



Setting Up the Dell™ DR Series System as a VTL Backup Target on Microsoft® Data Protection Manager

Dell Engineering
January 2016

Revisions

Date	Description
February 2015	Initial release
April 2015	Updated for current release
January 2016	Updated content related to spanned tapes and driver and registry requirements,

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. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

1	Executive summary	4
2	Installing and configuring the DR Series system	5
3	Creating and configuring iSCSI target containers for Microsoft DPM.....	9
3.1	Creating the iSCSI VTL container	9
3.2	Configuring the Microsoft DPM Server – Windows.....	11
3.3	Installing device drivers for the DR Series system iSCSI VTL.....	14
3.4	Configuring Microsoft DPM registry settings	16
3.4.1	Adjusting BufferQueueSize, ConnectionNoActivityTimeout, and ConnectionNoActivityTimeoutForNonCCJobs registry settings.....	17
3.4.2	Adding the TapeSize parameter.....	18
3.4.3	Adding the Storport key and BusyRetryCount parameter for each tape.....	19
3.4.4	Disabling TUR	21
3.5	Setting up Microsoft DPM to use the newly created iSCSI VTL	23
4	Performing backup and restore by using the DR Series system VTL.....	26
5	Restoring from tape	38
6	Setting up the DR Series system cleaner	44
7	Monitoring deduplication, compression, and performance	45
A	Managing VTL protocol accounts and credentials	46
A.1	Managing iSCSI account details.....	46
A.2	VTL default account summary table.....	47
B	Managing VTL media and space usage.....	48
B.1	General performance guidelines for DMA configuration	48
B.2	VTL space sizing and planning.....	48
B.3	Logical VTL geometry and media sizing.....	49
B.4	Media retention and grouping.....	50
B.5	VTL media count guidelines	50
B.6	Adding VTL media to a VTL container.....	50
B.7	Space reclamation.....	52
B.7.1	General guidelines.....	52
B.7.2	Product specific guidelines.....	52



1 Executive summary

This document provides information about how to set up the Dell DR Series system as a backup target for Microsoft Data Protection Manager (DPM) software (Microsoft DPM 2010 and later). This document is a quick reference guide and does not include all DR Series system deployment best practices. For additional information, see the DR Series system documentation and other data management application best practices whitepapers for your specific DR Series system at:

<http://support.dell.com/manuals>

Note: The DR Series system and DPM screenshots used in this document may vary slightly, depending on the DR Series system firmware version and Microsoft DPM version used.

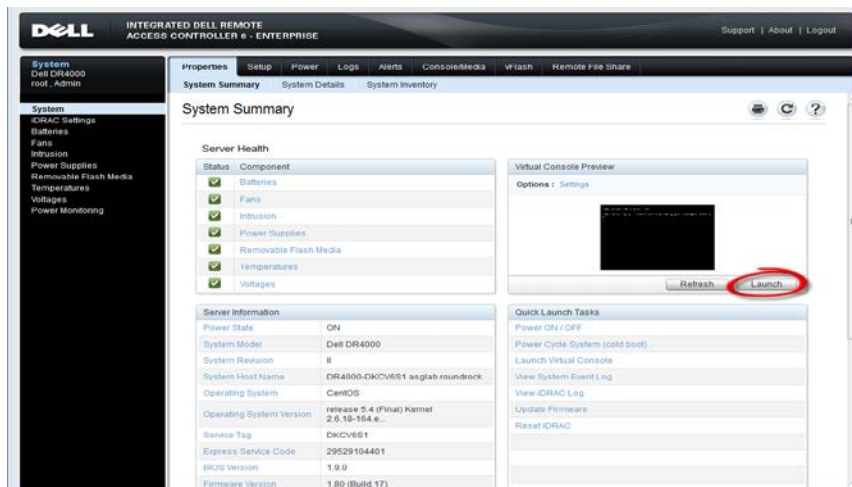


2 Installing and configuring the DR Series system

1. Rack and cable the DR Series system and power it on.
2. Initialize the DR Series system. For more information, in the *Dell DR Series System Administrator Guide*, refer to the following topics: “iDRAC Connection,” “Logging in and Initializing the DR Series System,” and “Accessing iDRAC6/iDRAC7 Using RACADM”.
3. Log on to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use the user name and password of “root/calvin”.



4. Launch the virtual console.



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

```
Ocarina release 1 (EAR-1.00.00) Build: 32858
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password: St0r@ge!
```

6. Set the user-defined networking preferences.

```
Would you like to use DHCP (yes/no) ?
Please enter an IP address:
Please enter a subnet mask:
Please enter a default gateway address:
Please enter a DNS Suffix (example: abc.com):
Please enter primary DNS server IP address:
Would you like to define a secondary DNS server (yes/no) ?
Please enter secondary DNS server IP address:
```

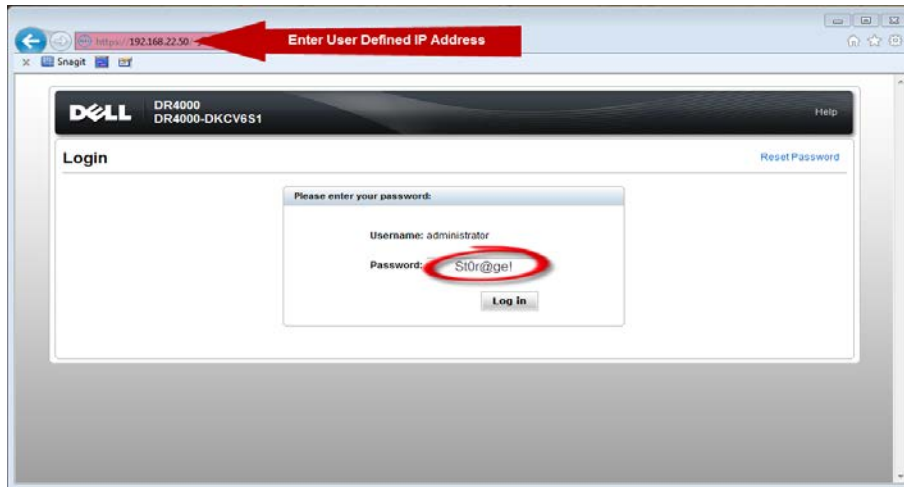
7. View the summary of preferences and confirm that it is correct.

```
=====
                          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) ? _
```



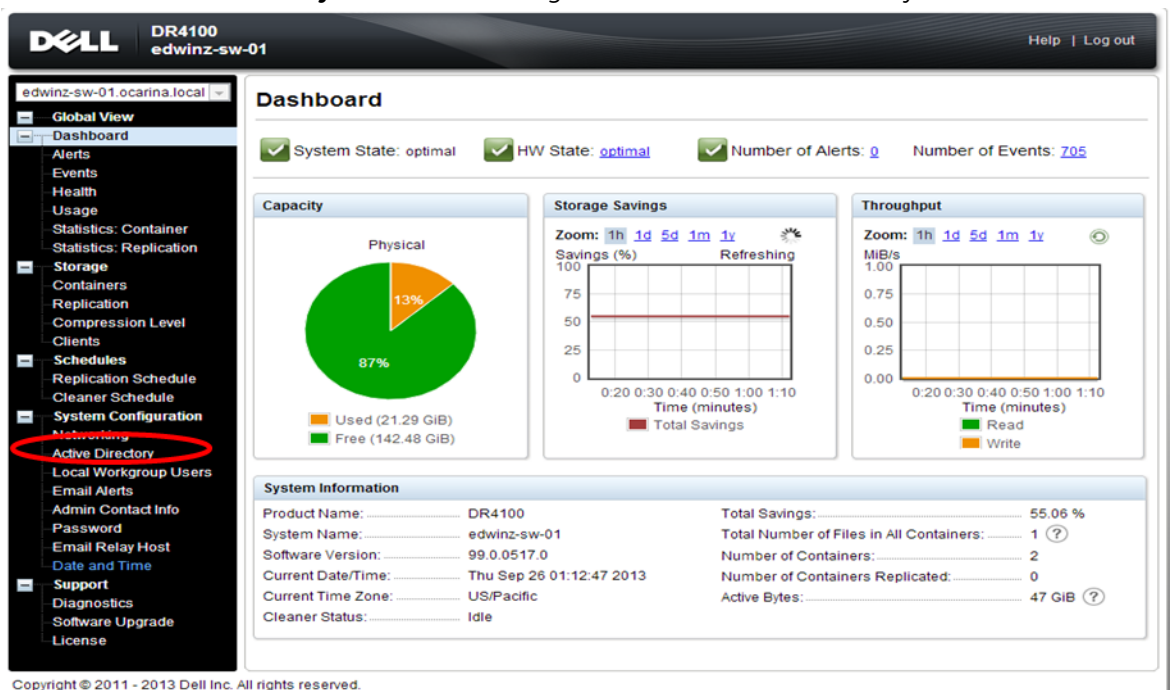
8. Log on to the DR Series system administrator console using the IP address you just provided for the DR Series system, the username **administrator**, and the password **St0r@ge!** (the "0" in the password is the numeral zero).



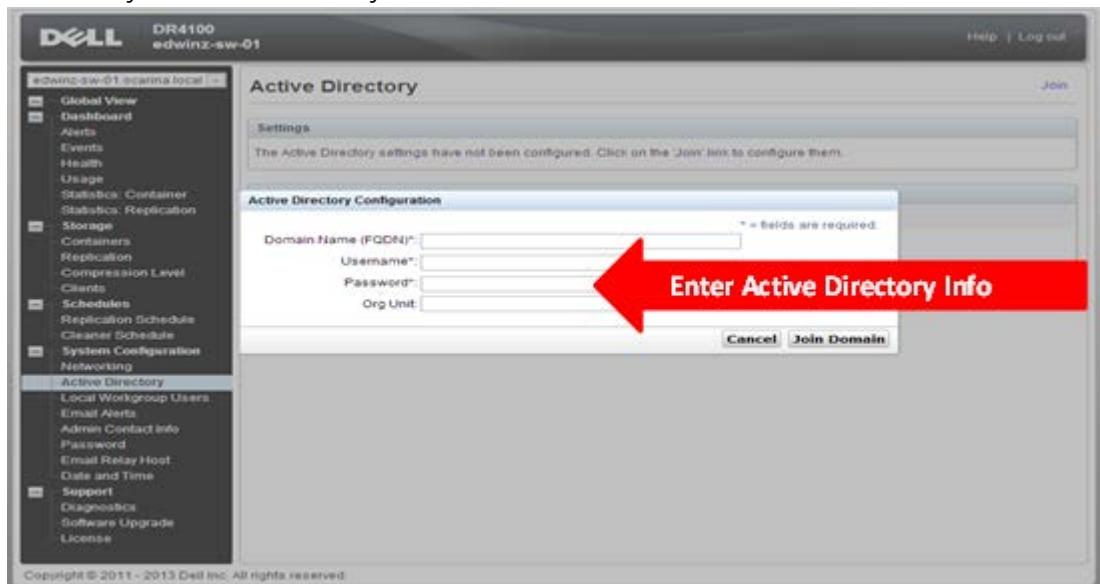
9. Join the DR Series system to Active Directory.

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

- a. Select **Active Directory** from the left navigation area of the DR Series system user interface.



b. Enter your Active Directory credentials.

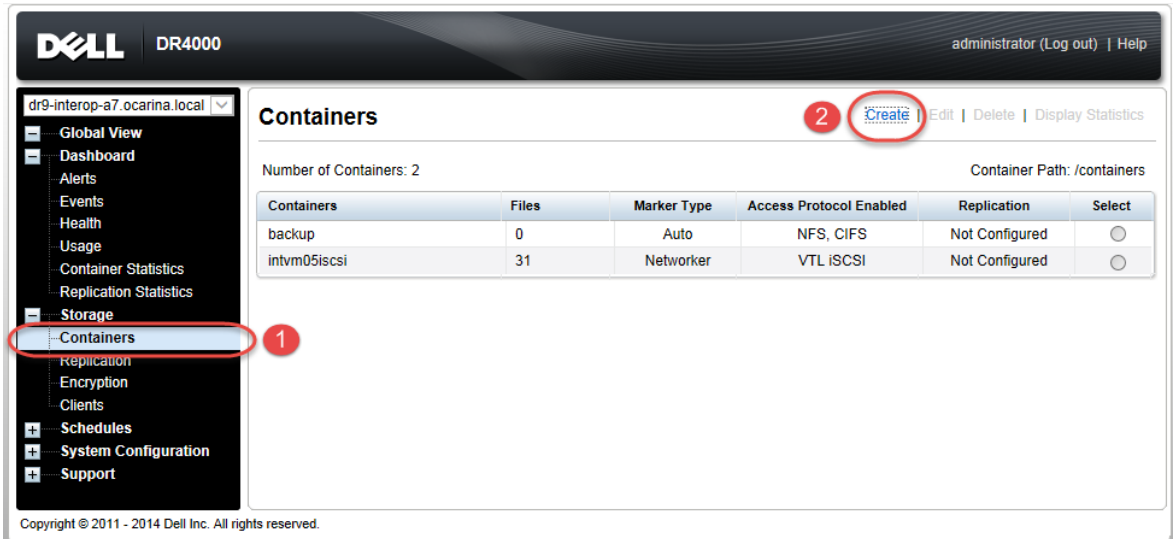


3 Creating and configuring iSCSI target containers for Microsoft DPM

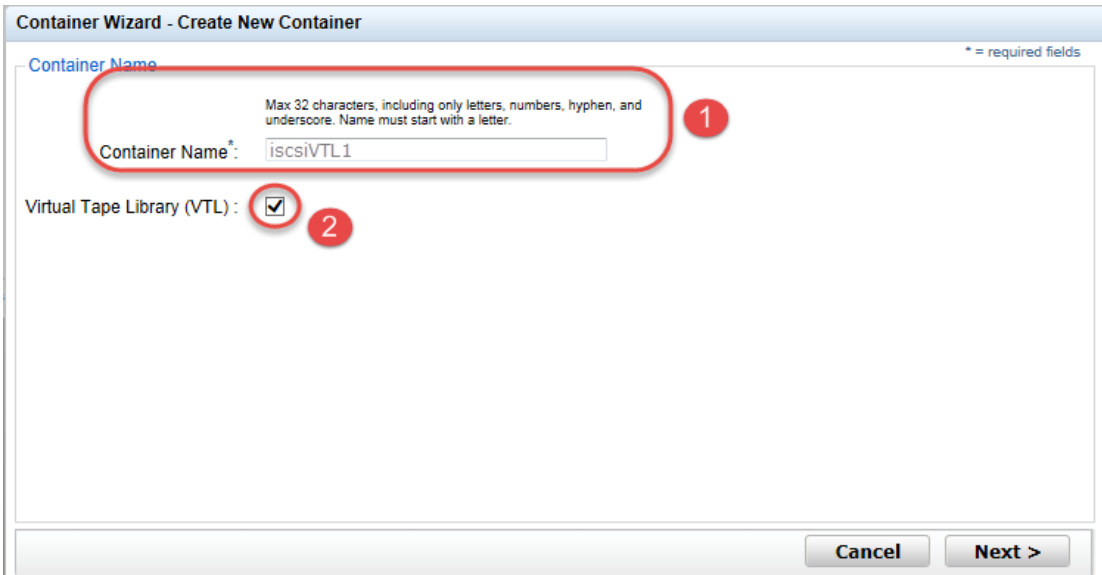
3.1 Creating the iSCSI VTL container

For this procedure, you need to create and export the iSCSI container as described in the following steps.

1. Select **Containers** in the navigation panel on the left navigation area, and then click the **Create** link at the top of the page.



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



- For the Access Protocol, select **iSCSI**, and then specify the Data Management Application **Access Control** by entering the Microsoft DPM server IP Address, IQN, or FQDN. For Microsoft DPM, you also need to specify Marker Type as **Auto**. Click **Next**.

Container Wizard - Create New Container

Configure Virtual Tape Library

Is OEM:

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

Access Protocol: NDMP iSCSI No Access

Access Control (initiator):

Marker Type: Unix Dump Networker BridgeHead
 None Auto Time Navigator

Container Name and Type
iscsi/VTL1
VTL

< Back Cancel Next >

- Click **Create a New Container** to create the VTL container.

