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

Dell Engineering

January 2016

A Dell Technical White Paper

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.

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

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

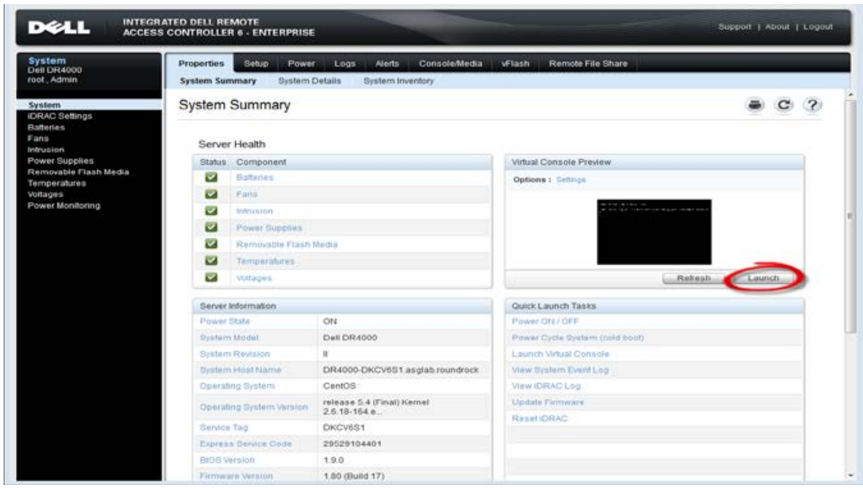
Note: The DR Series system and DPM screenshots used in this document may vary slightly, depending on the DR Series system firmware version and Microsoft DPM version used.

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”.

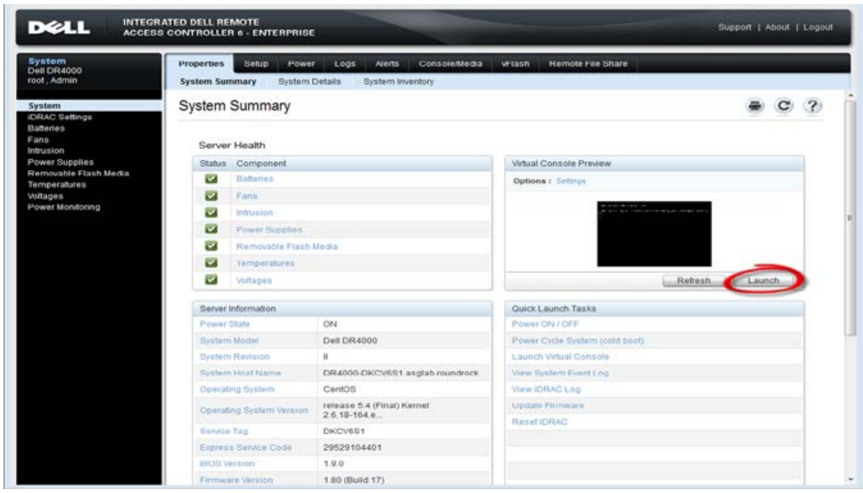
3. Log on to iDRAC using the default address **192.168.0.120**, or the IP that is assigned to the iDRAC interface. Use the user name and password of “**root/calvin**”.



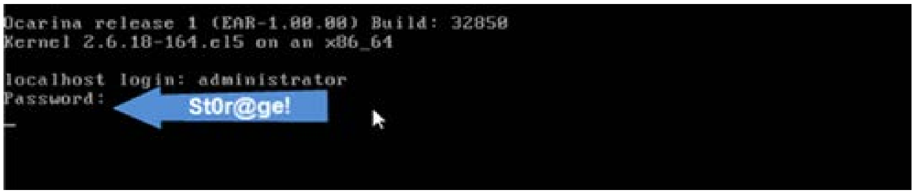
Status	Component
☑	Batteries
☑	Fans
☑	Intrusion
☑	Power Supplies
☑	Removable Flash Media
☑	Temperatures
☑	Voltages

Server Information	
Power State	ON
System Model	Dell DR4000
System Revision	II
System Host Name	DR4000-DKCV6S1.asglab.roundrock
Operating System	CentOS
Operating System Version	release 5.4 (Final) Kernel 2.6.18-164.e...
Service Tag	DKCV6S1
Express Service Code	29529104401
BIOS Version	1.9.0
Firmware Version	1.80 (Build 17)

