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

Dell Engineering
May 2016
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2014</td>
<td>Initial release</td>
</tr>
<tr>
<td>August 2014</td>
<td>Added screenshots where new functionality is introduced in 2014</td>
</tr>
<tr>
<td>April 2015</td>
<td>Updated for v3.2 release</td>
</tr>
<tr>
<td>June 2015</td>
<td>Updated the cleaner recommendations</td>
</tr>
<tr>
<td>May 2016</td>
<td>Updated with ISCSI VTL support and instructions</td>
</tr>
</tbody>
</table>

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.


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](image)

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.).

![Login](image)

**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.
Enter your Active Directory credentials.
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.

![Diagram of Containers interface]

2. Enter a Container Name, and click Next.

![Diagram of Container Name input]

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

![Diagram of Select Access Protocols]

---

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

8
4. Select to Enable Access Protocols (NFS or CIFS) as appropriate and select the Marker type as Auto. Click Next.

5. Configure access by doing one of the following:
   - For NFS, select the preferred client access credentials, and click Next.
   - For CIFS, select the preferred client access credentials, and click Next.
6. Check the configuration summary, and click **Create a New Container**.

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.

2. Enter a container name, select the **VTL** option, and then click **Next**.
3. Select the required tape size, the access protocol as **iSCSI**, and the marker type. Also, enter the initiator details as appropriate. Click **Next**.

4. Click **Create a New Container**.
5. Confirm that the container is successfully added on the Containers page.
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 Manager Administration Center.
2. Click **Storage Devices > View Storage Classes**.

![Image of Tivoli Storage Manager Administration Center]

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

![Image of Device Classes creation in Tivoli Storage Manager]

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

5. 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.

6. Click **Finish**.
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.)

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

### Creating a policy domain for the backup job

1. Click **Policy Domains** > **View Policy Domains**.
2. Click **Create a Policy Domain**.

   **R310-SYS-121_TSM SRV Policy Domains**
   Policy domains help you to apply consistent rules for data management sets, client node schedules, and management classes.

   ![Policy Domain Creation Interface]

   - **Select**: 
     - C
   - **Domain Name**: 
     - R310-SYS-121
   - **Description**: 
     - Installed
   - **Data store**: 
     - Data store

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.

6. Select **Yes** to assign this policy domain to clients, and click **Next**.
7. Select **View all client nodes** to display the set of clients to move to the DR Series system, and click **Next**.

![Create Policy Domain](image)

**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**.

![Create Policy Domain](image)
9. Click **Finish**.

### 2.4 Creating client node and backup sets

1. Open the client nodes 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.
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@ge!iscsi

   **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:
      ```bash
      node.session.auth.authmethod = CHAP
      ```
   b. Modify the following lines:
      ```bash
      # 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:
   ```bash
   iscsiadm -m discovery -t st -p <IP or IQN of DR>
   ```
   For example:
   ```bash
   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:
   ```bash
   iscsiadm -m node --portal <IP or IQN of DR:PORT> --login
   ```
   For example:
   ```bash
   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:
   ```bash
   iscsiadm -m session
   ```
   For example:
   ```bash
   ```

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\.
tsmldst.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
```
3.2.6 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/tsmscsi/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**.

![Image of TSM-ISCsi Properties](TSM-ISCsi.png)

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

![Image of TSM-ISCsi Properties](TSM-ISCsi.png)
8. For Advanced Options, select the option, **Do not prompt me to insert the tape volumes into the library.** Click **Next**.

9. 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

![Add Storage Pool Volume](image)

<table>
<thead>
<tr>
<th>Select</th>
<th>Volume Name</th>
<th>Estimated Capacity</th>
<th>Percentage Utilized</th>
<th>Status</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6WV9AP001</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP002</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP003</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP004</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP005</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP006</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP007</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP008</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP009</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
<tr>
<td></td>
<td>6WV9AP010</td>
<td>0 KB</td>
<td>0</td>
<td>Empty</td>
<td>Read/Write</td>
</tr>
</tbody>
</table>

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.
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.
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.
Configuring CIFS authentication

This appendix describes the steps for syncing 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/St0r@ge!
  - Run the following command: authenticate --set --user administrator

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

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

When an authentication method has been selected, set the 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 reclamation jobs should be scheduled to happen at different times.
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 “tsmldst,” 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 –

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-tsmiscsi-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 tsmscsi script from the device driver installation directory.

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

Then all the devices will be listed in following locations:

   TSM drives       /dev/tsmscsi/mt#
   IBM drives       /dev/IBMtape#
   TSM Library      /dev/tsmscsi/lb#
6. 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 created for TSM installation.