Container Wizard - Create New Container

Configuration Summary

Container Name and Type
Container Name: iscsi/VTL1
Connection Type: VTL

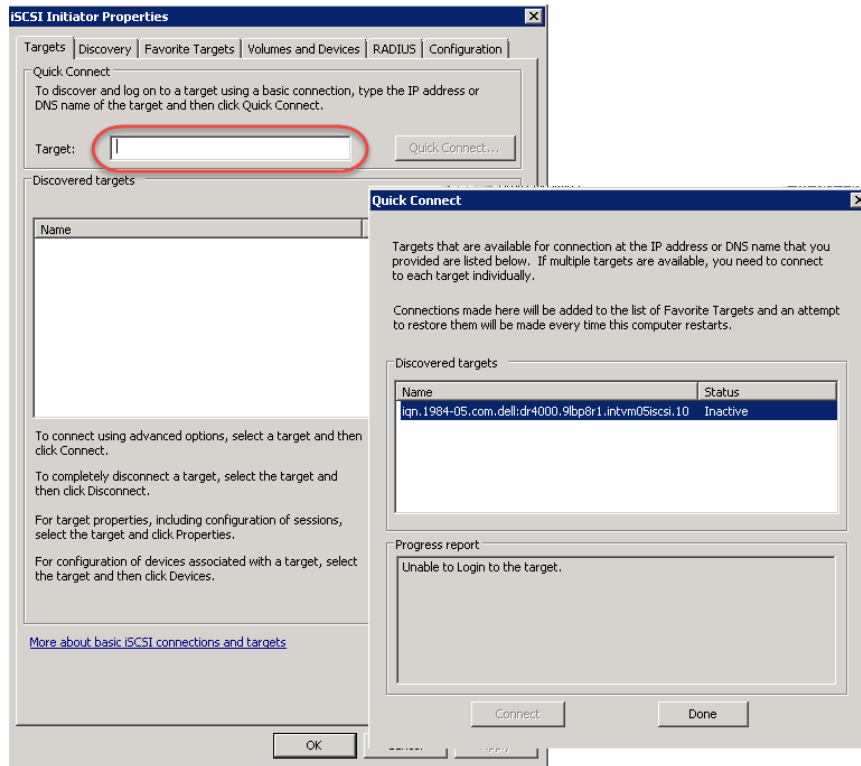
Virtual Tape Library
OEM: no
Tape Size: 10gb
Access Protocol: iSCSI
Access Control: iqn.1991-05.com.microsoft:2k8r2intvm05
Marker Type: Auto

< Back Cancel Create a New Container



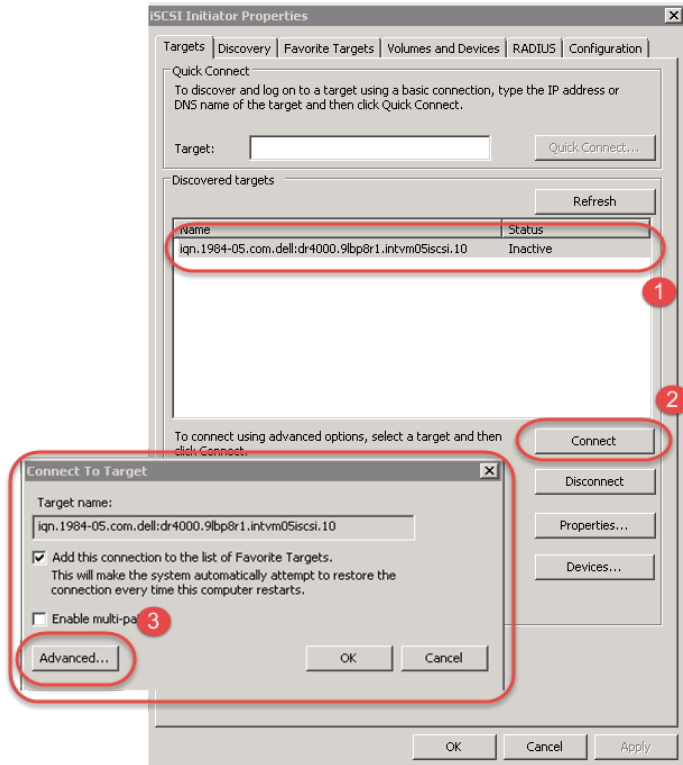
3.2 Configuring the Microsoft DPM Server – Windows

1. Configure the iSCSI Initiator Software for Windows by providing the IP or FQDN of the DR unit in the **Target** field, and then click **Quick Connect**. The Quick Connect dialog box opens that indicates a connection was made but is set inactive as show below.



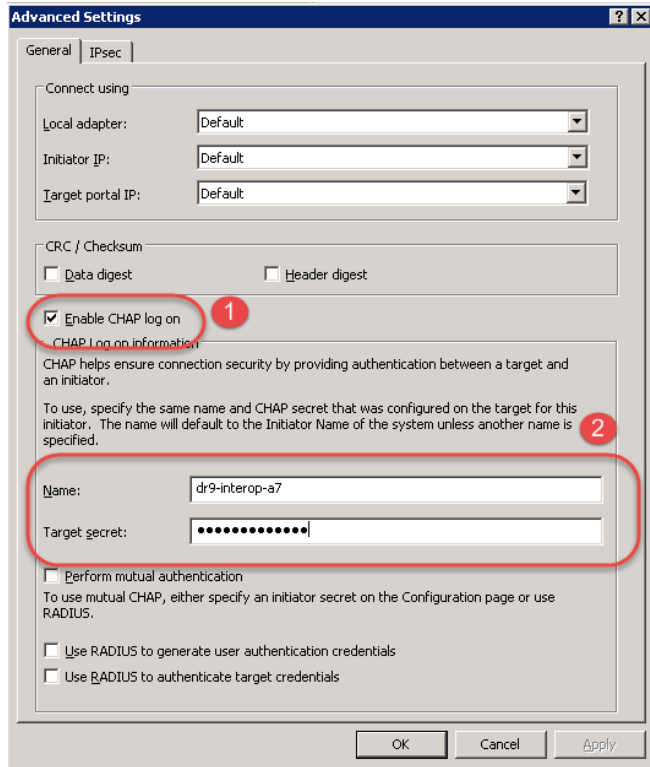
2. Click **Done** to close the dialog box and proceed by selecting the newly discovered target. This target will have an *Inactive Status* as it requires authentication parameters to be provided for iSCSI logon. Select the Target from the list, click the **Connect** button, and then in the **Connect to Target** dialog box, click the **Advanced** button.



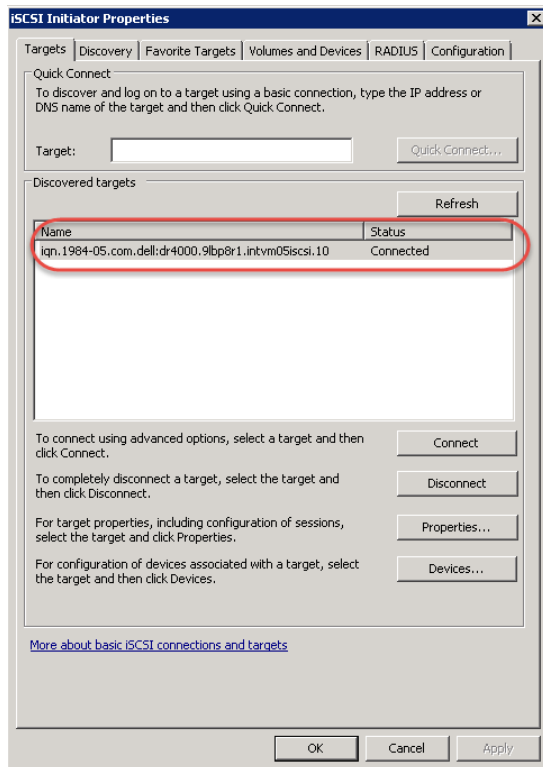


3. In the **Advanced Settings** dialog box, select to **Enable CHAP log on** and type the **User Name** and **Target Secret / Password**. Click **OK**. See Appendix A for more details about accounts and credentials.





The iSCSI target should now show as connected, and the device discovery can now proceed.

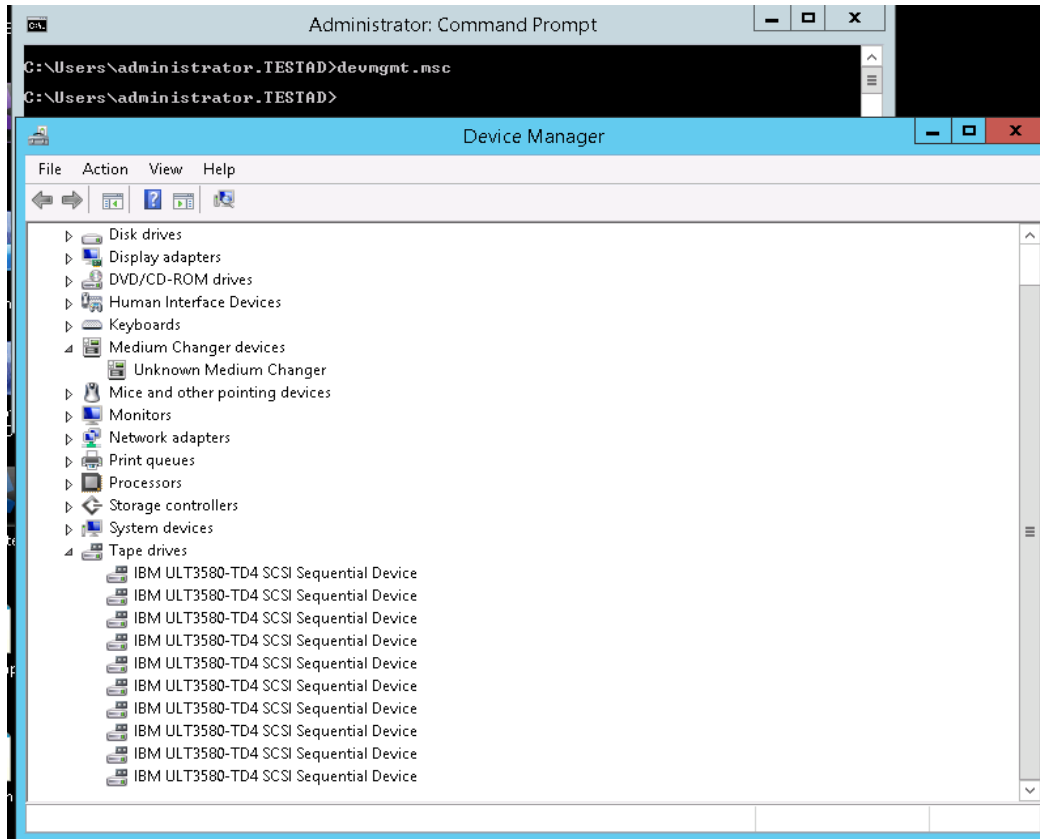


3.3 Installing device drivers for the DR Series system iSCSI VTL

After making an iSCSI connection to the VTL, the next step is to install drivers. For the DR Series system to work properly with Microsoft DPM, you need to install drivers for the medium changer and tape drives.

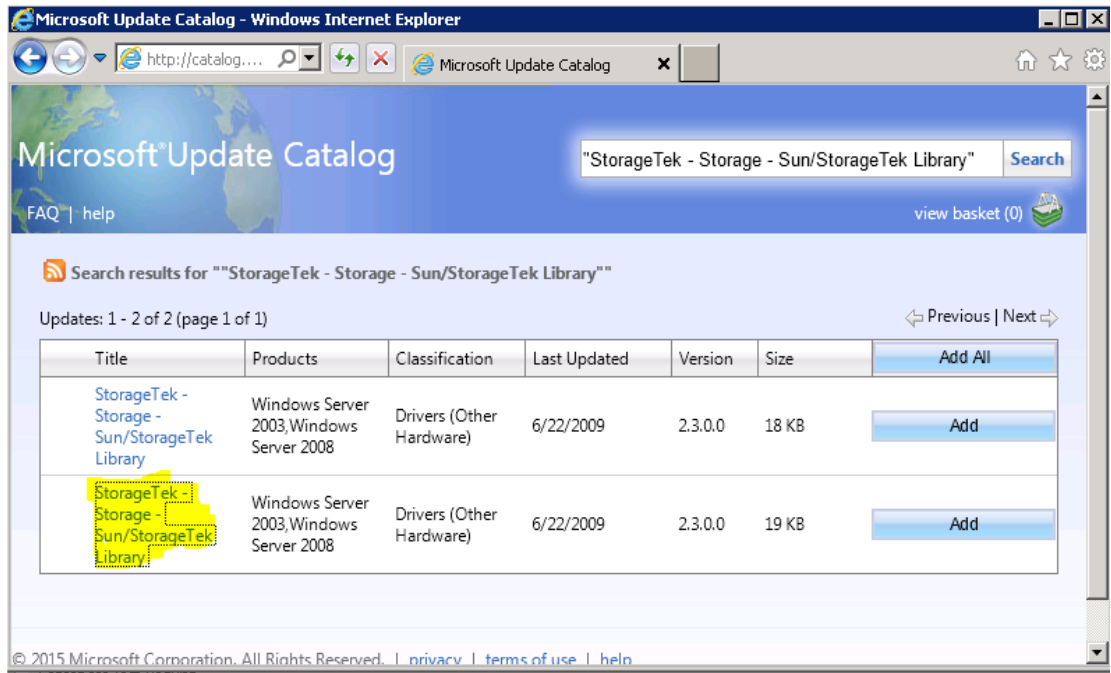
1. From the **cmd** prompt, type the following command to open Device Manager.
devmgmt .msc

The DR Series system iSCSI VTL will be listed in the Device Manager as shown in the following screenshot.

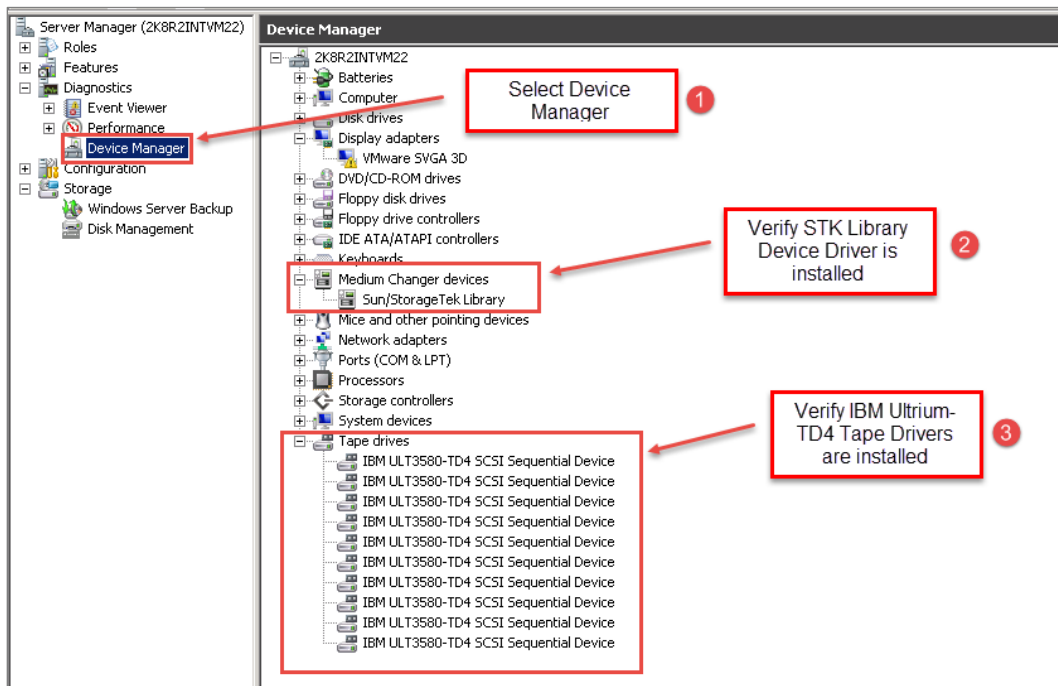


2. To install device drivers for the Medium Changer, you need to get the device drivers at the following link: <http://catalog.update.microsoft.com/v7/site/Home.aspx>. Search for the following: "StorageTek - Storage - Sun/StorageTek Library"





3. Extract the package contents and install the drivers through the Device Manager. (You can refer to Microsoft online help for instructions on installing device drivers.) After installation, the library drivers will appear in the Device Manager, as shown in the following screenshot.