4. Launch the virtual console.

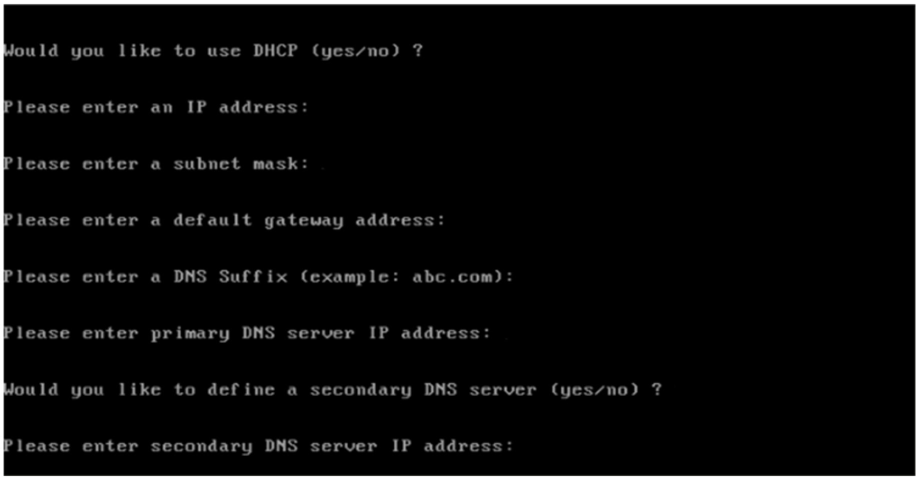

INTEGRATED DELL REMOTE ACCESS CONTROLLER 6 - ENTERPRISE
System Summary
Server Health: Batteries, Fans, Intrusion, Power Supplies, Removable Flash Media, Temperatures, Voltages
Server Information: Power State ON; System Model Dell DR4000; System Revision II; System Host Name DR4000-DKCV6S1.asglab.roundrock; Operating System CentOS; Operating System Version release 5.4 (Final) Kernel 2.6.18-164.e...; Service Tag DKCV6S1; Express Service Code 29529104401; BIOS Version 1.9.0; Firmware Version 1.80 (Build 17)
Virtual Console Preview: Refresh, Launch

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).



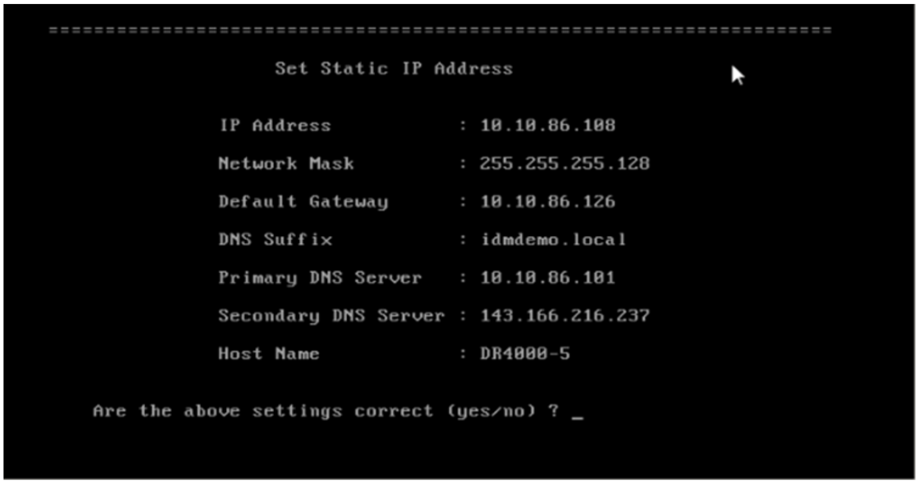
```
Ocarina release 1 (EAR-1.00.00) Build: 32850
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password:
_
```

