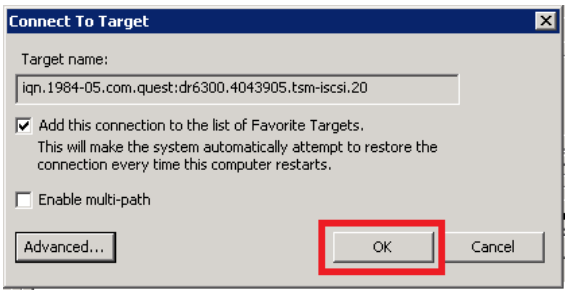
4 Click **Advanced**.



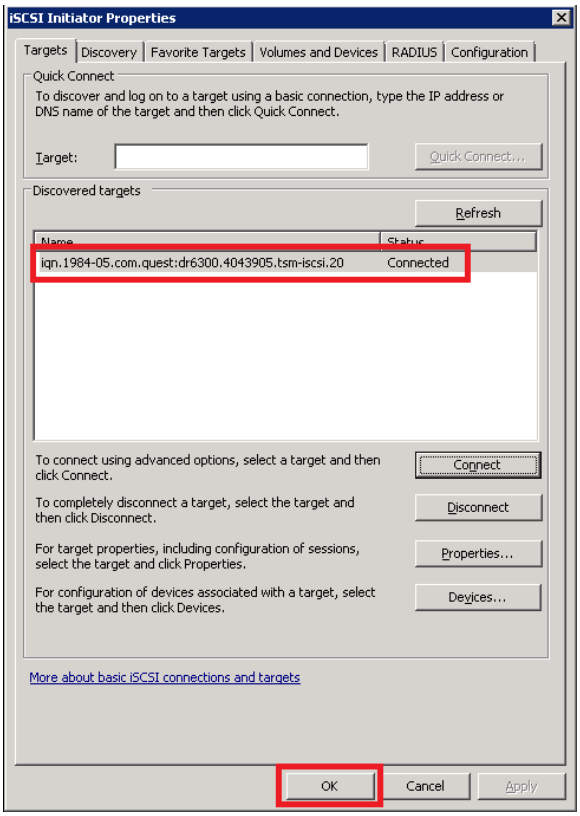
5 Click **Enable CHAP log on**, provide the name: iscsi_user, with the password: St0r@ge!iscsi, and click **OK**.

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





6 Check the Status as connected and click **OK.**



Configuring the iSCSI Initiator for Linux (TSM Server)

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

```
#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 <FQDN 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 <FQDN 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.quest:dr6300.3071067.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 “cat /proc/scsi/scsi” command to see the LUN and HOST details.

Configuring the DR Series system VTL for the Windows and Linux TSM server

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

```
cd “C:\Program Files\Tivoli\TSM\server\tsmdiag”
tsmdlst.exe
```

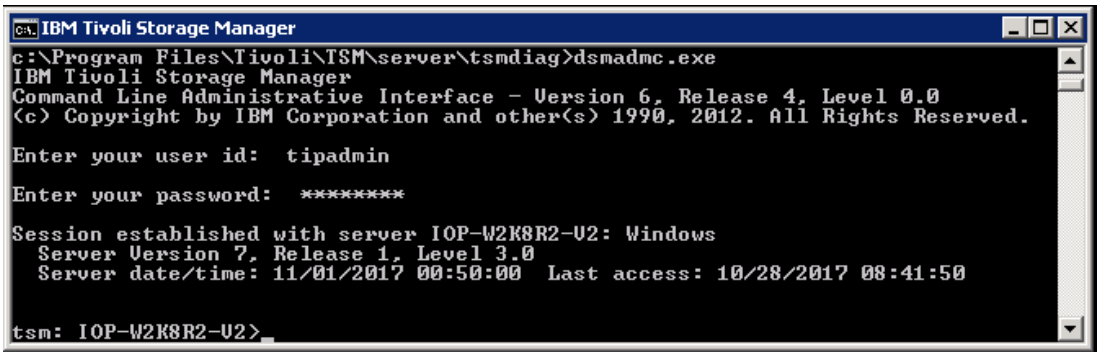
For Linux: For discovering the tape devices and associated IDs, see Appendix C of this document.

Windows configuration

All commands should be executed on the TSM Server Prompt.

1 Open a CMD prompt and cd to “C:\Program Files\Tivoli\TSM\server\tsmdiag”

2 Run “dsmadmc.exe” and enter the username/password for the TSM server.



3 Define Library -

```
# define library TSM-iscsi libtype=scsi shared=yes autolabel=yes
(TSM-iscsi is user defined name for the library)
```

4 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, and Device = Device ID for medium changer listed by “tsmdlst” command.

5 Define Drive -

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

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

6 Define Drive Path -

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

7 Audit the Library -

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

8 Checkin the Library Volumes –

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

Linux Configuration

All commands should be executed at the TSM Server Prompt.

1 You can get the TSM Server prompt by using the following commands:

```
[root@dma-rhel7-v1 bin]# ./dsmadmc

Enter your user id:  tipadmin

Enter your password:

Session established with server DMA-RHEL7-V1: Linux/x86_64

  Server Version 7, Release 1, Level 3.0

  Server date/time: 11/23/2017 02:38:33  Last access: 11/23/2017
02:37:32

tsm: DMA-RHEL7-V1>
```

2 Define Library:

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

3 Define Library path –

```
# define path RHEL-TSM-SERVER TSM-iscsi srct=server autodetect=yes
destt=library