- You need to upgrade the device drivers for the tape drive as well. Use the following drivers, which you can download from IBM as per your operating system at:

http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Tape%2Bdrivers%2Band%2Bsoftware&product=ibm/Storage_Tape/Tape+device+drivers&release=1.0&platform=Windows&function=all

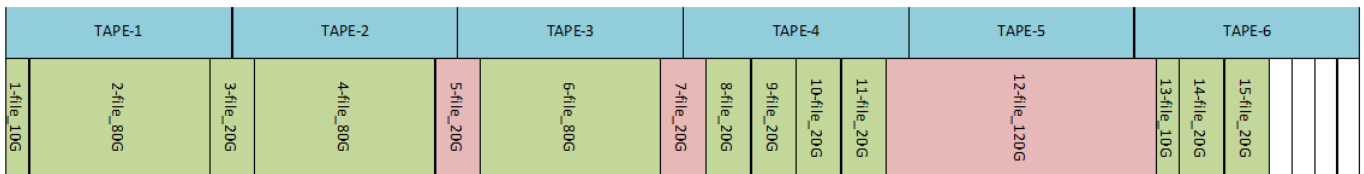
- Windows 2008 R2 SP1 - IBMTape.x64_w08_6250
- Windows 2012 R2 - IBMTape.x64_w12R2_6248_WHQL_Cert

Note: You should Install the drivers in non-exclusive mode. (Double-click the nonexclusive executable.)

- Extract the .cab file, and then use Device Manager to install the driver by pointing to the extracted location.

3.4 Configuring Microsoft DPM registry settings

Note: Restoration of certain files that span across multiple tapes might fail if they are restored as part of a single job. When an attempt is made to restore all of the files in the same job, the recovery of the files (shown in the following graphic in pink) **might still fail**. However, with the registry setting listed below, when these files are individually restored the restores will pass.



For DPM to work properly with the DR Series system, you need to apply the following DPM registry settings. The following subsections describe how to adjust these settings in more detail.

Registry Setting	Value to add/edit
Set BufferQueueSize	1
Set ConnectionNoActivityTimeout and ConnectionNoActivityTimeoutForNonCCJobs	7200
TapeSize	Add this parameter
Storport key	Add for each tape
BusyRetryCount	Add for each tape
TUR	Disable
Service_Name	Add the AutoRun value

Note: A system reboot is required for updated registry settings to take effect.

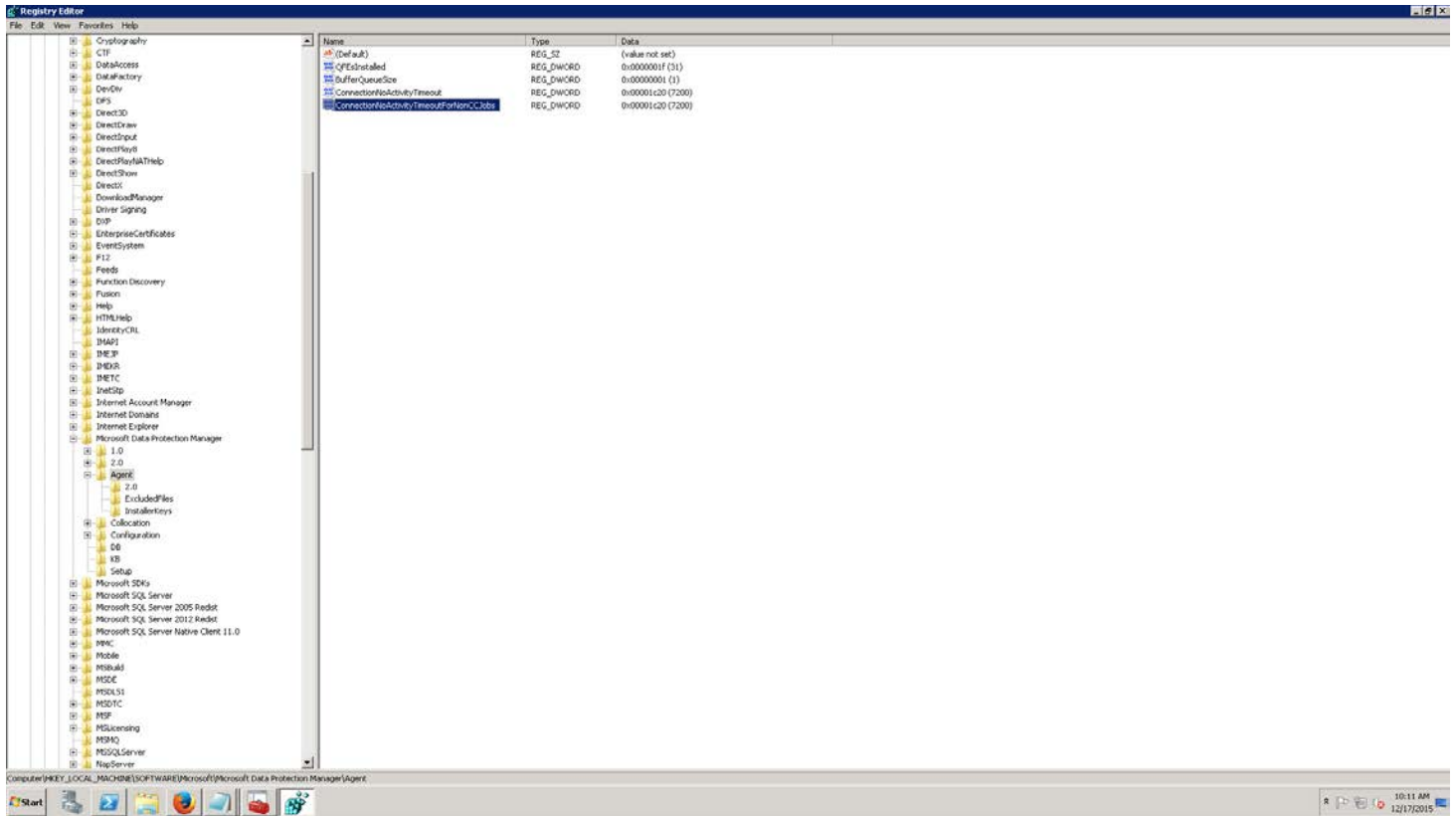


3.4.1 Adjusting BufferQueueSize, ConnectionNoActivityTimeout, and ConnectionNoActivityTimeoutForNonCCJobs registry settings

Follow these steps:

1. Open a Command Prompt and type the following command to open the Registry Editor window.
`regedit`
2. In the Registry Editor window, go to the following path:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent`
3. Right-click and select **New > DWORD (32 bit) Value**, and then enter the value as: **BufferQueueSize**
4. Right-click **BufferQueueSize**, and select **Modify**. Select the Base value as Decimal and then enter **00000001** as the value in the text box. Click **OK**.
5. Right-click and select **New > DWORD (32 bit) Value**, and then enter the value as:
ConnectionNoActivityTimeout
6. Right-click **ConnectionNoActivityTimeout**, and then select **Modify**. Select the Base value as Hexadecimal, and enter **00001c20** as the value in the text box. Click **OK**.
7. Right-click and select **New > DWORD (32 bit) Value**, and then enter the value as:
ConnectionNoActivityTimeoutForNonCCJobs
8. Right-click **ConnectionNoActivityTimeoutForNonCCJobs**, and then select **Modify**. Select the Base value as Hexadecimal, and then enter **00001c20** as the value in the text box. Click **OK**.





3.4.2 Adding the TapeSize parameter

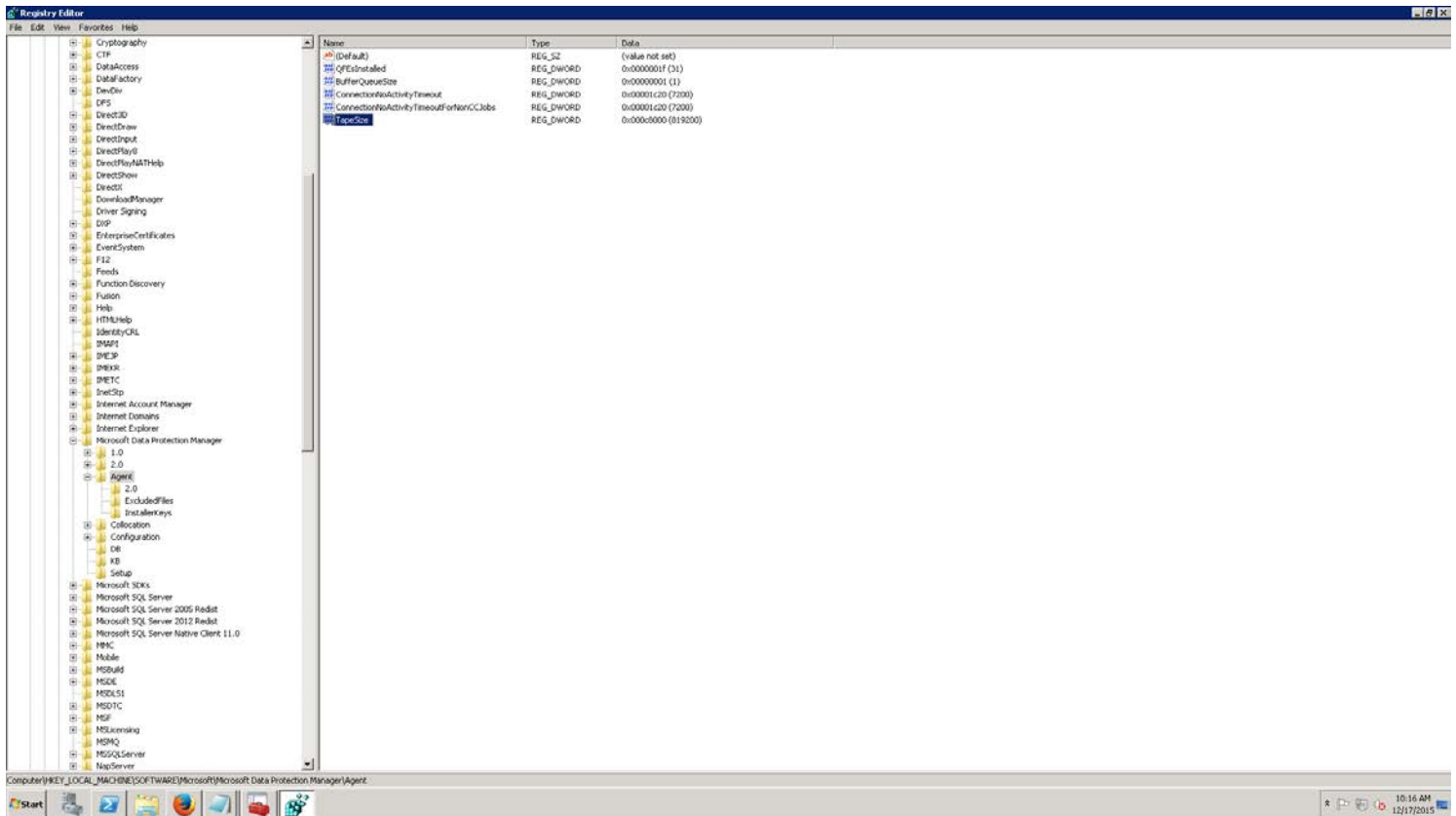
Follow these steps:

1. Open a Command Prompt and then type the following command to open the Registry Editor window:
regedit
2. In the Registry Editor, go to the following path:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent
3. Right-click and select **New > DWORD (32 bit) Value**, and enter the value as: **TapeSize**
4. Right-click **TapeSize**, and then select **Modify**. Select the Base value as Decimal, and enter (TapeSize * 1024) as the value in the text box. Click **OK**.

Note: If you are using 800GB tapes, then the value becomes $800 * 1024 = 819200$.

Note: If the TapeSize parameter is not defined, by default, it is 30GB.





3.4.3 Adding the Storport key and BusyRetryCount parameter for each tape

Follow these steps.

1. To add the Storport key, go to the following path:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI\<DEVICEID>\<INSTANCE>\DeviceParameters

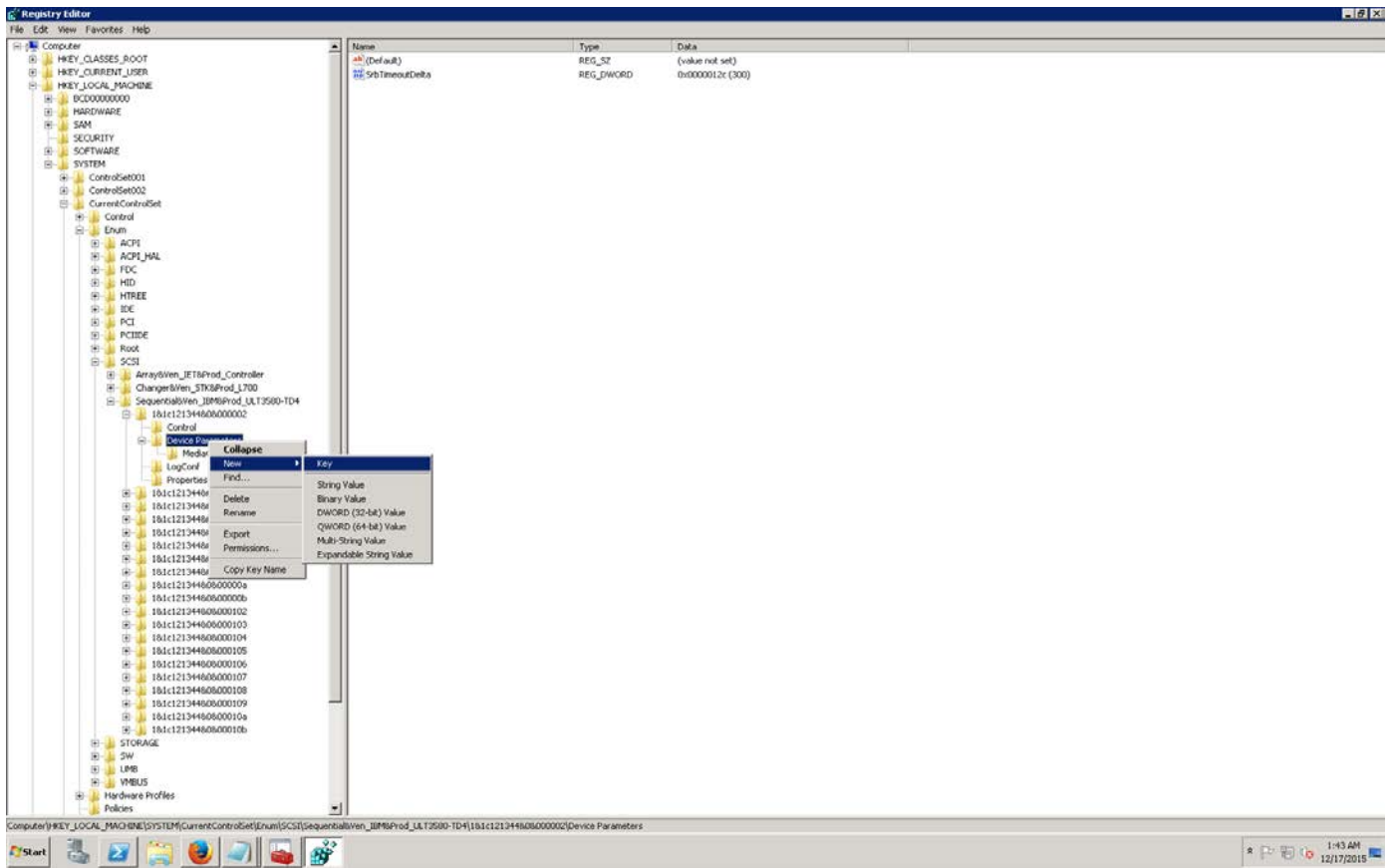
2. To get a list of all the tape devices in your DPM Server to which you need to add the registry key, run the following command from an administrative command prompt.

wmic tapedrive list brief

This command returns a list of tape drives **Scsi\DeviceID\Instance** that you can use to make the above change.

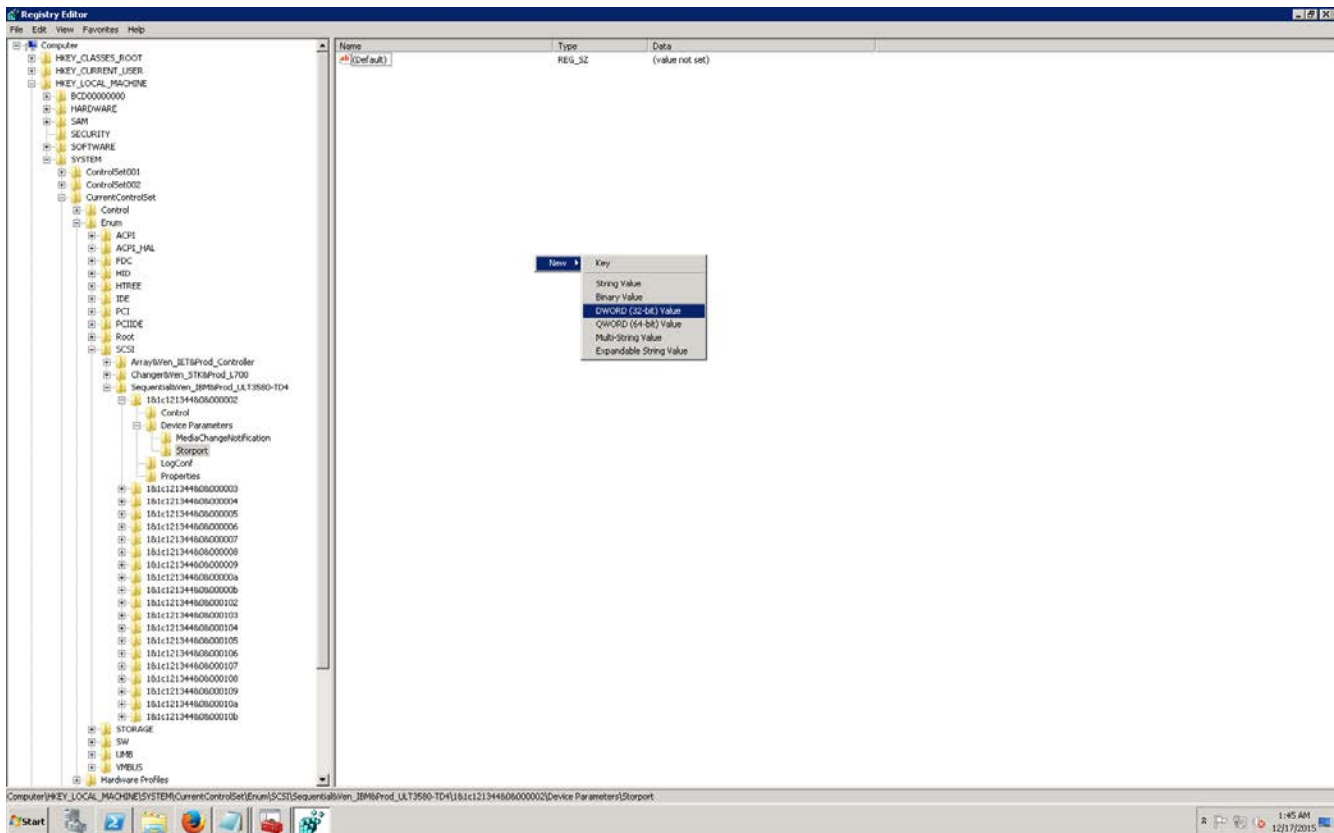
3. Right-click **DeviceParameters**, select **New > Key**, and change NewKey as **Storport**.





4. To add BusyRetryCount value for Storport key, right-click and select **New > DWORD (32 bit) Value**. Enter the value as **BusyRetryCount**
5. Right-click **BusyRetryCount** and select **Modify**. Select the Base value as Decimal, and enter **250** as the value in the text box. Click **OK**.
6. Ensure the Storport and BusyRetryCount settings are configured for all tape drives



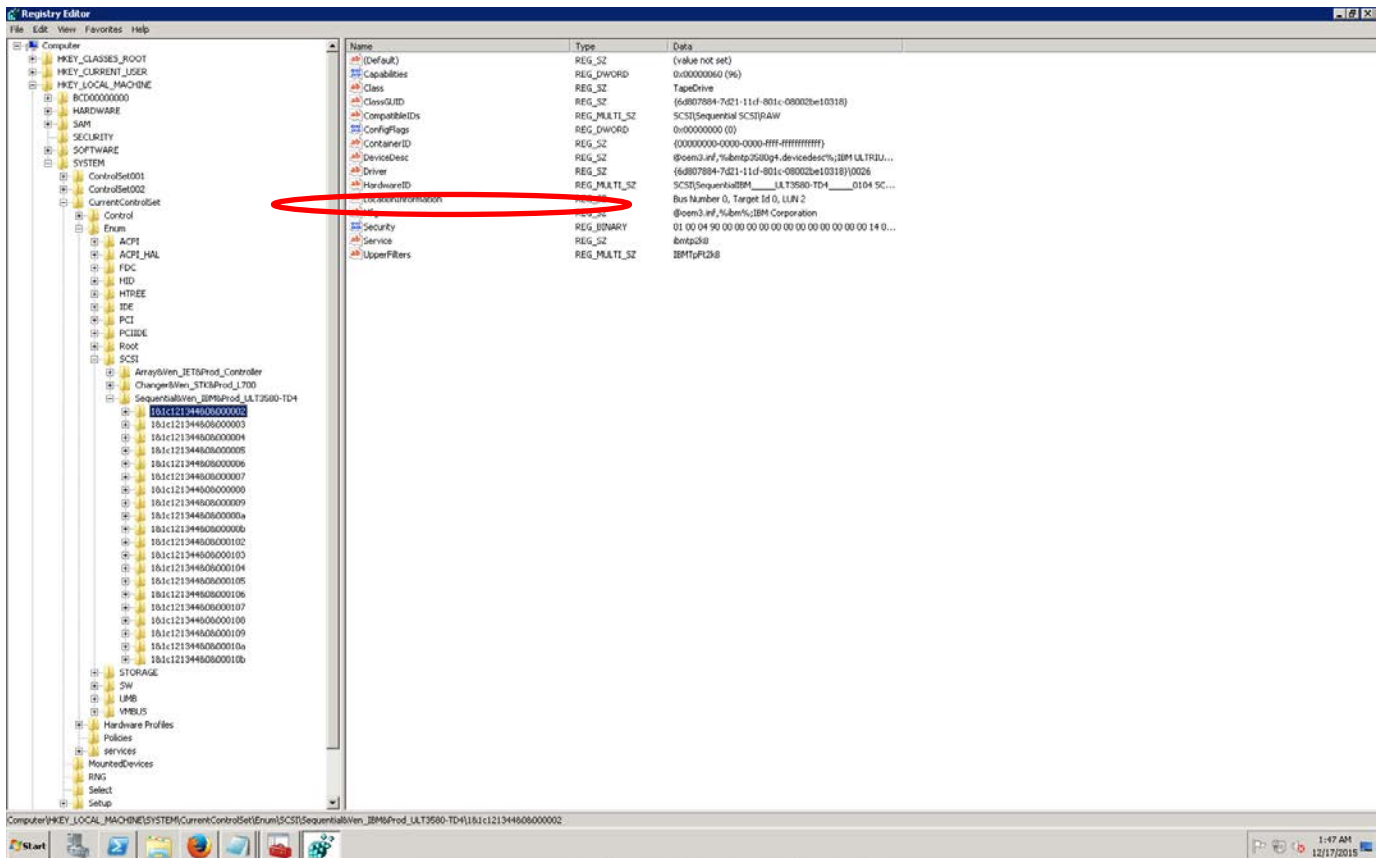


3.4.4 Disabling TUR

Follow these steps.

1. To disable TUR, you need to find the service name used by the tapes. To find the service name, go to the following path:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI\<DEVICEID>\<INSTANCE>



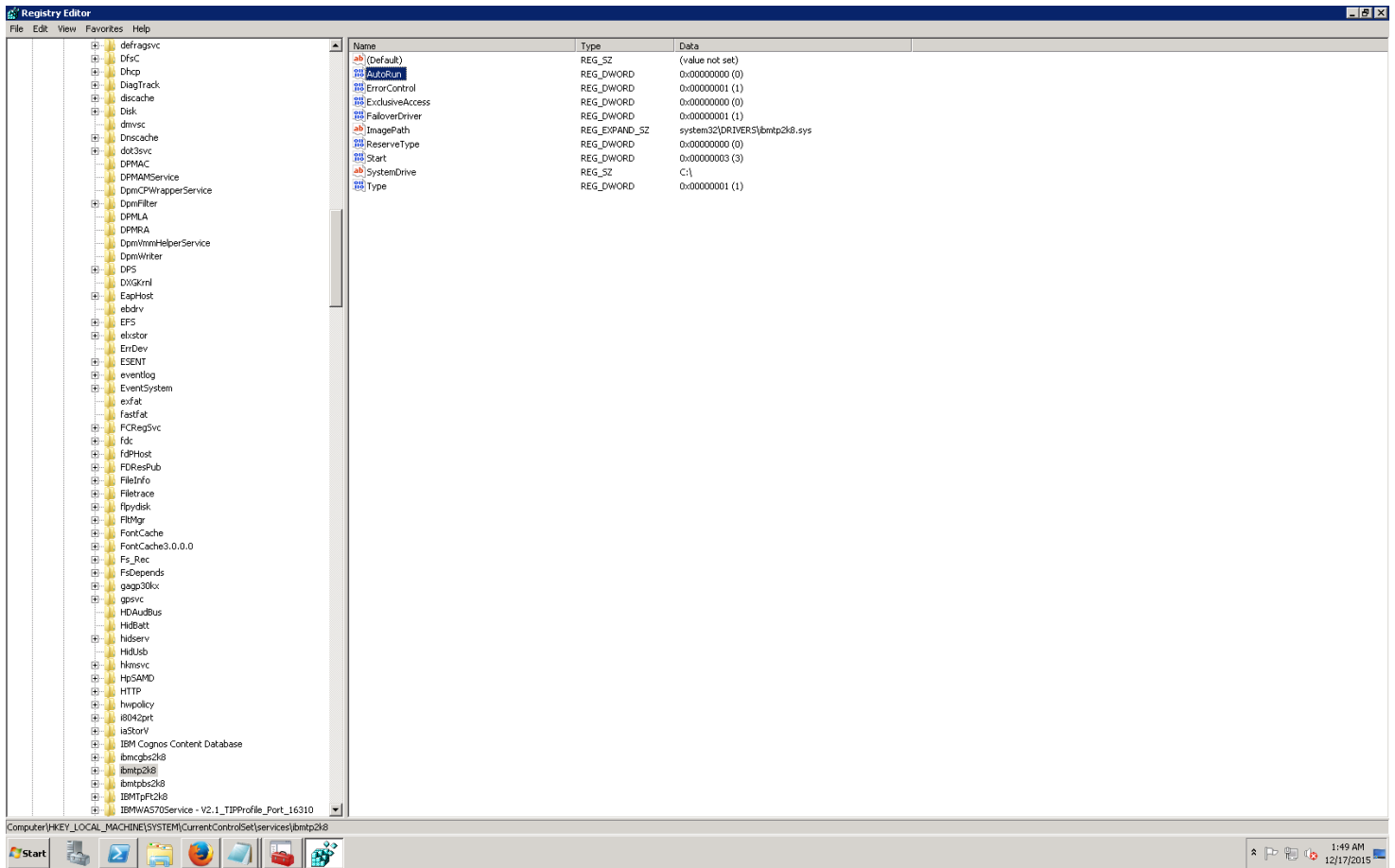


If you click INSTANCE, you can see the Service parameter.

- If DPM installed on Win 2012R2, Service name will be "ibmtp2k12".
- If DPM installed on Win 2008R2 SP1, Service name will be "ibmtp2k8".

2. Go to the following location, and select the appropriate service.
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Service_Name
3. Right-click and select **New > DWORD (32 bit) Value**. Enter the value as: **AutoRun**
4. Right-click **AutoRun** and select **Modify**. Select the Base value as Decimal and enter Zero as the value in the text box. Click **OK**.
5. Reboot system for the registry setting to take effect

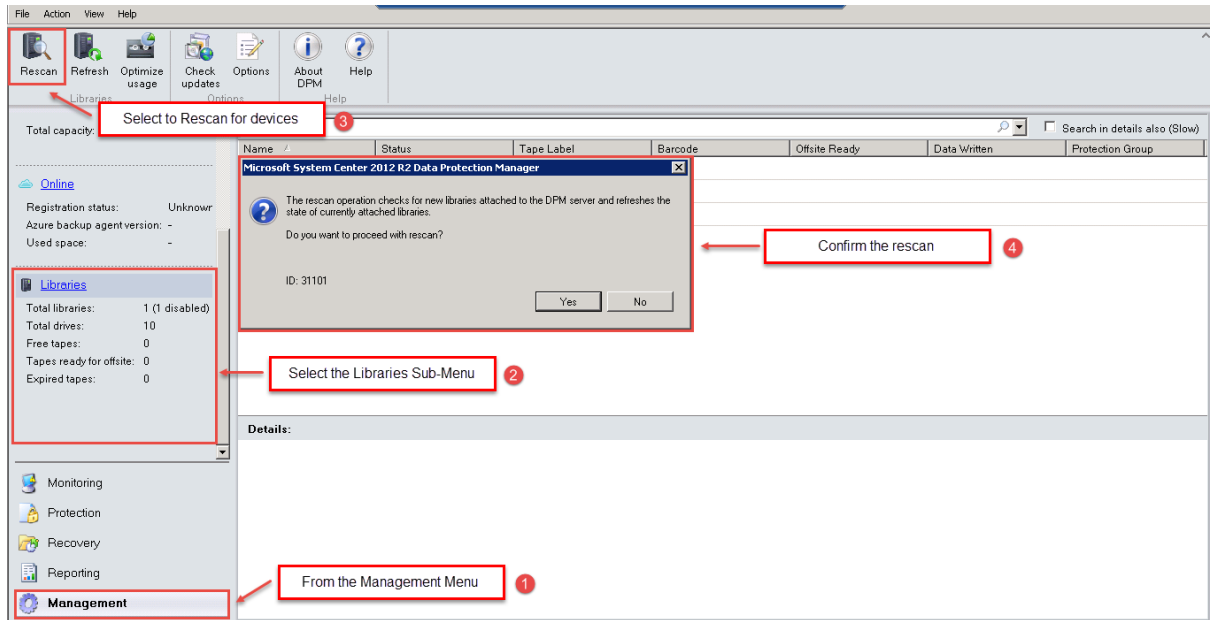




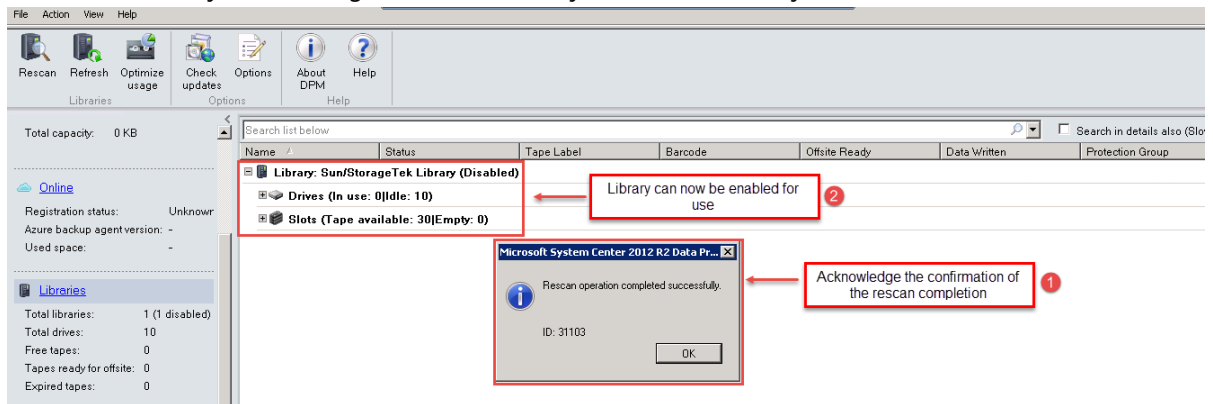
3.5 Setting up Microsoft DPM to use the newly created iSCSI VTL

1. Within the Microsoft DPM Administration interface, access the **Libraries** submenu item and select to **Rescan for Devices**.