device=/dev/tsmscsi/lb0
```

4 Define Drive -

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

5 Define Drive Path –

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

6 Audit the Library -

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

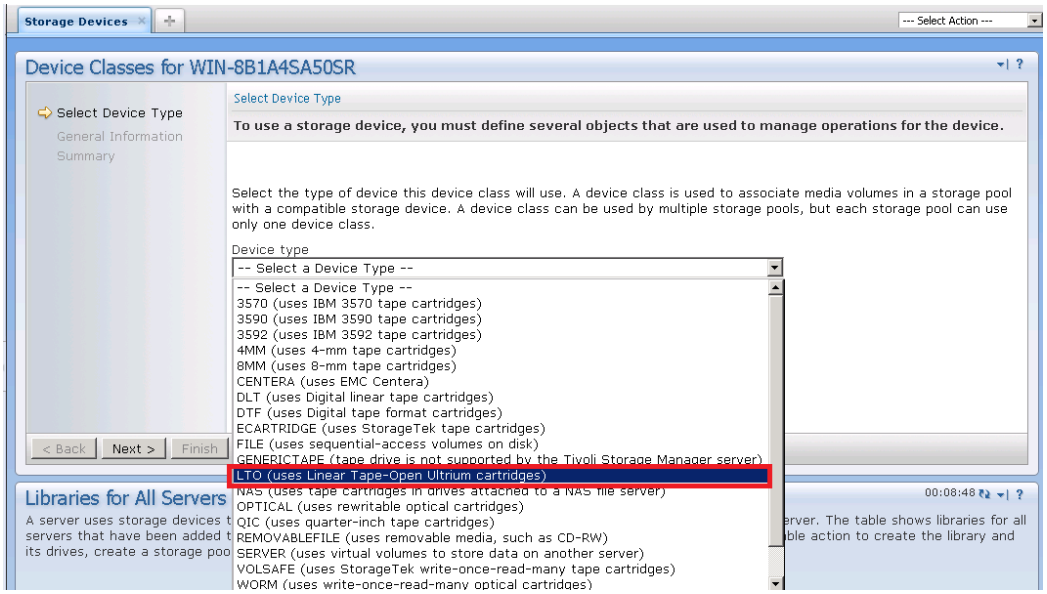
7 Checkin the Library Volumes –

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

Configuring the device class for iSCSI VTL

1 Follow Steps 1, 2, and 3 as described in the preceding Device Class creation section.

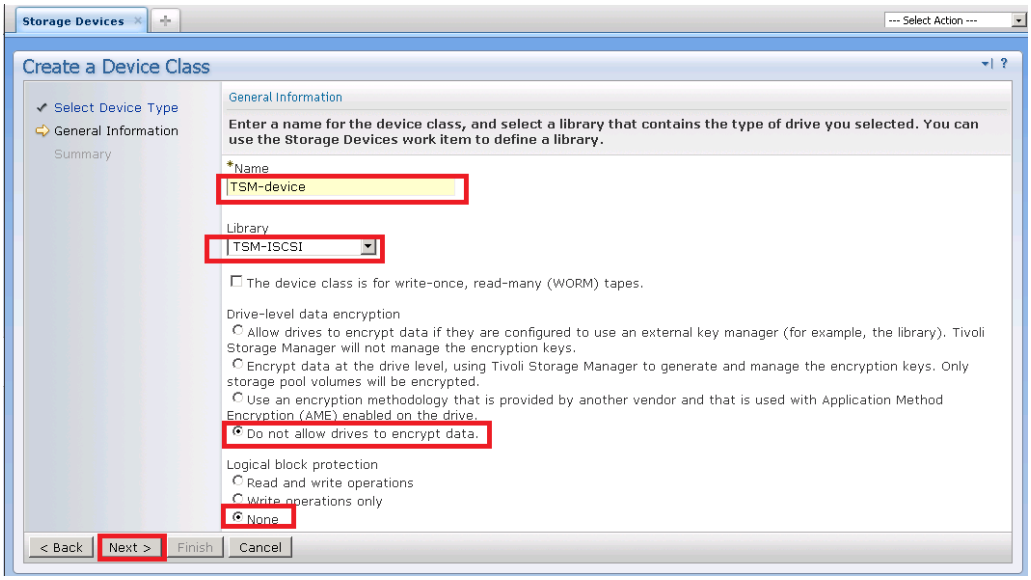
2 Select the Device Type as **LTO** for iSCSI VTL.



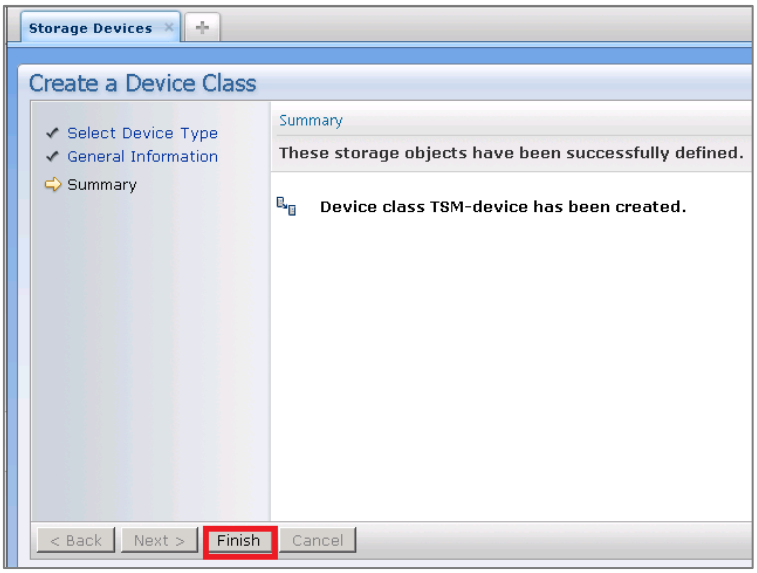
3 In the General Information section, provide the name and select the configured library.

4 In the Drive-level data encryption section, select the **Do not allow drives to encrypt data** option.

5 For Logical Block Protection, click **None**.



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

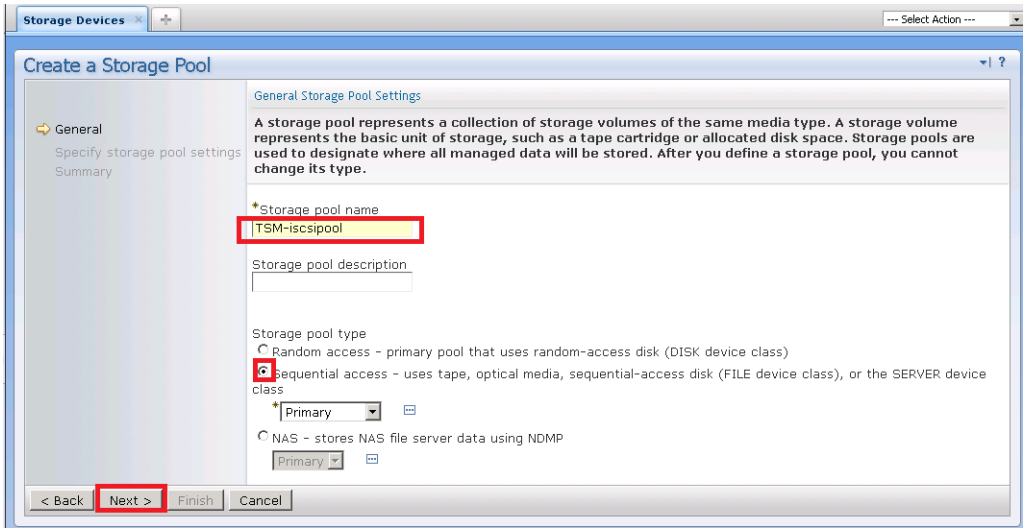


Configuring the storage pool for iSCSI VTL

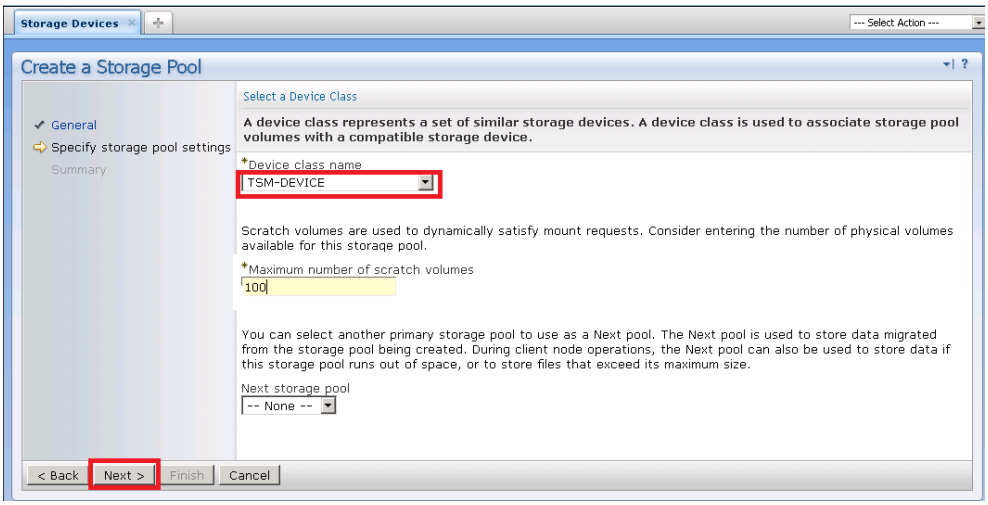
1 Follow the steps 1, 2 and 3 from the preceding Storage Pool creation section of this document.

2 In the General storage pool settings section, provide the pool name and type.

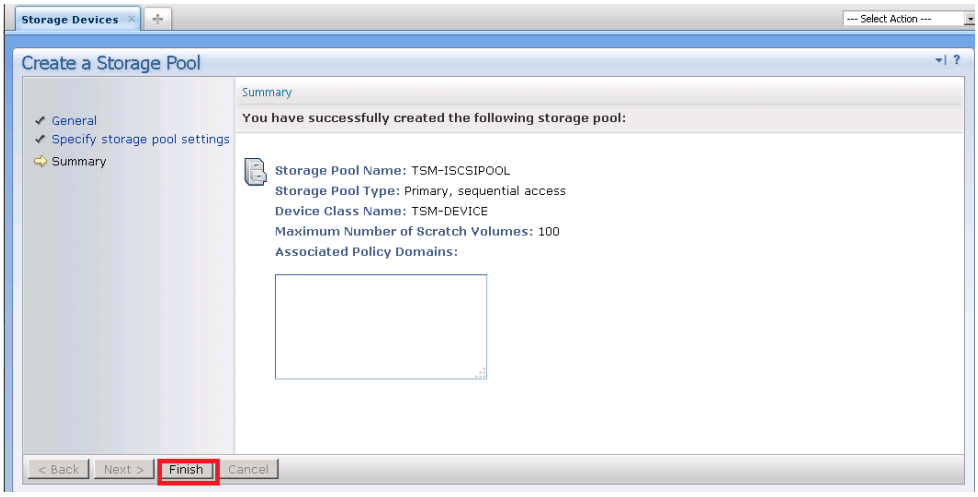
3 Click **Next**.



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



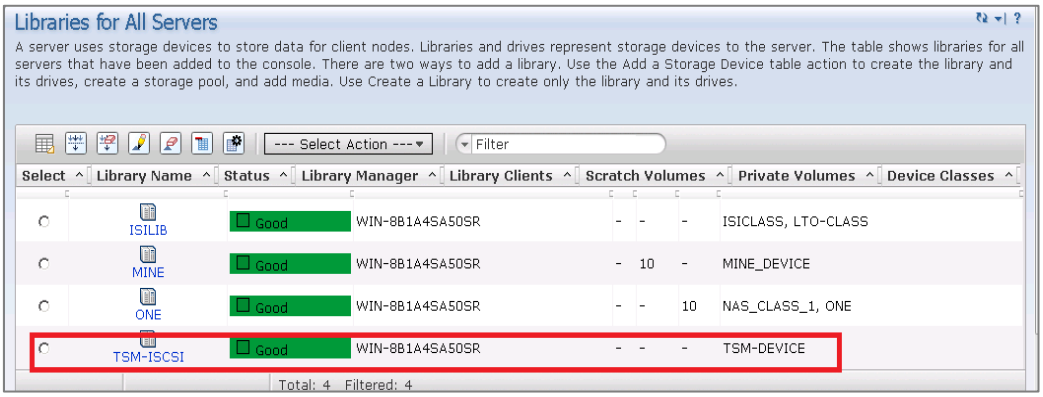
5 Click **Finish**.



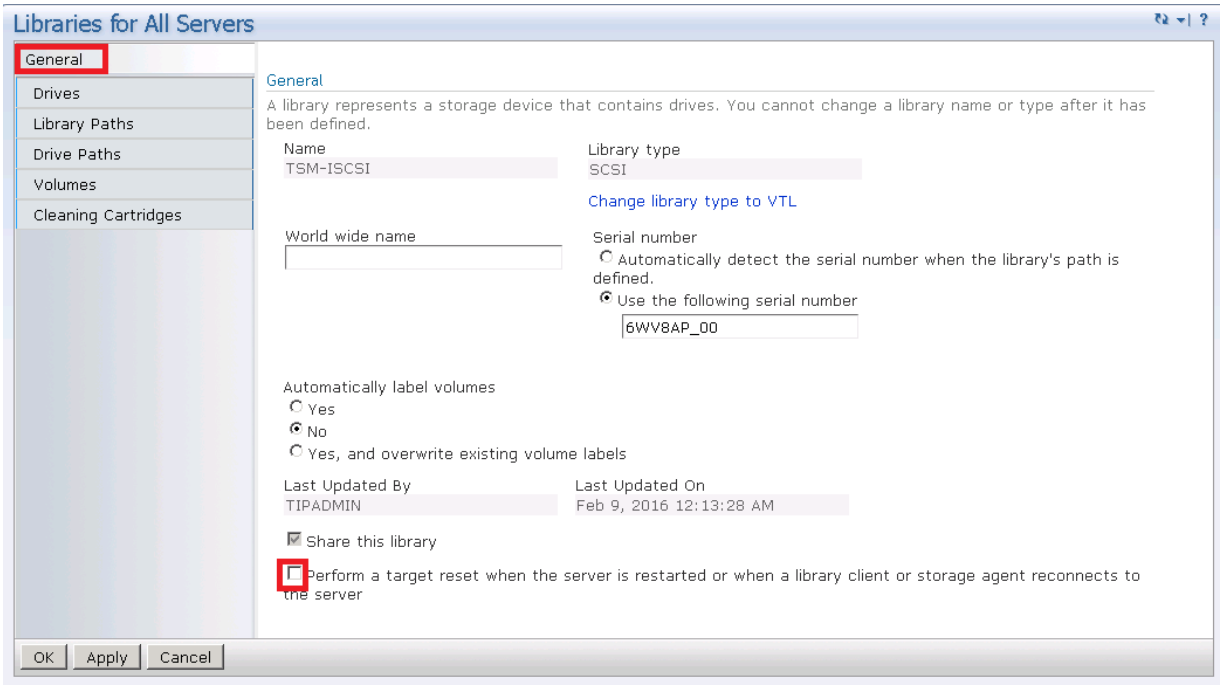
Adding volumes to the library

1 After creating the storage pool, click **Storage Devices** in the left pane.

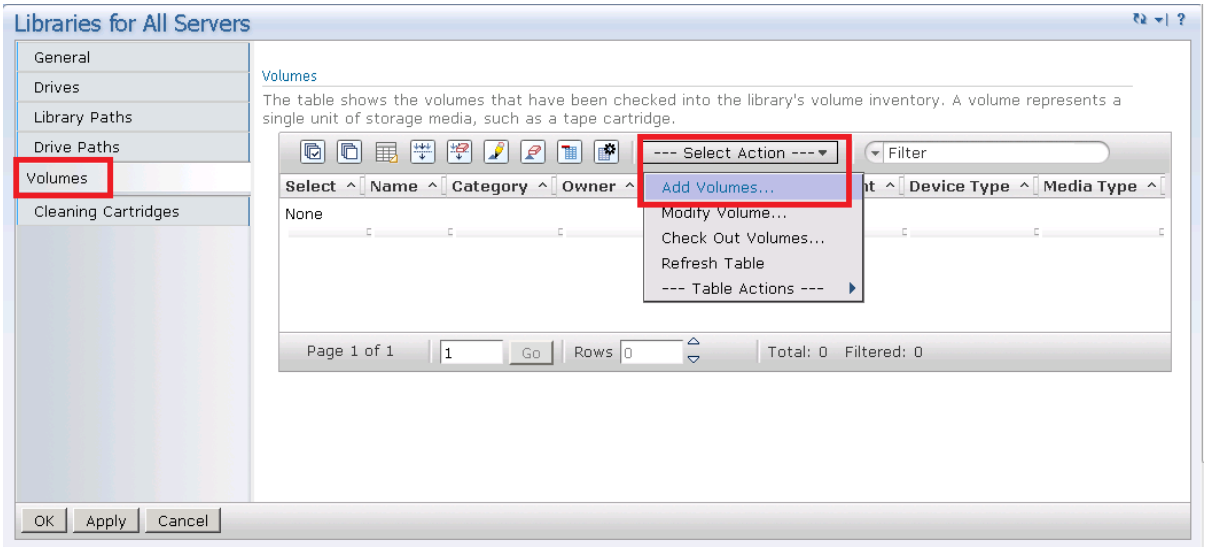
2 Select the library configured earlier.



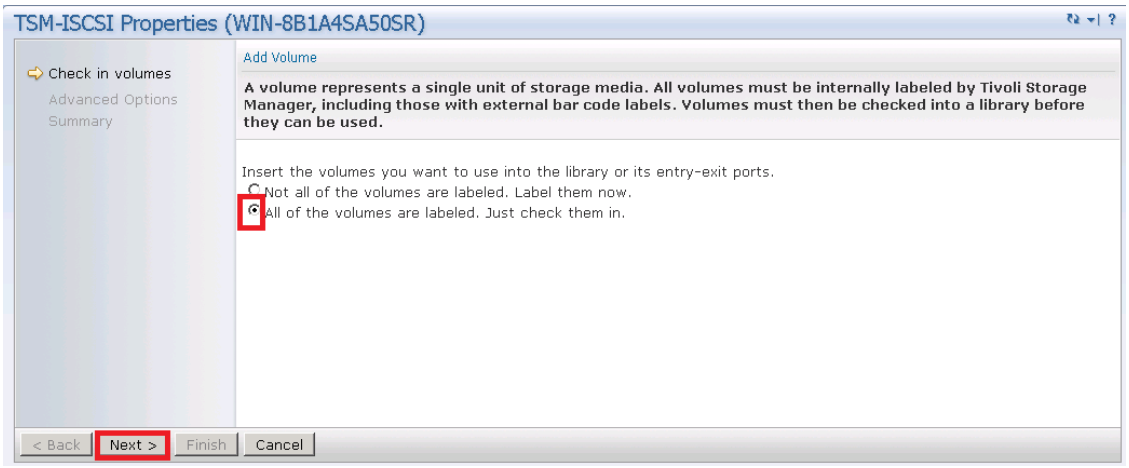
3 Clear the column selection (which was default earlier), disable the target reset option when the server is restarted, and click **OK**.



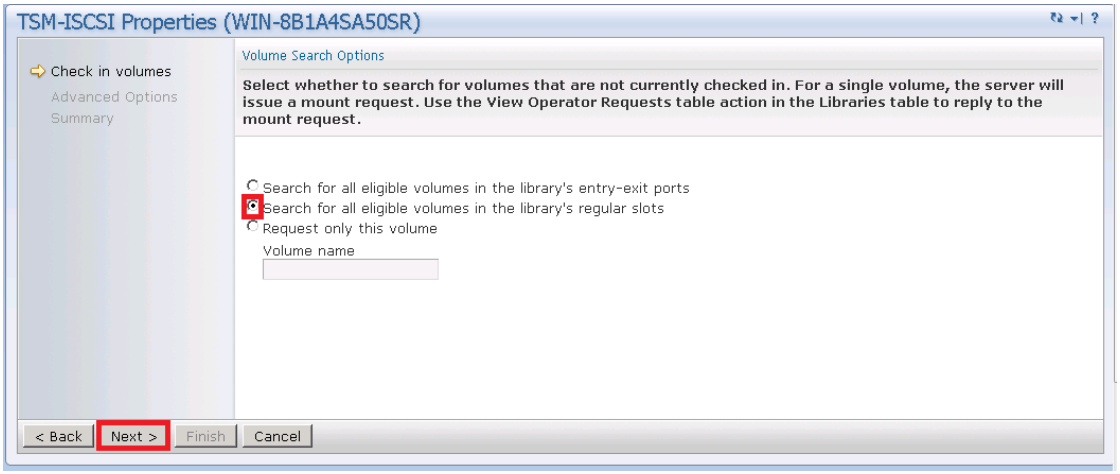
4 In the volumes section, click **Add Volumes** and click **OK**.



5 Enable the option, **All of the volumes are labeled**, and click **Next**.

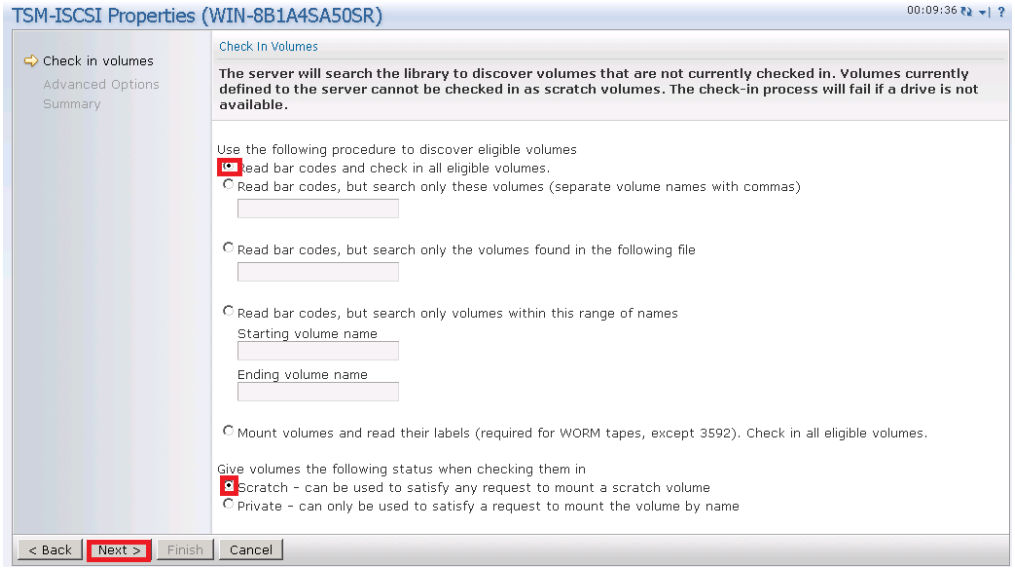