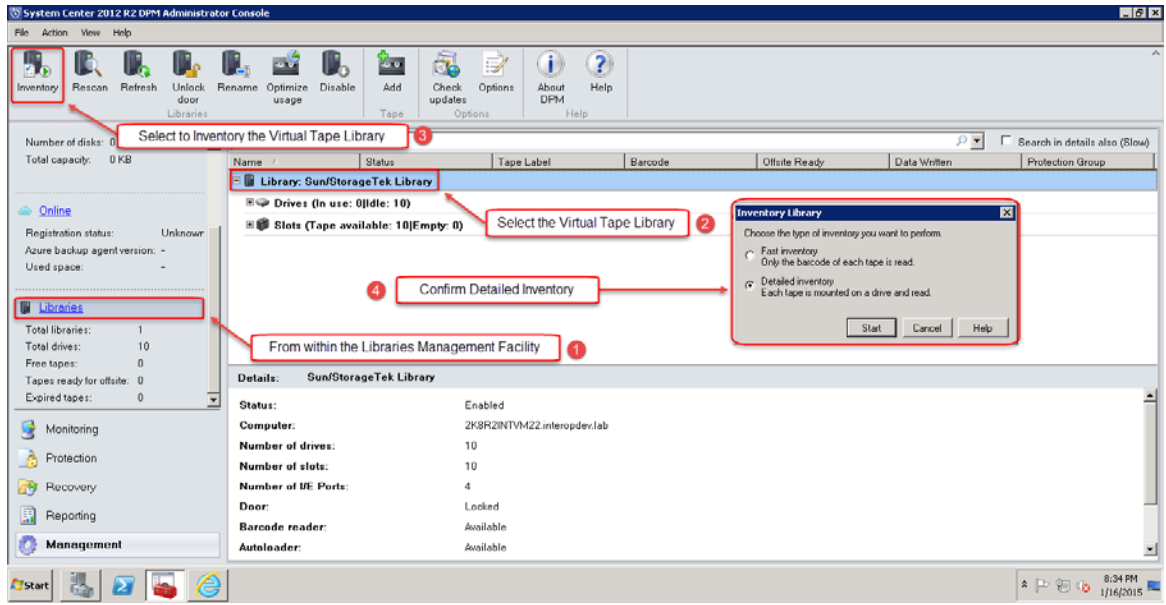


2. Once the iSCSI library has been detected by the Microsoft DPM application, then proceed to **Enable** the library for use. Right-click the newly discovered library and select to enable it.

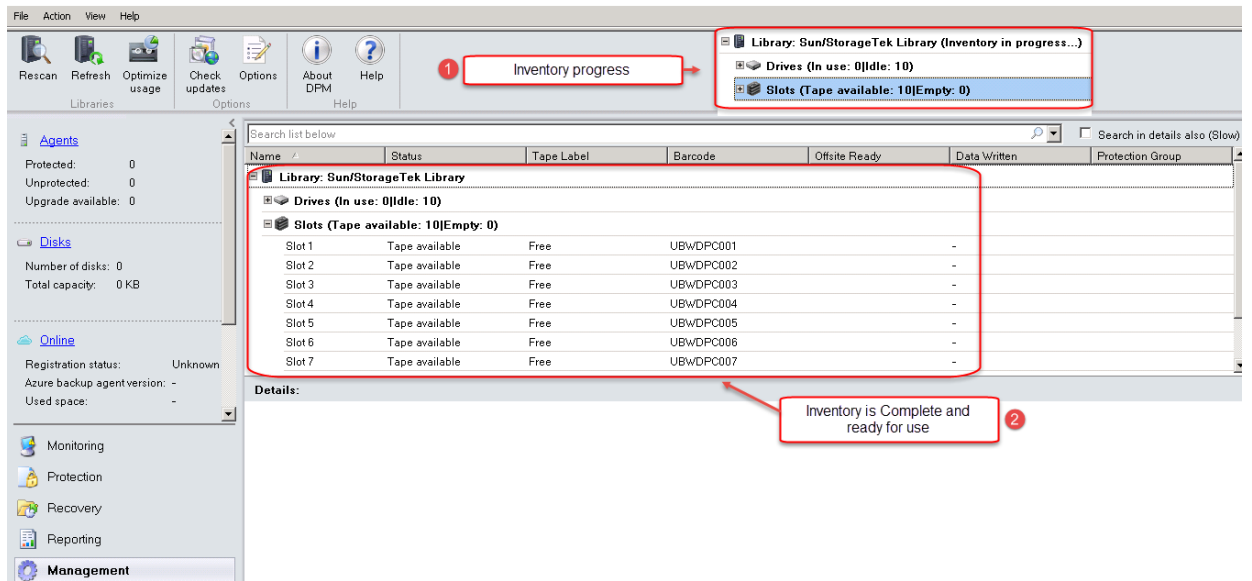


3. Once the library has been enabled to use, it must now be inventoried to identify the media available for further configuration. Select and confirm to **Inventory** the newly added library.





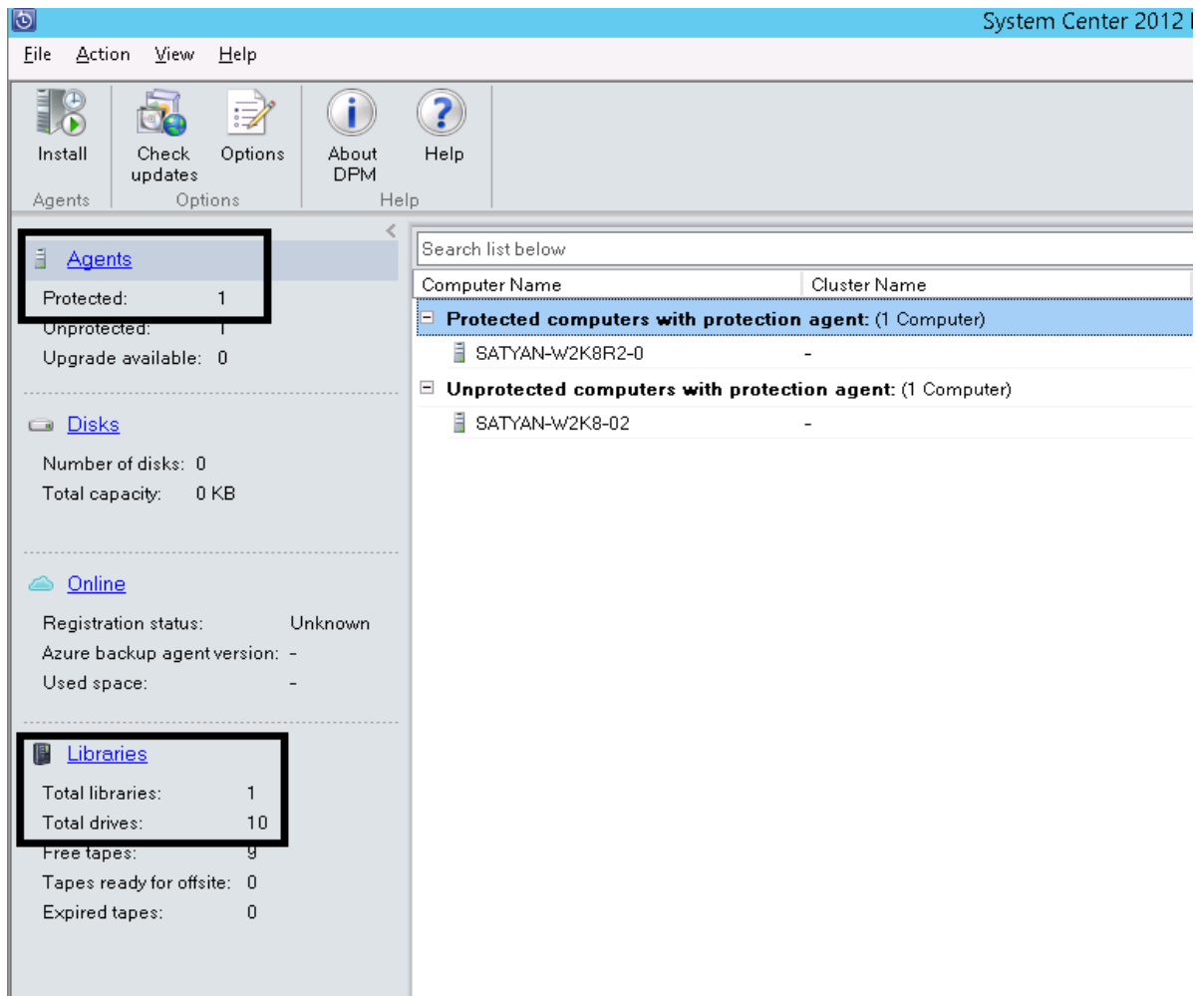
4. Once the inventory is complete, the media can now be placed into production as needed.



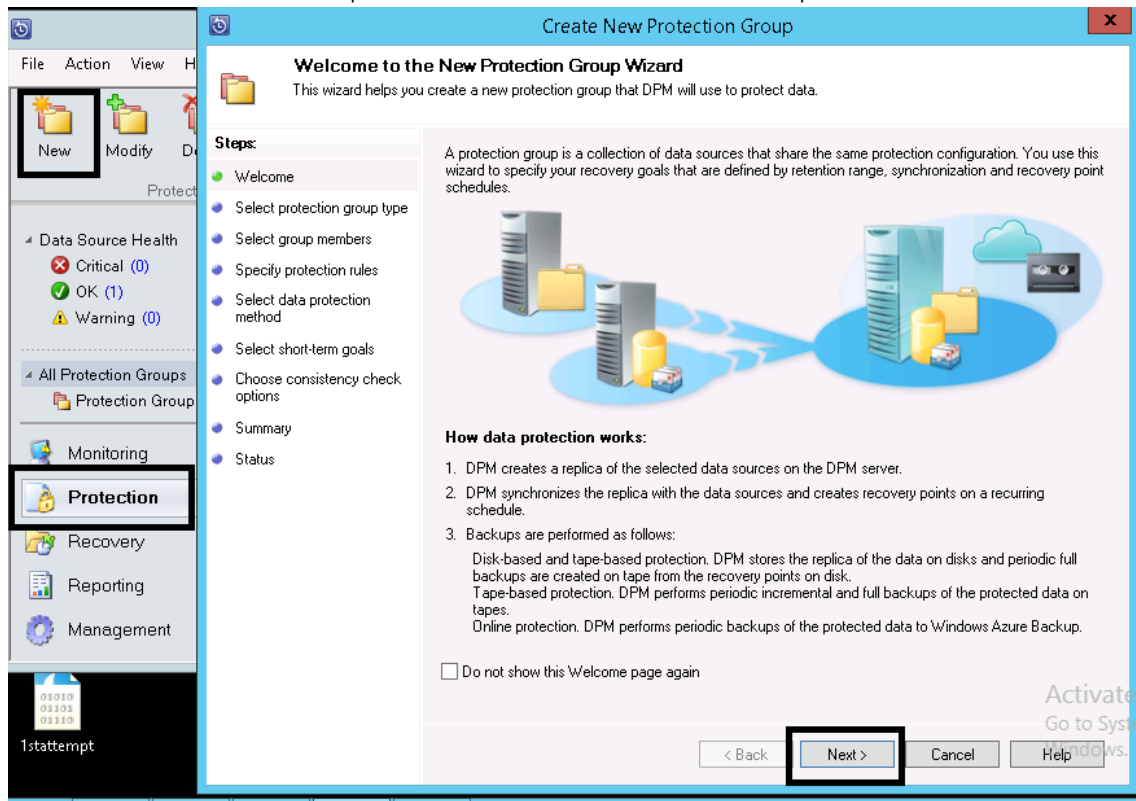
4 Performing backup and restore by using the DR Series system VTL

This section describes how to perform file-based backup and restore.

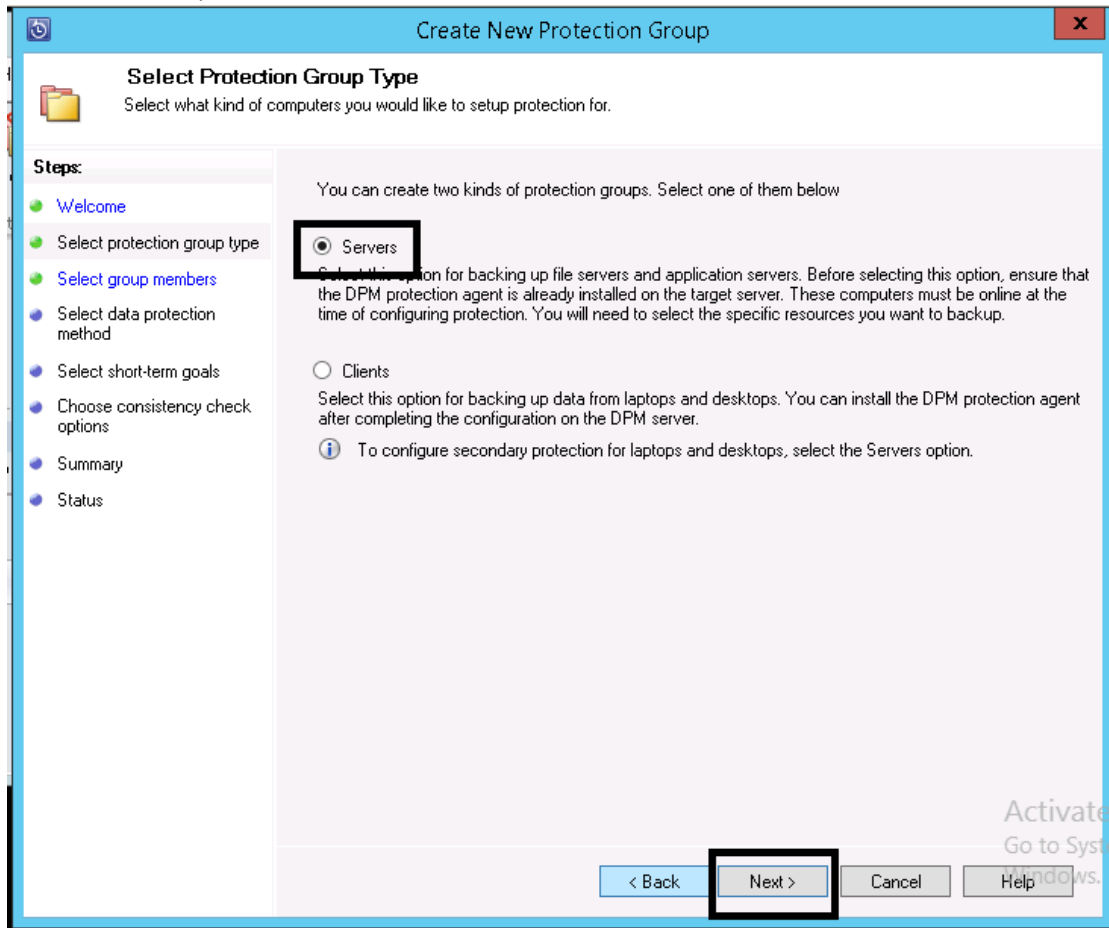
1. Install/push the DPM agent on the client that contains the files to be protected. After a successful installation on the DPM agent, the client is listed under **Agents > Protected**. The DPM installation shows 1 protected agent and 1 library.



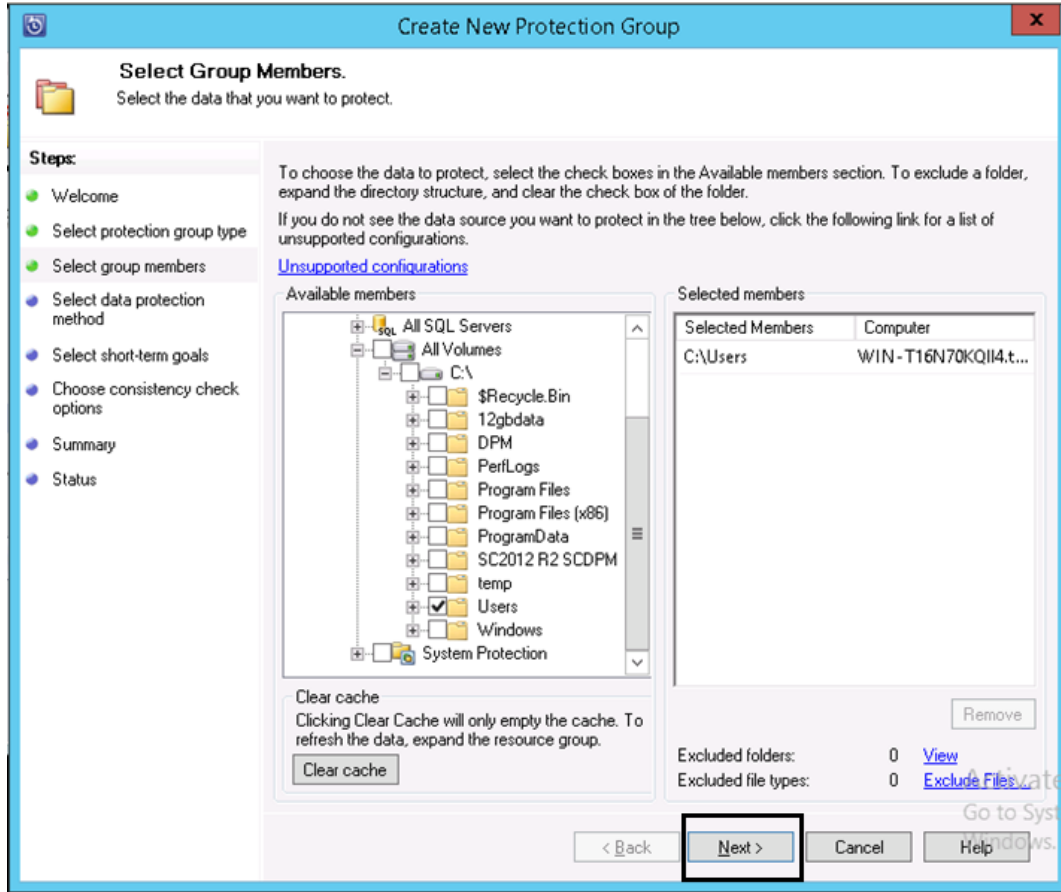
2. Click **Protection > New** to open the Create New Protection Group Wizard, and then click **Next**.