6 Enable the option, **Search for all eligible volumes in the library's regular slots**, and click **Next**.

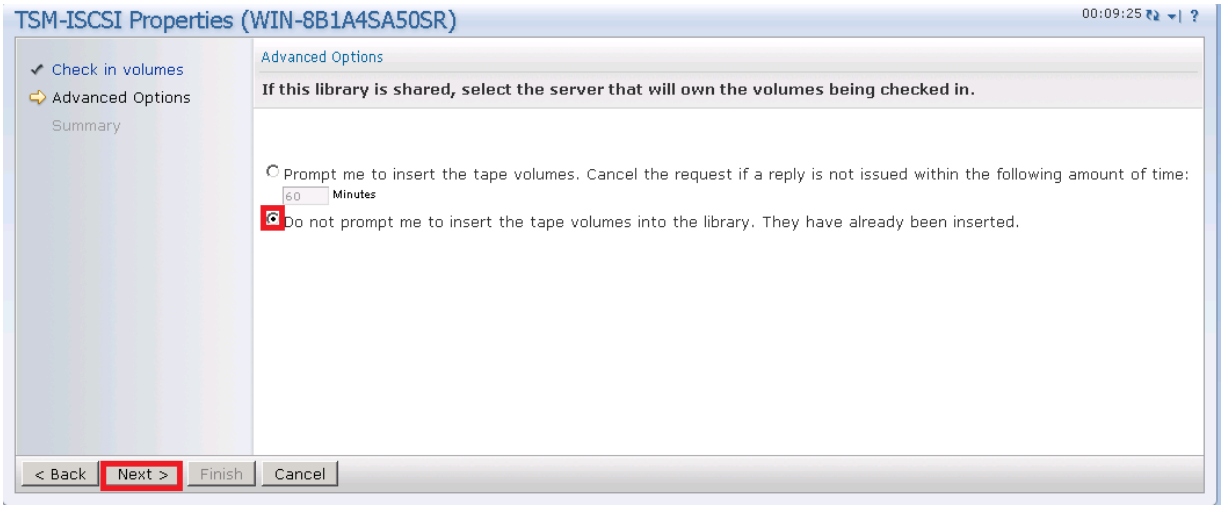


7 On the Check in Volumes page, in the section Discover Eligible Volumes, select the option, **Read bar codes and check in all eligible volumes**.

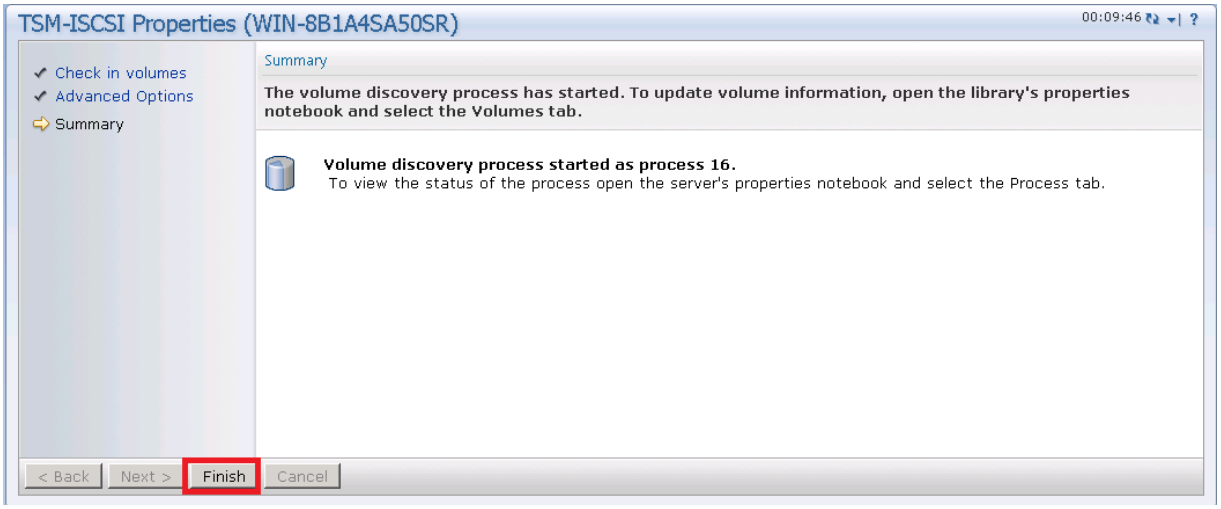
8 Select the **Scratch** option and click **Next**.



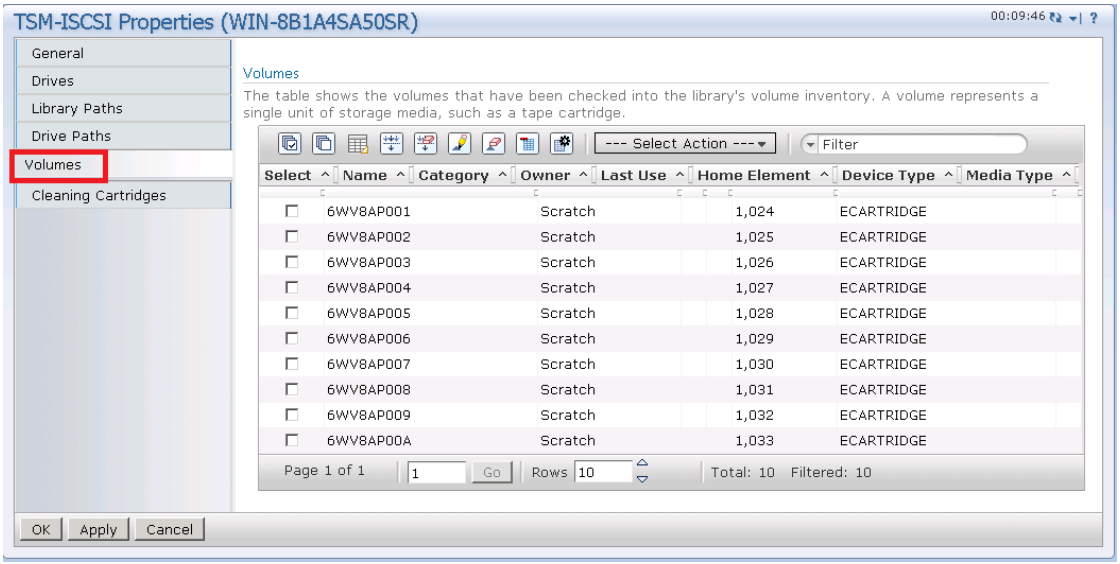
9 For Advanced Options, select the option, **Do not prompt me to insert the tape volumes into the library**, and click **Next**.



10 Click **Finish**.

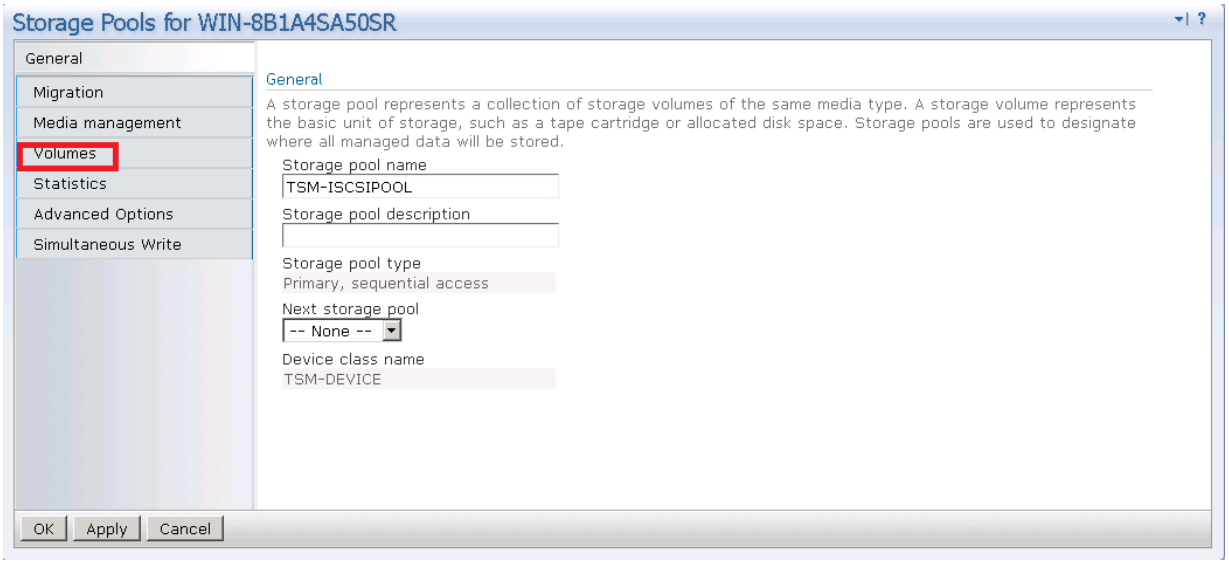


11 Check that all the volumes are created.

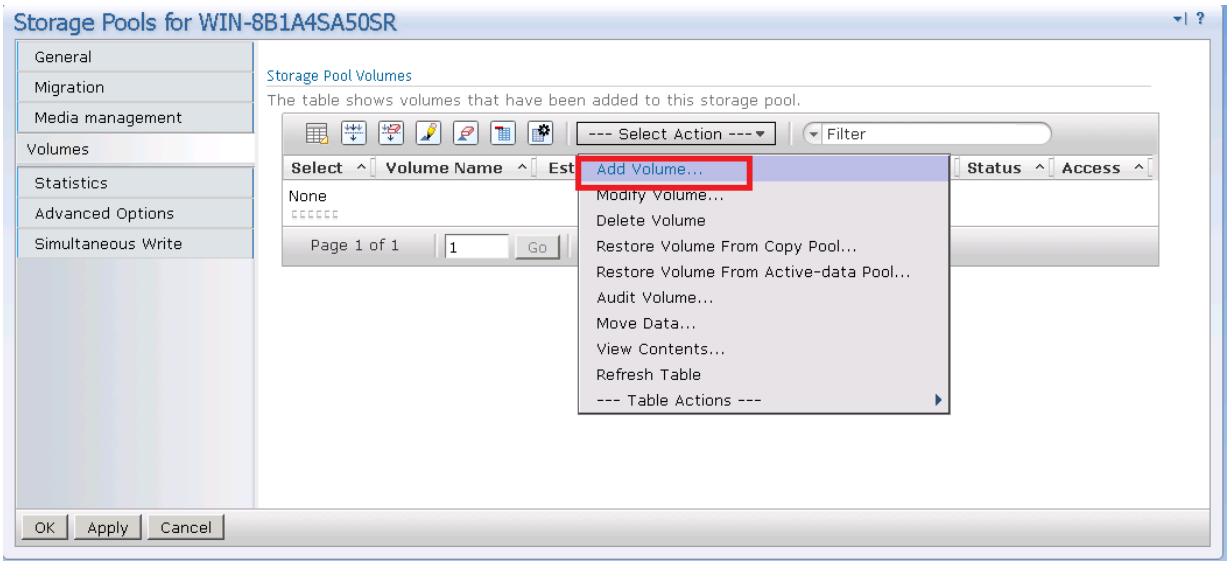


Adding volumes to the storage pool

1 Go to the **STORAGE POOL** section, which was created earlier for the iSCSI target, and click **Volumes**.

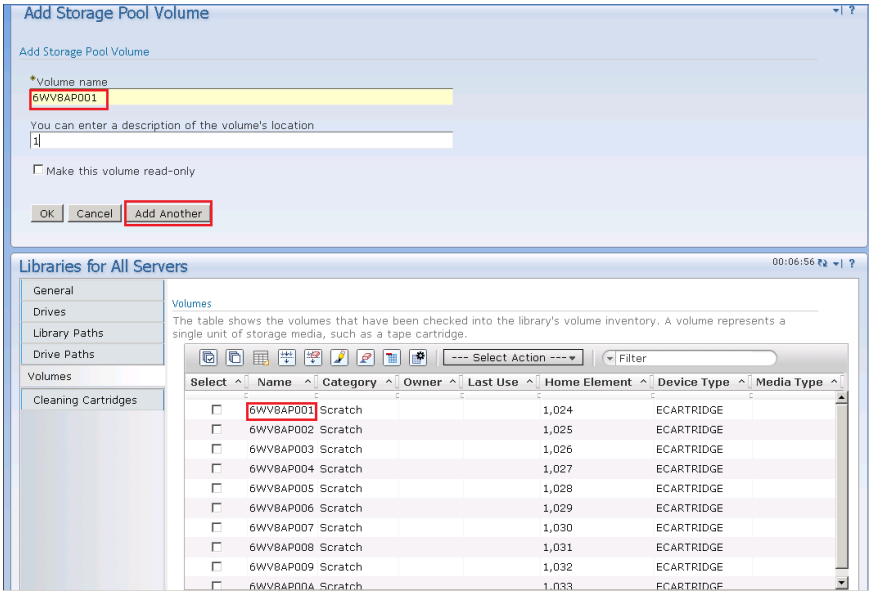


2 In the Volumes section, click on **Add Volume**.

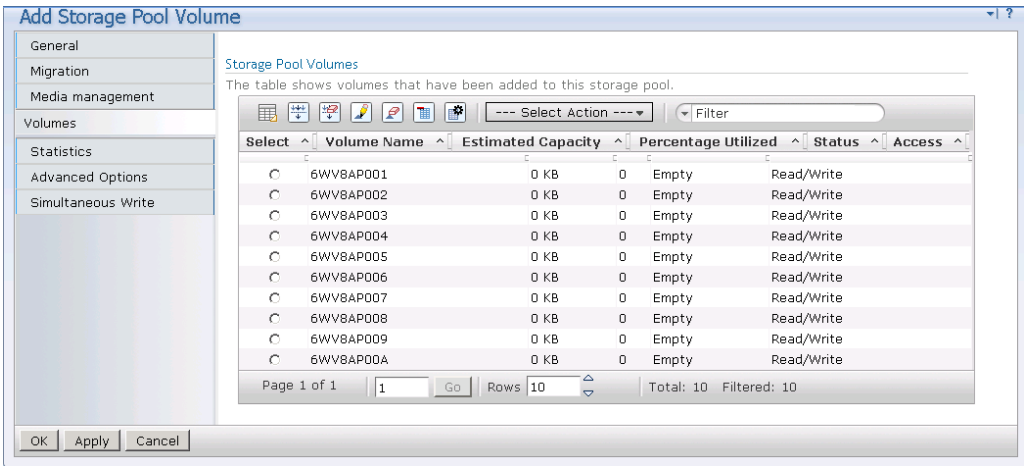


3 Provide the details of the volumes one by one in the volumes name field.

NOTE: Provide exactly the same volume name as present in the LIBRARY into volume name for the storage pool.



4 Verify that all of the storage pool volumes are configured.



Creating the policy domain for iSCSI VTL

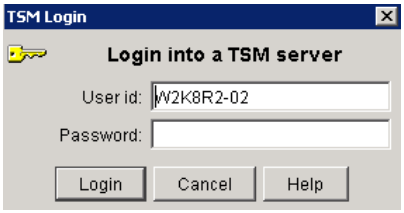
Follow the steps as described in the preceding Policy Domain creation section of this document.

Creating the client node for iSCSI VTL

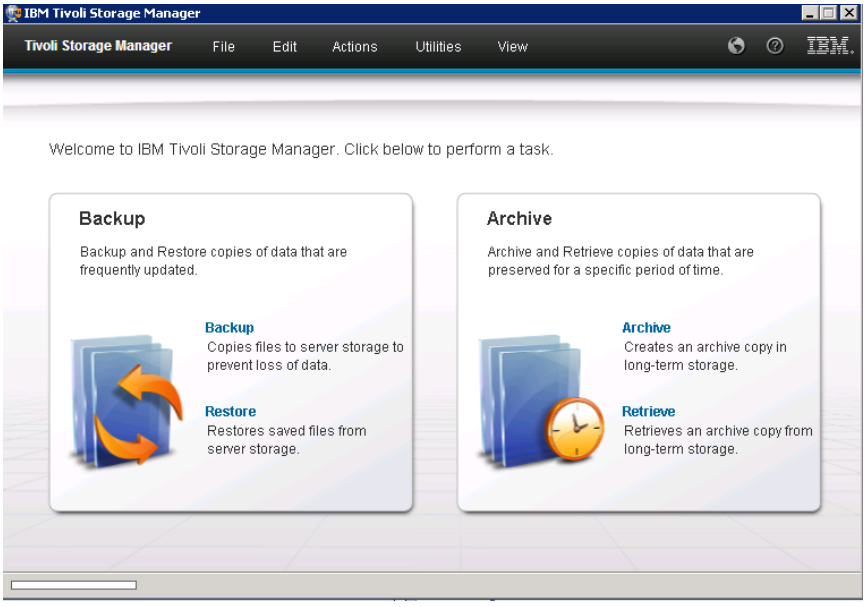
Follow the steps as described in the preceding Client Node creation section of this document.

Using the backup and archive GUI

1 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 is 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 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 of this document for additional best practices.

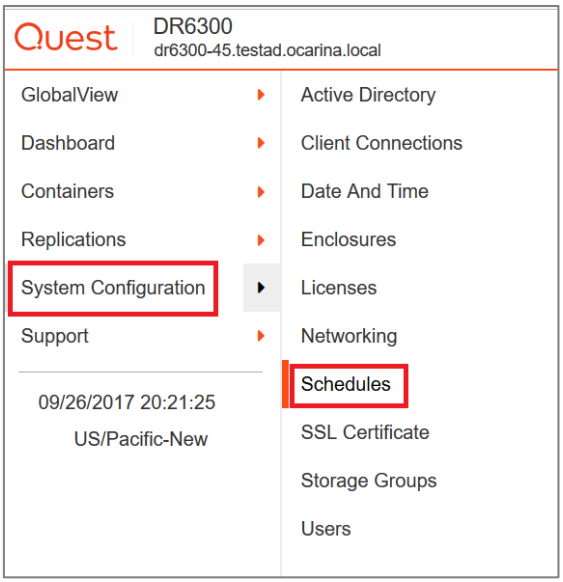
Setting up the DR Series system cleaner

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.

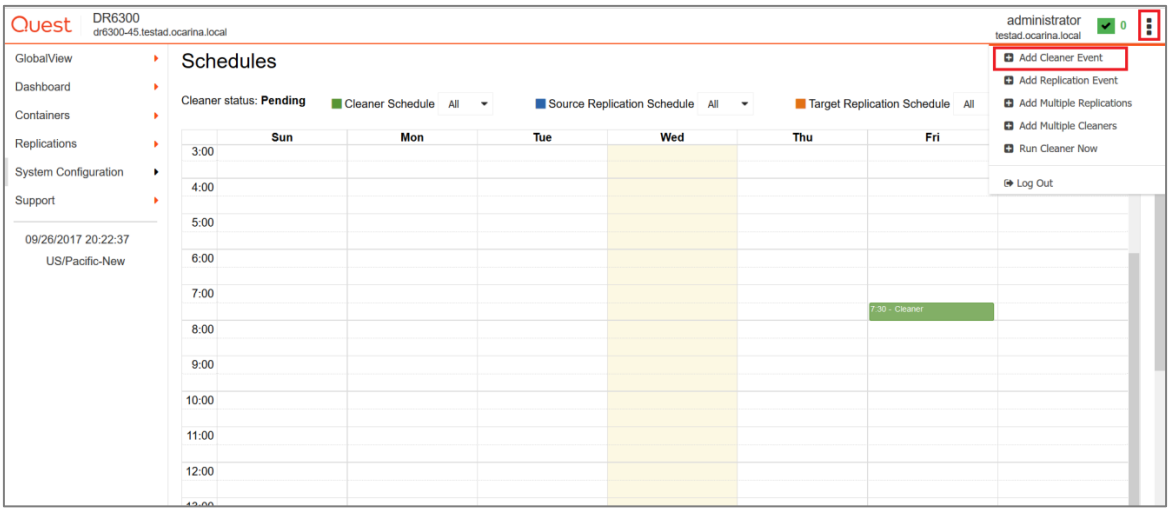