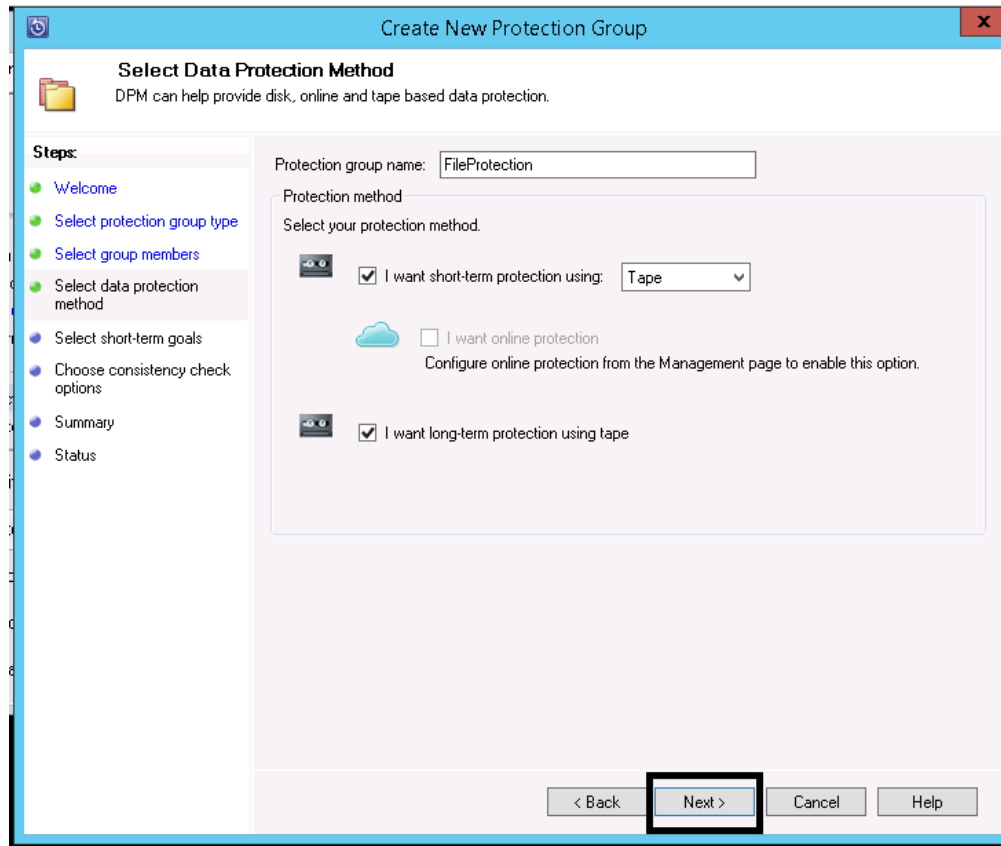
3. Select server options, and then click **Next**.



4. Select the folder that needs to be protected, and click **OK** for the system state selection. Click **Next**.



5. Enter a name for the protection group, and select **Tape** for short term protection. Select the option, **I want long-term protection using tape**, and click **Next**.



6. Specify the short-term recovery goals and click **Next**.

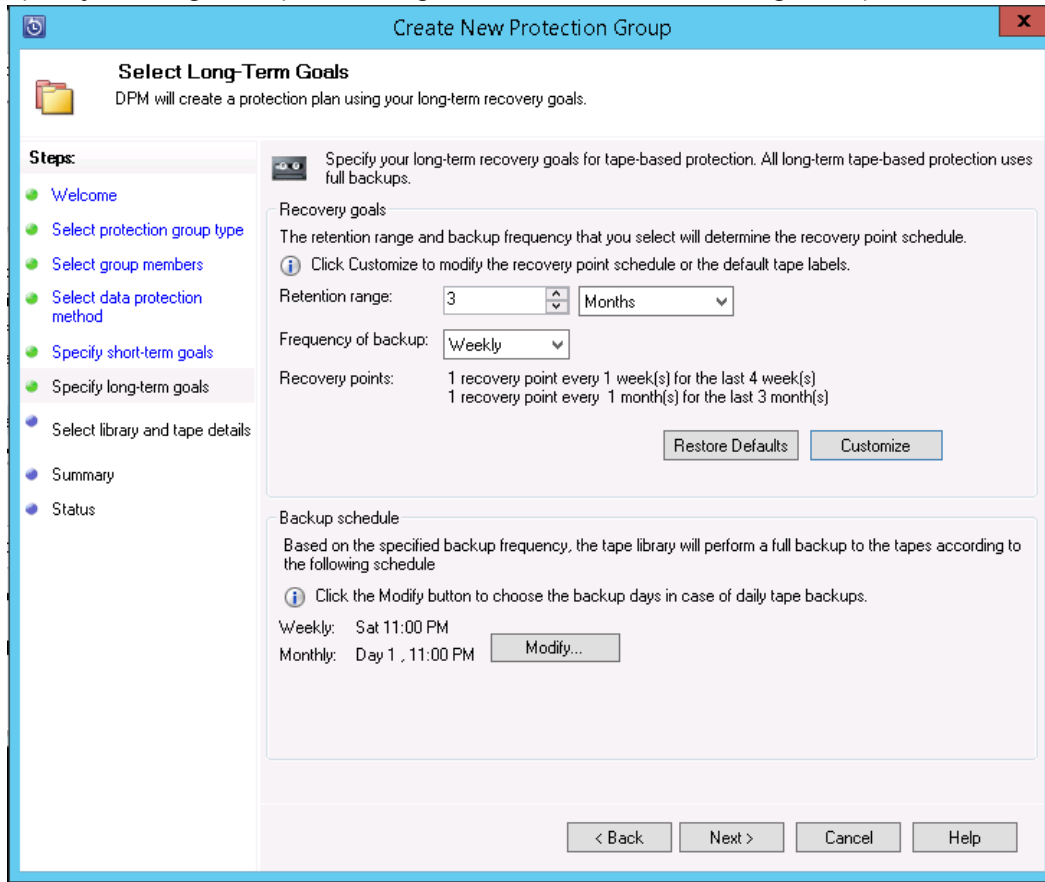
The screenshot shows the 'Create New Protection Group' wizard in Microsoft Data Protection Manager. The current step is 'Specify Short-Term Protection', which involves configuring backup goals for tape. The interface includes a 'Steps' sidebar on the left with the following items: Welcome, Select protection group type, Select group members, Select data protection method, Specify short-term goals (highlighted), Specify long-term goals, Select library and tape details, Summary, and Status. The main area contains the following configuration options:

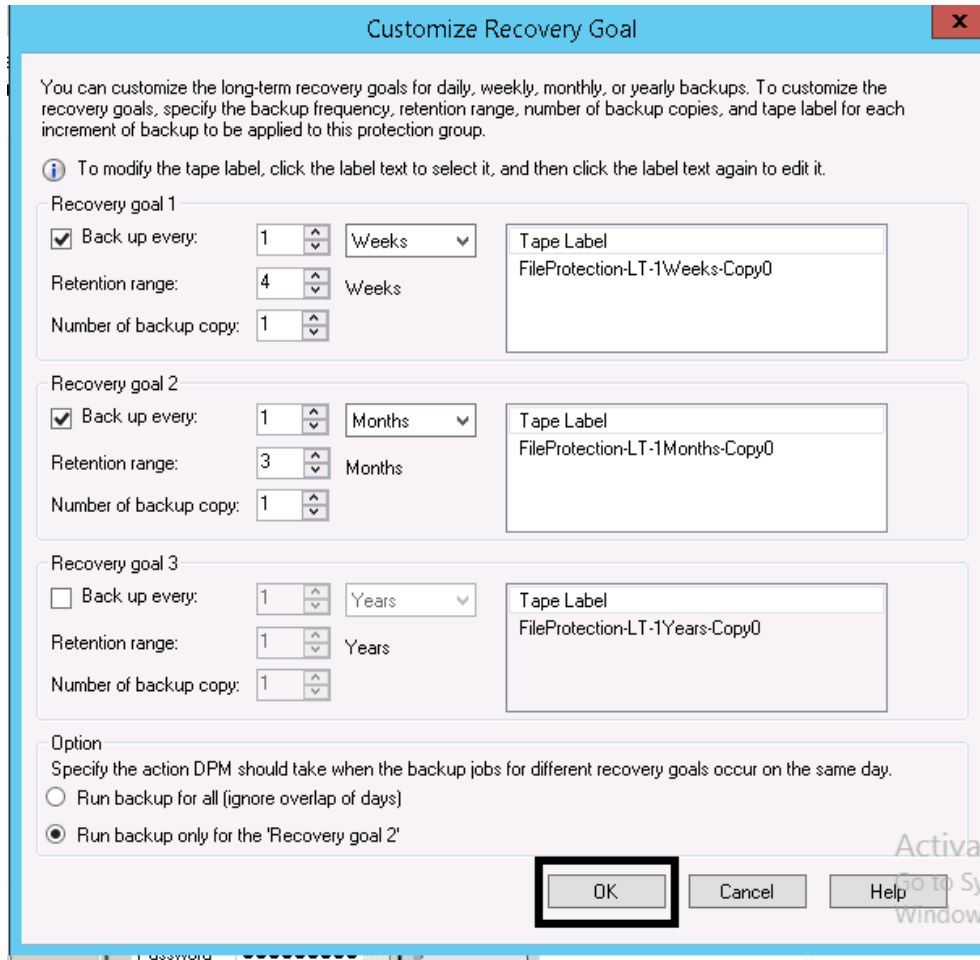
- Retention range:** 1 weeks
- Frequency of backup:** Daily
- Backup mode:** Full and incremental backups
- Backup schedule:**
 - Specify your backup day and time.
 - Full backup time:** 11:00 PM
 - Full backup day:** Saturday
 - Incremental backup time:** 11:00 PM
 - Incremental backup days:** Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

An information icon indicates: 'Incremental backups can't be scheduled on days of full backups'. At the bottom, there are four buttons: '< Back', 'Next >' (highlighted with a black box), 'Cancel', and 'Help'.



7. Specify the long-term protection goals. Customize these settings if required, and click **Next**.

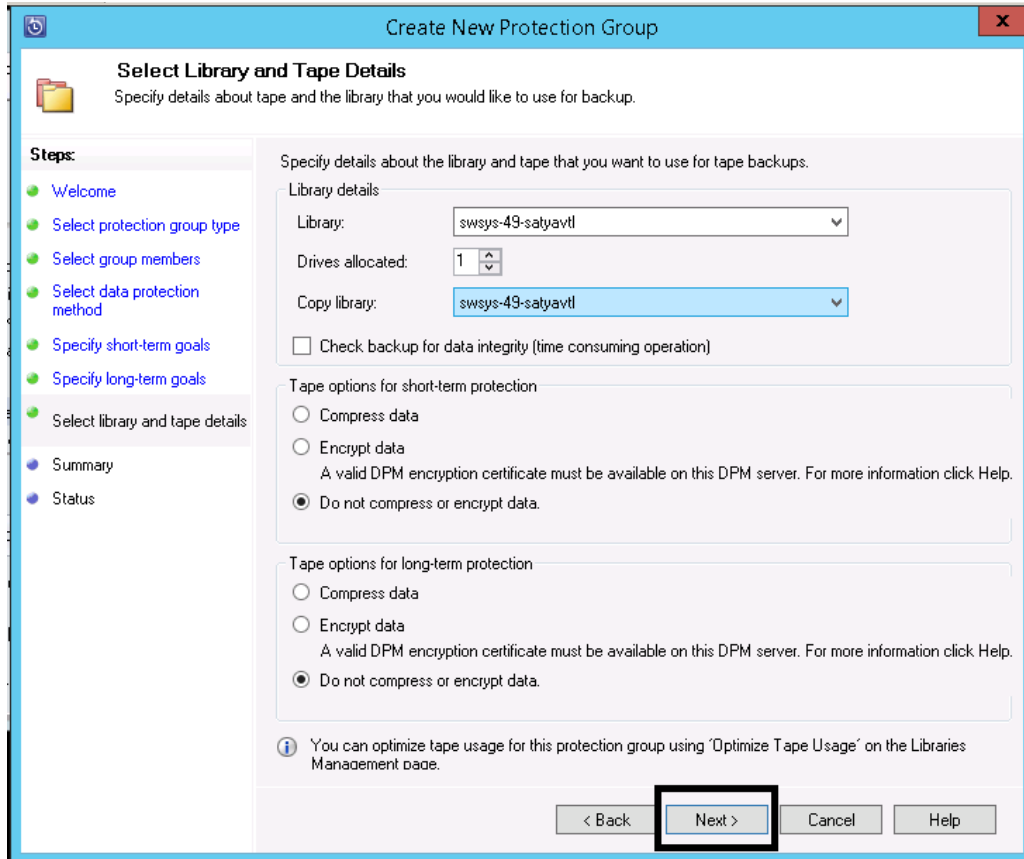




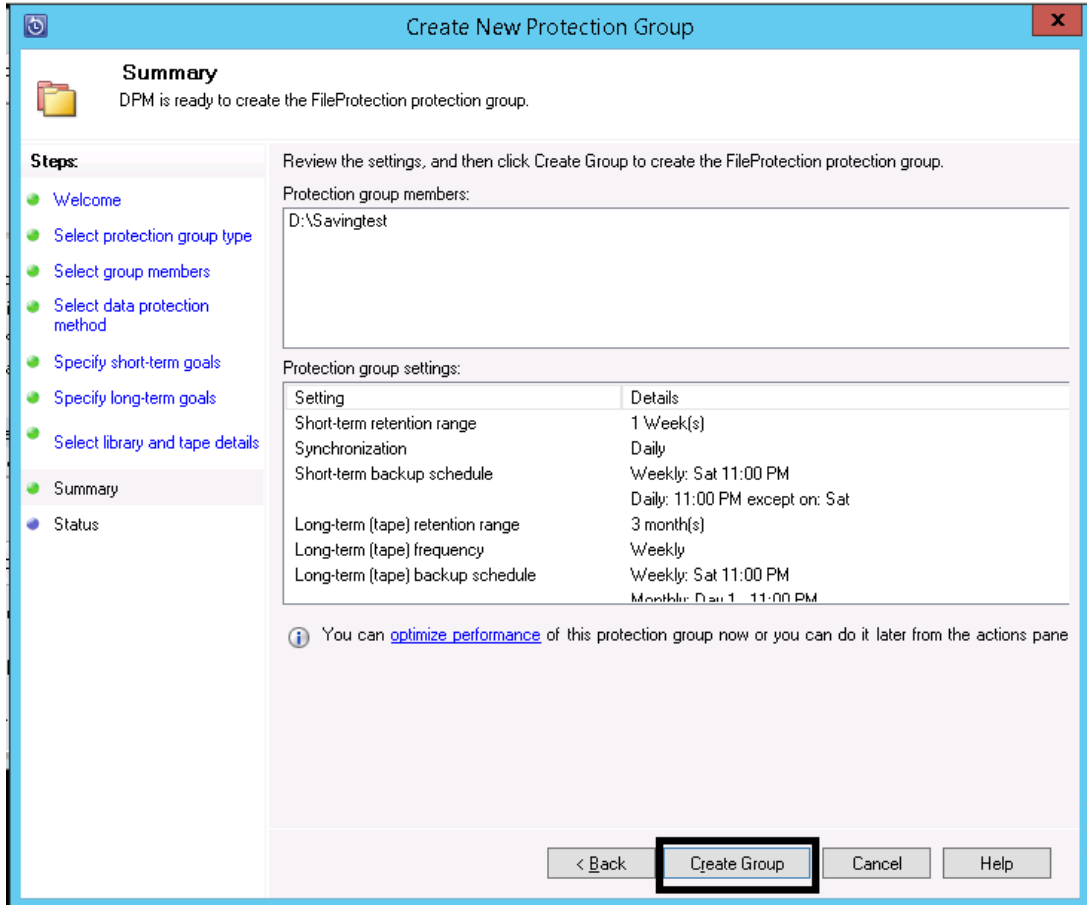
8. Under Library and Tape Detail, do the following:
 - a. Select the **Library** for primary backup and **Copy Library** for additional copy of the backup.
 - b. You can also select **Check backup for data integrity**.
 - c. Select **Do not compress or encrypt data** for both short-term and long-term backup,
 - d. Click **Next**.