The system cleaner runs during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner to force it to run during a scheduled time.

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. Follow these steps to add a cleaner event on the DR Series system.

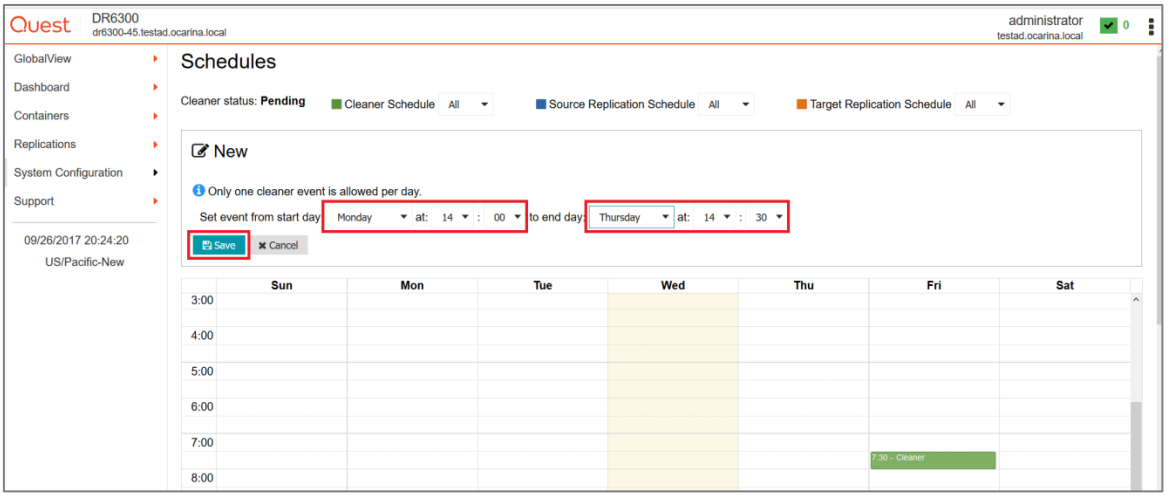
1 On DR series GUI select **System Configuration** then click **Schedules**



2 On the **Action Menu** in the upper right corner of the page, select **Add Cleaner Event**.



3 Enter the day, start time, and end time for the cleaner event, and then click **Save**.

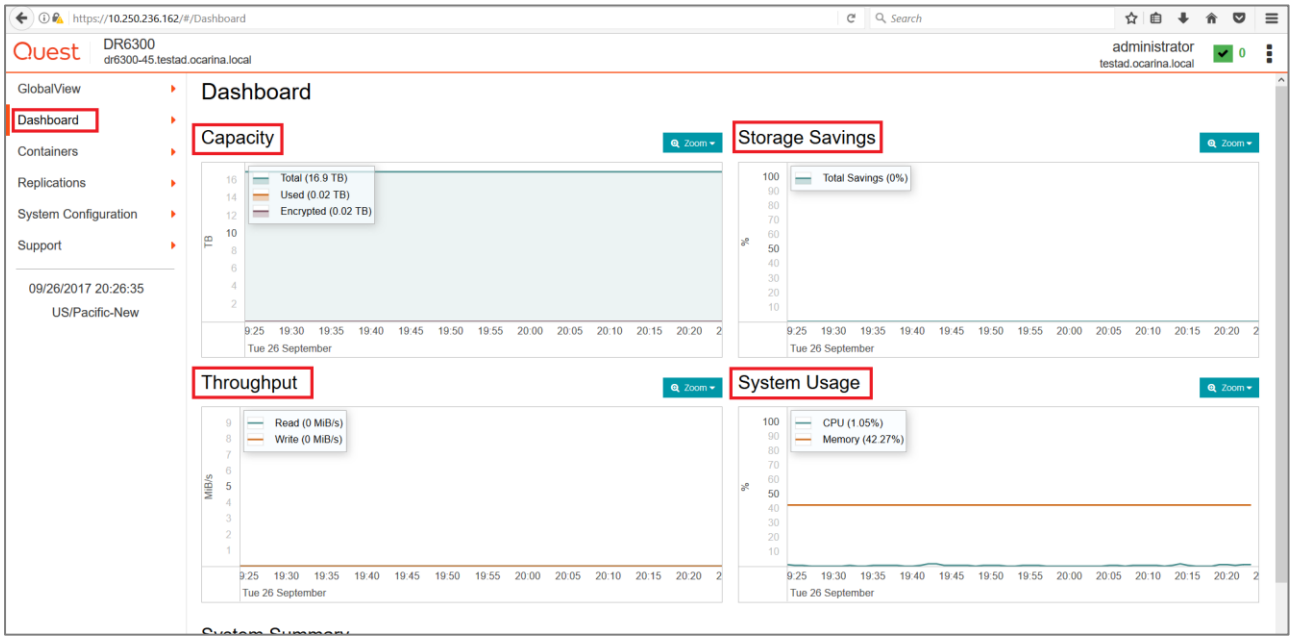


6

Monitoring deduplication, compression, and performance

After backup jobs have completed, the DR Series stracks capacity, storage savings and throughput on the DR Series system GUI 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 complete, 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.

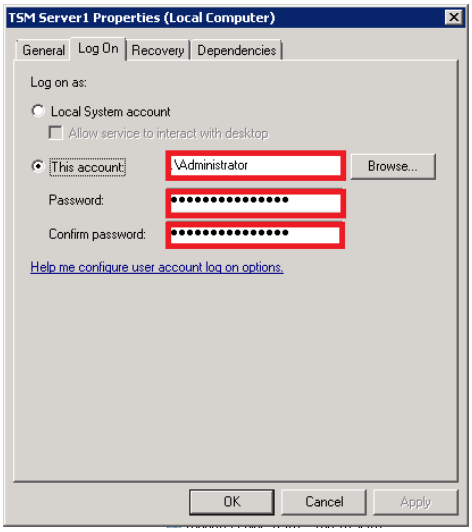
There are two methods for allowing the Tivoli Storage Manager service account to authenticate to a DR Series system.