Note: The DR Series system has built-in compression and encryption features; therefore, enabling these features on DPM might affect savings.

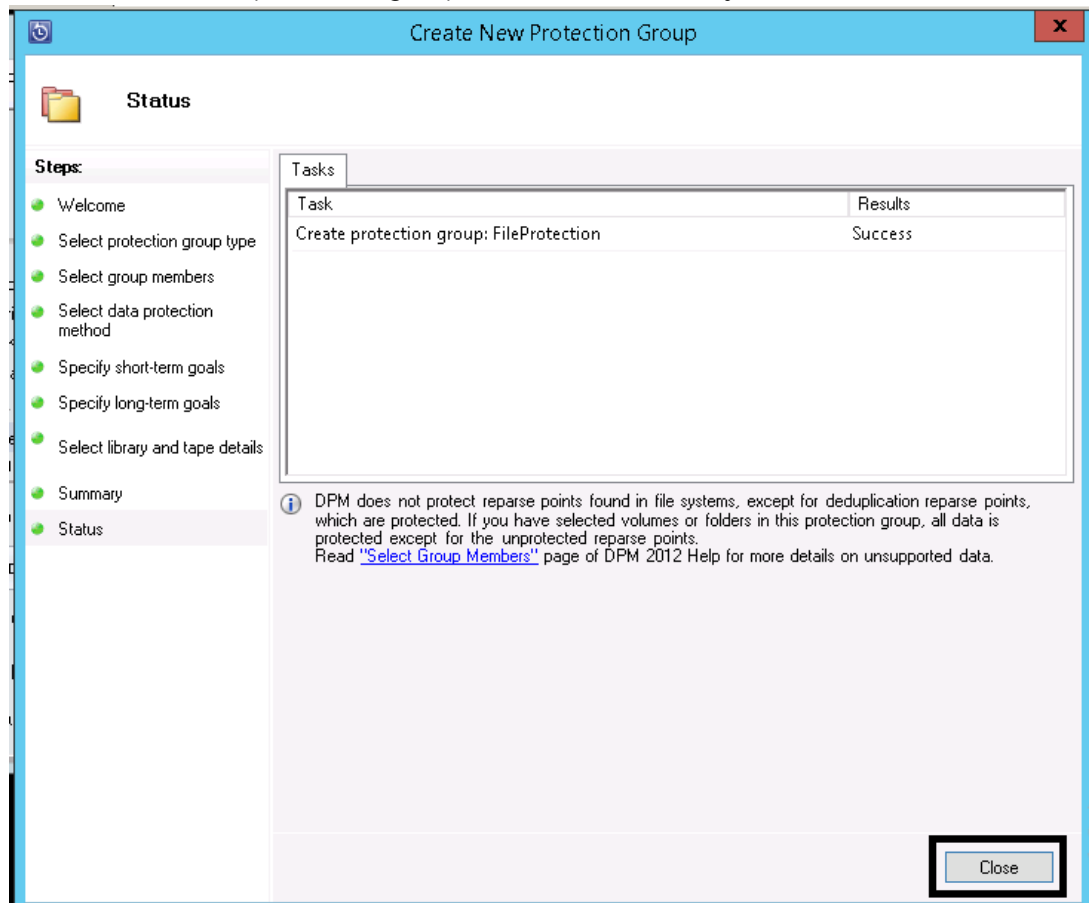




9. Review the protection group summary and click **Create group**.

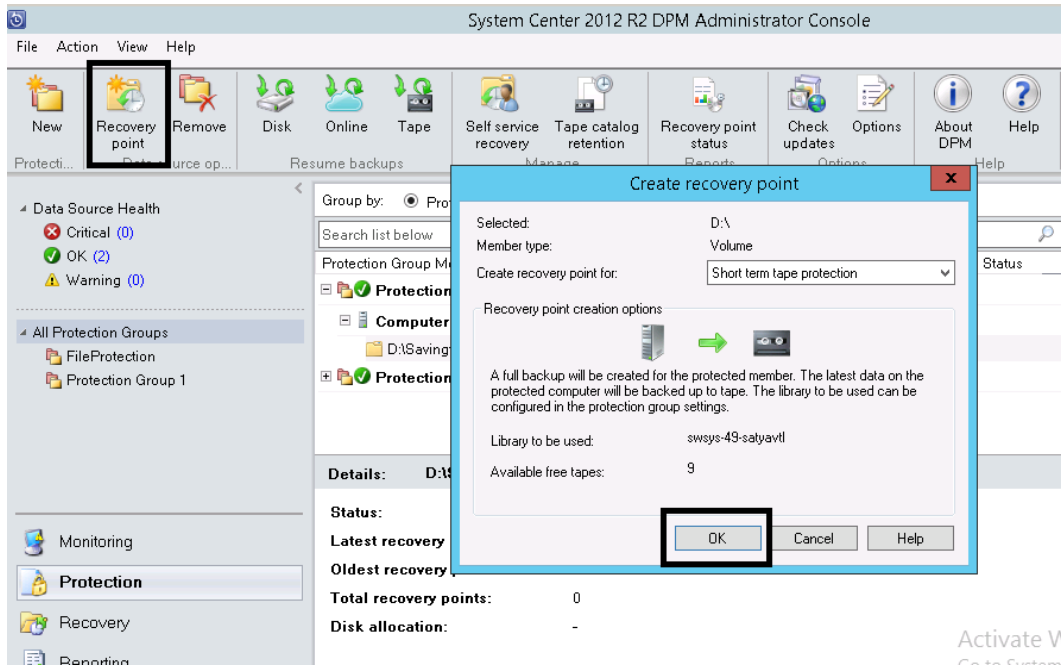


10. Make sure that the protection group is created successfully. Click **Close**.



11. To start an offline backup, expand the protection group, and select the data entry. Click **Recovery Point** to start a full backup. Click **OK**.



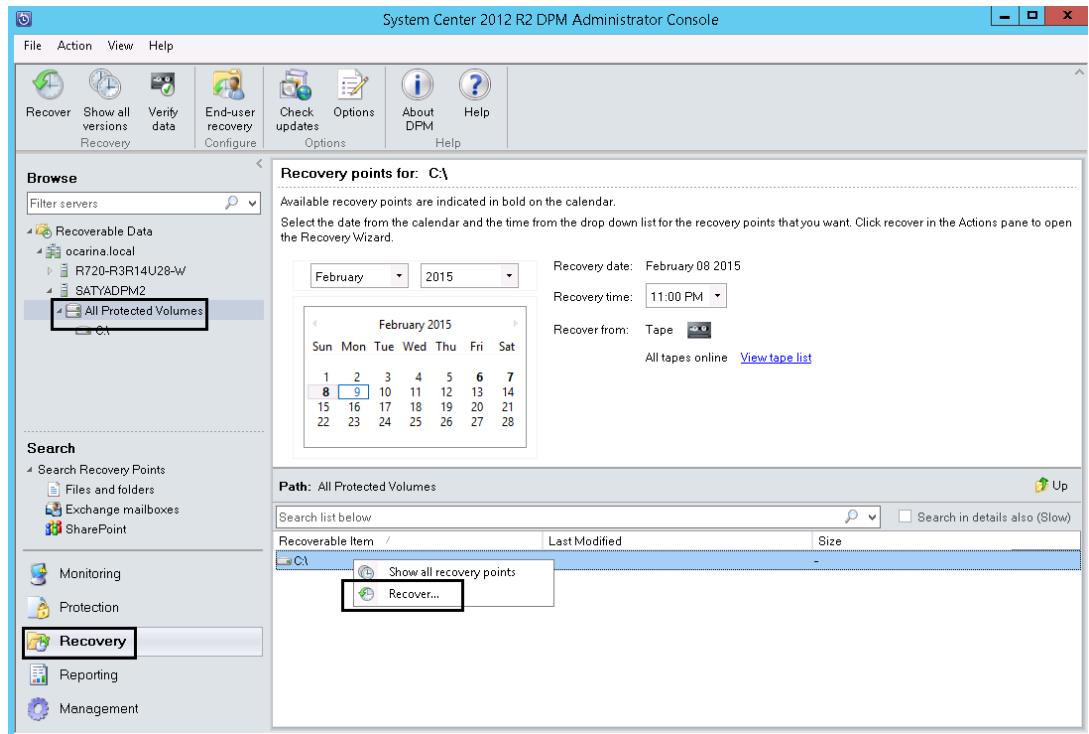


12. You can view the progress of the backup job from the Monitoring tab.

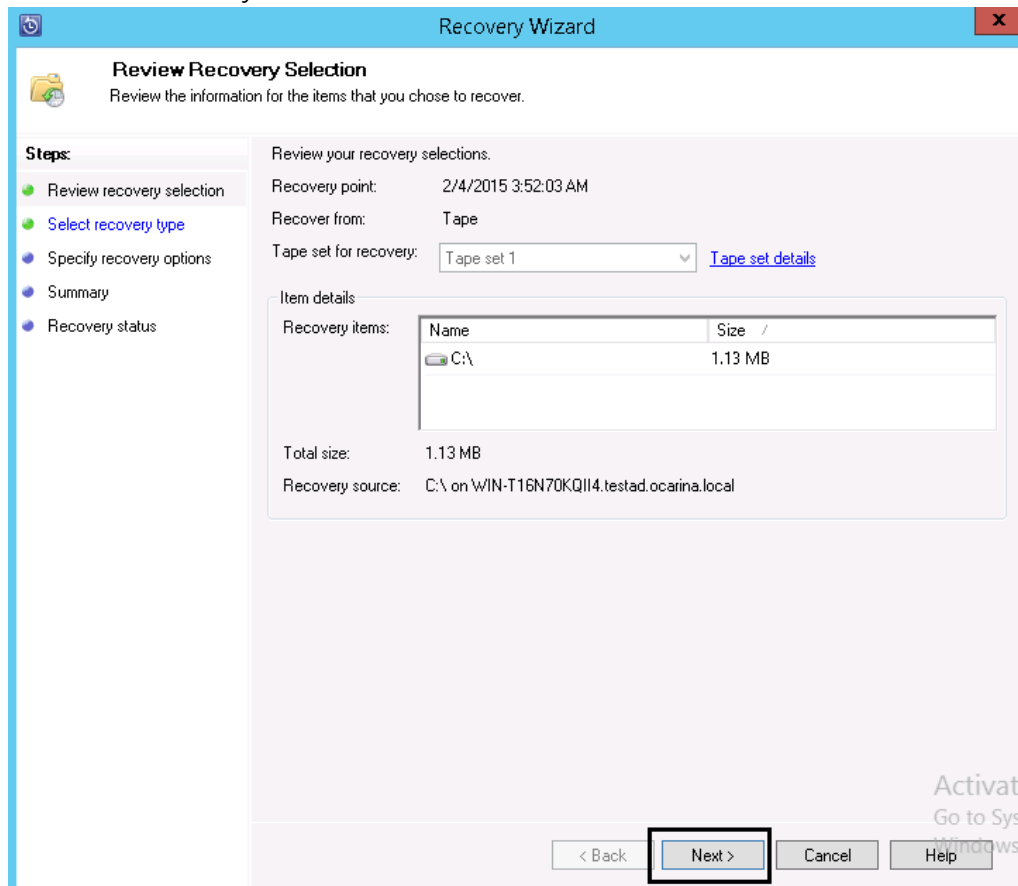


5 Restoring from tape

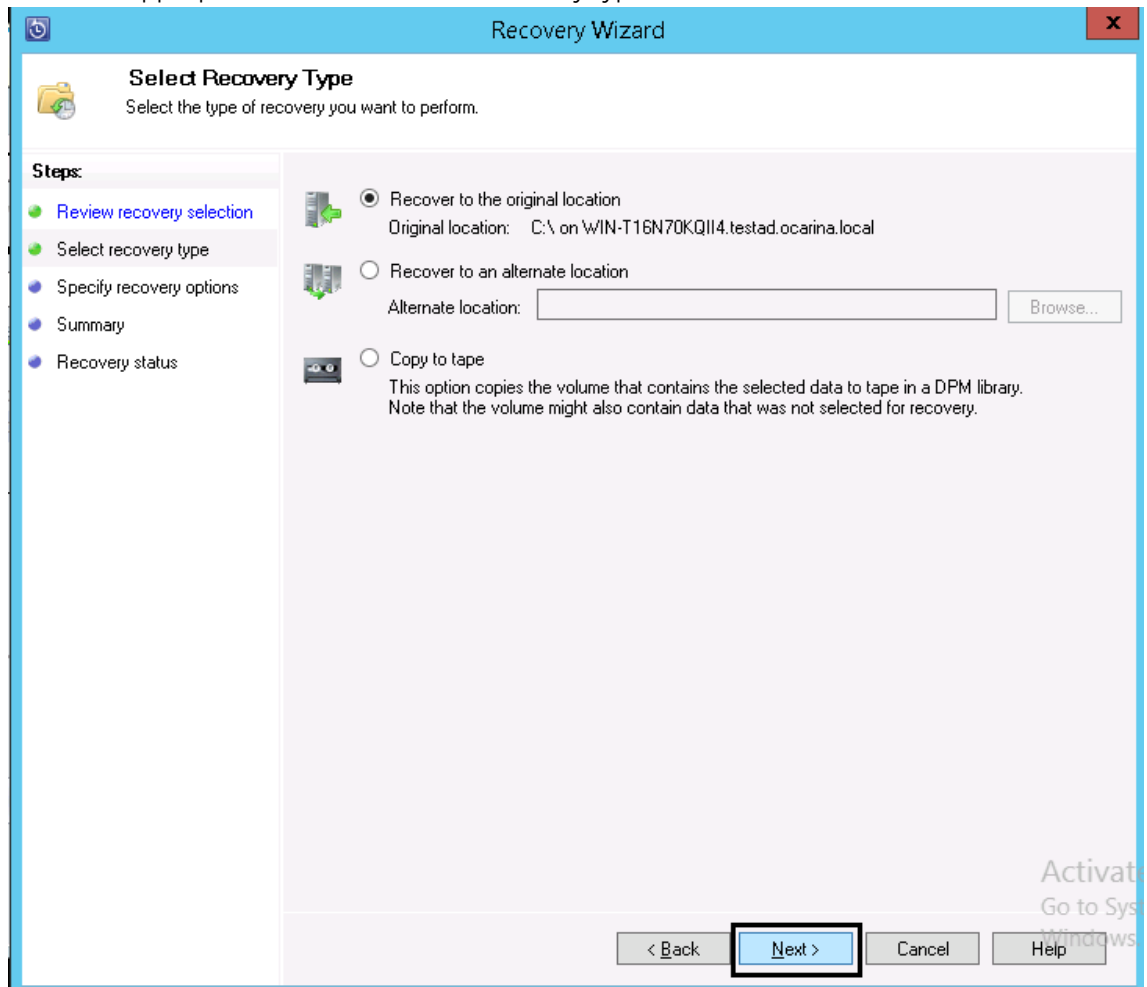
1. Click **Recovery** and select your protected volume. On the right, select the recovery point that you want to restore and right-click the recoverable item that you want to restore. The Restore Wizard opens.