- 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@dr6300-45 > authenticate --set --user administrator
Enter new password for CIFS user administrator:
Re-enter new password for CIFS user administrator:
Changed administrator's password.
administrator@dr6300-45 >
administrator@dr6300-45 >
```

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

Deduplication and compression

The DR Series system has inline deduplication and Compression built-in and does not require any additional deduplication/compression 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 and then compress the data blocks.

Enabling deduplication/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 deduplication/compression is not done before the data stream is sent to the DR Series system.

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.

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.

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 along 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, need to define library manually in the TSM server as follows.

Please see the following link for more details:

http://publib.boulder.ibm.com/tividd/td/ITSML/GC23-4692-02/en_US/HTML/anrlqs52254.htm

To configure the Tivoli Storage Manager 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 Tivoli Storage Manager device driver package (TIVsm-tsmscsi-x.x.x-x) is installed for your corresponding architecture.

   Get the required driver software from IBM fix central site - https://www-945.ibm.com/support/fixcentral/

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 tsmscsi script from the device driver installation directory.

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

Then all the devices will be listed in following location –

TSM drives	/dev/tsmscsi/mt#
IBM drives	/dev/IBMtape#
TSM Library	/dev/tsmscsi/lb#

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

```
chmod 777 /dev/tsmscsi/*
chown tsminst1:tsmsrvrs /dev/tsmscsi/*
chmod 777 /dev/IBM*
chown tsminst1:tsmsrvrs /dev/IBM*
```

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