2. Review the recovery selection and click **Next**.



3. Make the appropriate selection for the recovery type and click **Next**.

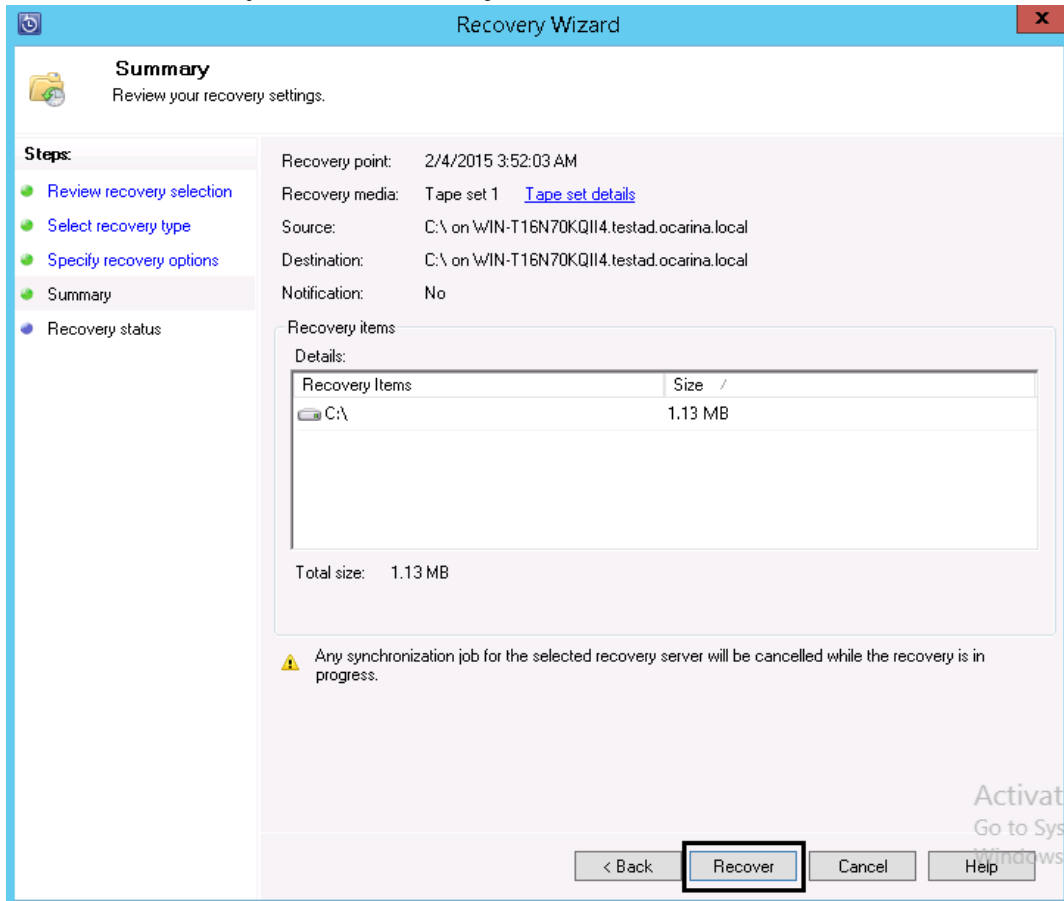


4. Specify the recovery options and click **Next**.

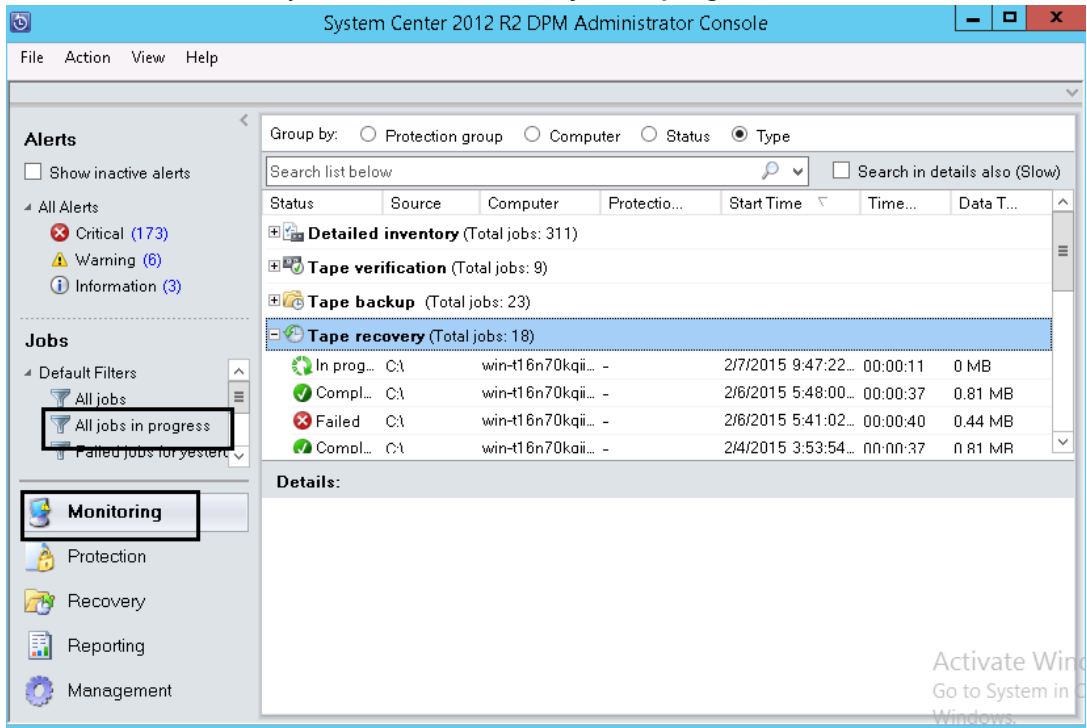
The screenshot shows the 'Specify Recovery Options' dialog box in the Recovery Wizard. The dialog has a blue title bar with the text 'Recovery Wizard' and a close button. Below the title bar, there is a header section with a folder icon and the text 'Specify Recovery Options' and 'Specify the options to apply to the recovery.' On the left side, there is a 'Steps' pane with five items: 'Review recovery selection', 'Select recovery type', 'Specify recovery options' (which is highlighted), 'Summary', and 'Recovery status'. The main area of the dialog contains several sections: 'Recovery library' with a dropdown menu set to 'satyan-sw-01-VTL-Test'; 'Existing version recovery behavior' with radio buttons for 'Create copy' (selected), 'Skip', and 'Overwrite'; 'Restore security' with radio buttons for 'Apply security settings of the destination computer' (selected) and 'Apply the security settings of the recovery point version'; 'Network bandwidth usage throttling' with a status of 'Disabled' and a 'Modify...' link; 'SAN Recovery' with a checkbox for 'Enable SAN based recovery using hardware snapshots' and a link to 'Click on Help to learn about the prerequisite steps'; and 'Notification' with a checkbox for 'Send an e-mail when this recovery completes' and a 'Recipients' field with a 'Separate e-mail addresses with comma' option and an example: 'Example: Kim@Contoso.com, Terry@Adventure-works.com'. At the bottom right, there are four buttons: '< Back', 'Next >' (highlighted with a red box), 'Cancel', and 'Help'. A watermark for 'Activate Windows' is visible in the bottom right corner.



5. Review the summary and click **Recovery**.



- To monitor the restore job, click **Monitor > All jobs in progress**.



6 Setting up the DR Series system cleaner

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

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

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

DELL DR4000
DR4000-DKCV6S1 Help | Log out

Cleaner Schedule **Schedule Cleaner** Schedule

System time zone: US/Central, Mon Jan 23 15:18:49 2012

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

Note: When no schedule is set, the cleaner will run as needed.



7 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 Managing VTL protocol accounts and credentials

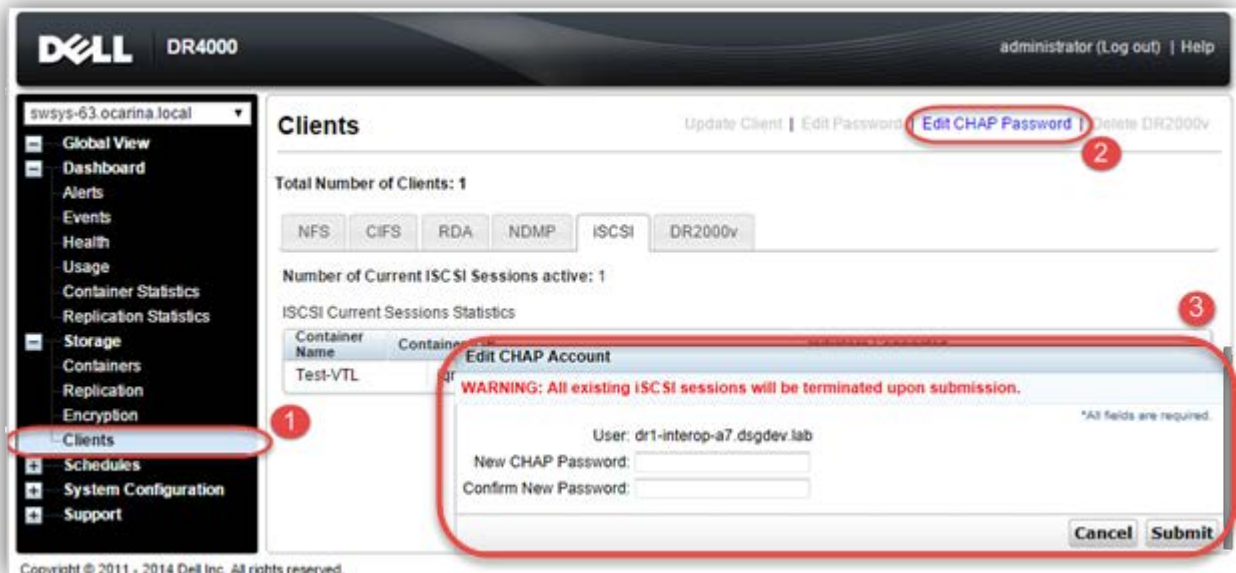
A.1 Managing iSCSI account details

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

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

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

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



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

```
> iscsi --setpassword
WARNING: All existing iSCSI sessions will be terminated!
Do you want to continue? (yes/no) [n]?
Enter new CHAP password:#####
Re-type CHAP password:#####
```



A.2 VTL default account summary table

Service	Account	Default Credentials	CLI Modifier
iSCSI	iscsi_user	St0r@ge!iscsi	iscsi--setpassword



B Managing VTL media and space usage

B.1 General performance guidelines for DMA configuration

- The DR Series system (version 3.2 and later) provides inline VTL deduplication, compression, and encryption at rest functionality. Backup applications (such as Dell NetVault, Symantec BackupExec, Symantec NetBackup, and so on) should be configured so that any multiplexing, pre-compression, software-side deduplication, or encryption is disabled. Enabling any of these features may adversely affect the space savings and ingest performance of the DR Series system VTL feature.
- Slots and media should be configured so as to accommodate the environment backup requirements. Initially, the logical capacity of a VTL should be no more than twice the physical size of the DR Series system. If the initial VTL setup is over-subscribed at higher than a 2-1 ratio without proper planning the DR Series system could fill up prematurely and cause unexpected system outage. It is highly advisable to configure the DR Series system VTL feature such that the media count be made to accommodate your initial data protection requirements. and then media be added as the deduplication statistics become available to ascertain growth, media, and space requirements.
- Media Type selection will depend on a number of factors including the DMA used, the backup cycles, data sources, and more. As a general rule, using smaller tapes is better than using larger tapes so as to allow for a higher level of control over space usage by backup operations. This also allows for easier handling in the event of a system running out of physical space as well as the normal data cleanup procedures.
- Adding media to an existing DR Series system VTL is painless and should be leveraged to incrementally add media as needed. Although this may require a higher level of involvement in managing the media usage, it will result in better performance and avoid unplanned outages.

B.2 VTL space sizing and planning

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

1. Determine Existing Data Set
2. Determine the change rate (Differential)
3. Determine the retention period
4. Calculate the data footprint during the retention period for existing data sets based on a 10-1 deduplication ratio



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

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

Note: For complete details, see the Dell DR Series Capacity Sizing Guide: A Dell Technical White Paper or contact a support or sales specialist for assistance.

B.3 Logical VTL geometry and media sizing

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

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

IMPORTANT NOTE: Media can always be added as needed. Media cannot however be deleted; therefore, care must be taken to avoid creating too many media items.

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



20TB Total initial footprint with a 10% change rate

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

NOTE: For complete details please refer to the Dell DR Disk Backup Appliance Capacity Sizing Guide: A Dell Technical White Paper or contact a support or sales specialist for assistance.

B.4 Media retention and grouping

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

B.5 VTL media count guidelines

Type	Capacity	Max number of Tapes supported
LTO-4	800GiB	2000

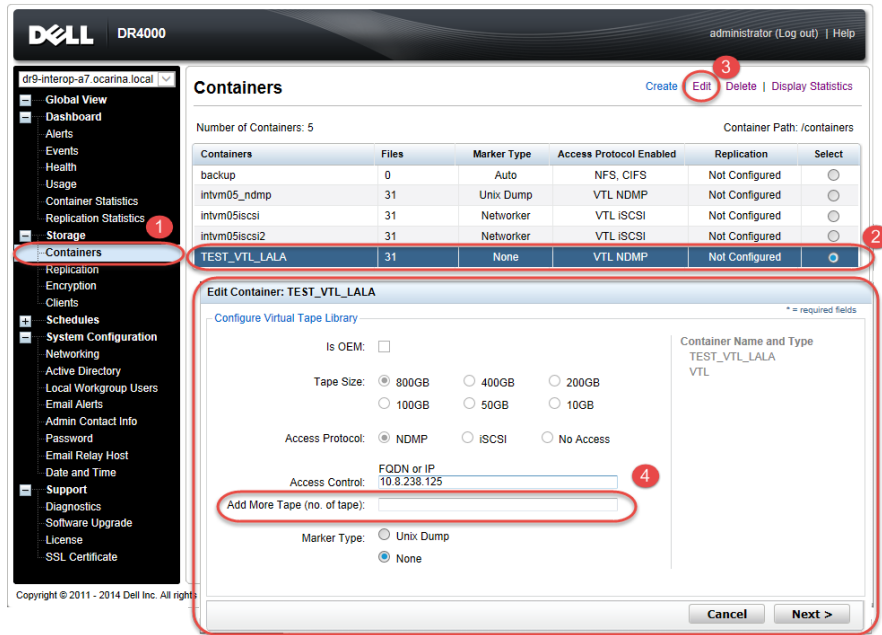
B.6 Adding VTL media to a VTL container

Follow these steps.

1. To add media to an existing VTL container, select **Containers** in the left navigation area of the DR Series system user interface.



2. Select and edit the target VTL container.
3. In the field **Add More Tape (no of Tape)**, enter the number of tapes to add to the VTL container.

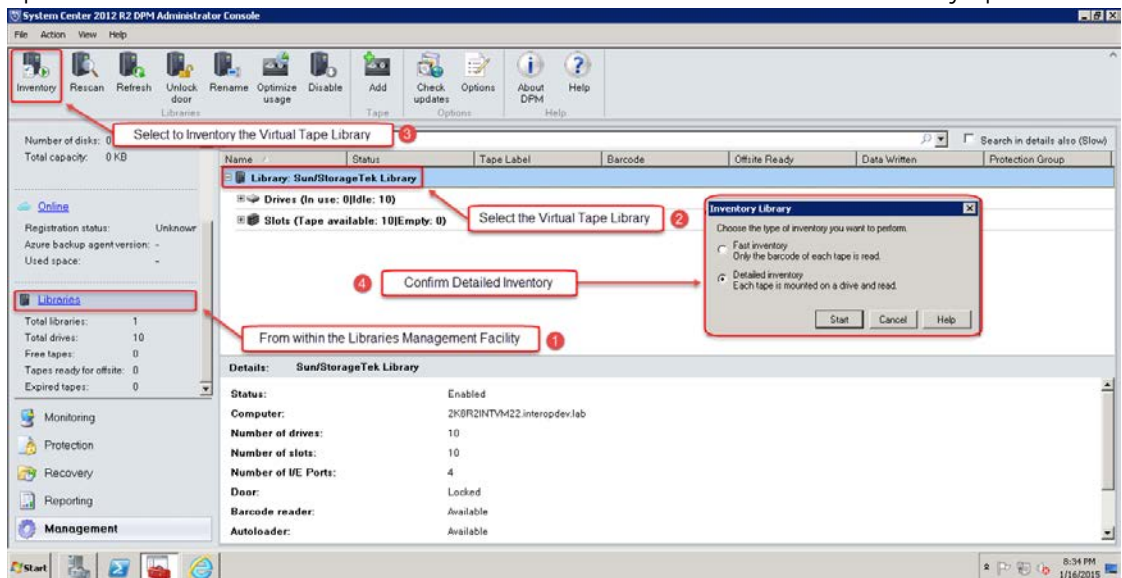


Alternatively, you can also use the “vtl –create_carts” CLI command for this operation:

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

Created 10 cartridges

4. After the VTL media has been added to the target VTL container, Microsoft DPM must now be updated to be able to use said media. Select the VTL and conduct an inventory update.



B.7 Space reclamation

B.7.1 General guidelines

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

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

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

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

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

B.7.2 Product specific guidelines

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