6. Set the user-defined networking preferences.



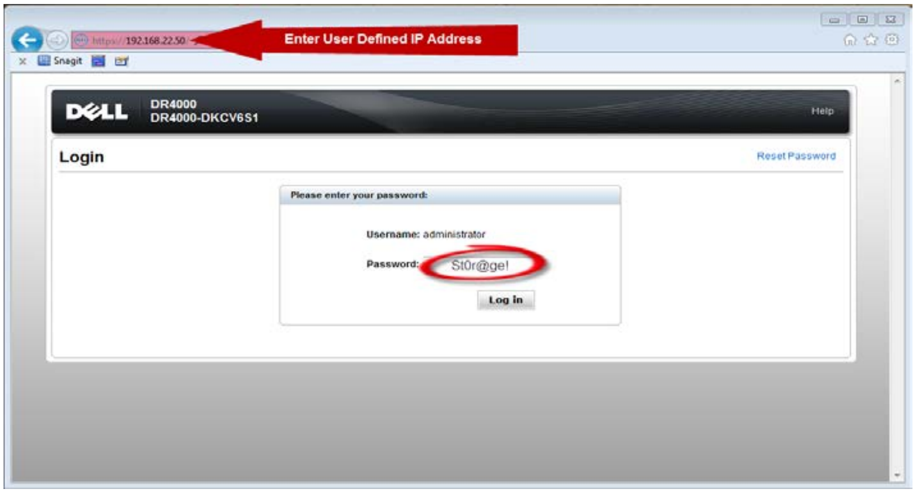
```
Would you like to use DHCP (yes/no) ?

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).



Please enter your password:

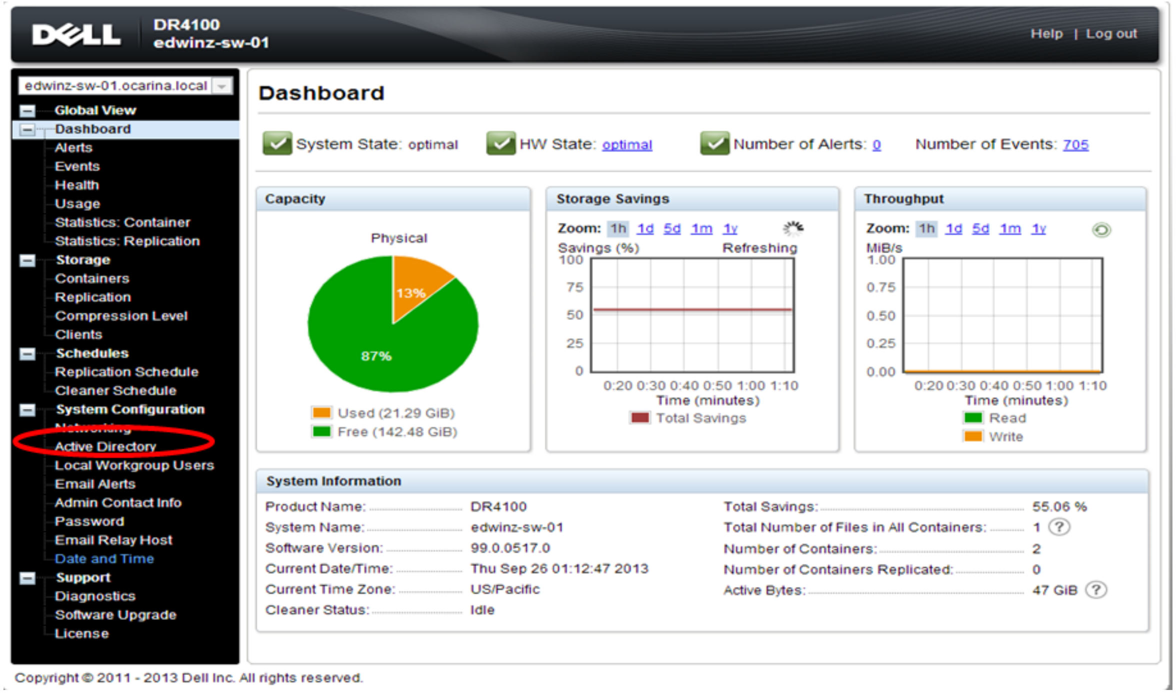
Username: administrator

Password: St0r@ge!

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.



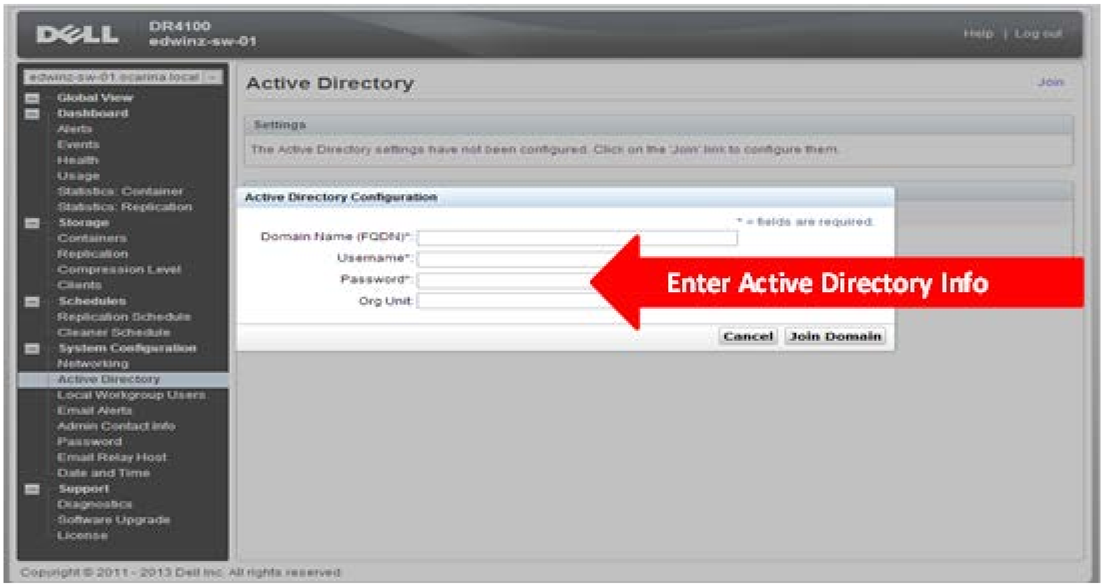
✓ System State: optimal ✓ HW State: optimal ✓ Number of Alerts: 0 Number of Events: 705

System Information

Product Name:	DR4100	Total Savings:	55.06 %
System Name:	edwinz-sw-01	Total Number of Files in All Containers:	1
Software Version:	99.0.0517.0	Number of Containers:	2
Current Date/Time:	Thu Sep 26 01:12:47 2013	Number of Containers Replicated:	0
Current Time Zone:	US/Pacific	Active Bytes:	47 GiB
Cleaner Status:	Idle		

Copyright © 2011 - 2013 Dell Inc. All rights reserved.

b. Enter your Active Directory credentials.



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

Active Directory Configuration

* = fields are required.

Domain Name (FQDN)*:

Username*:

Password*:

Org Unit:

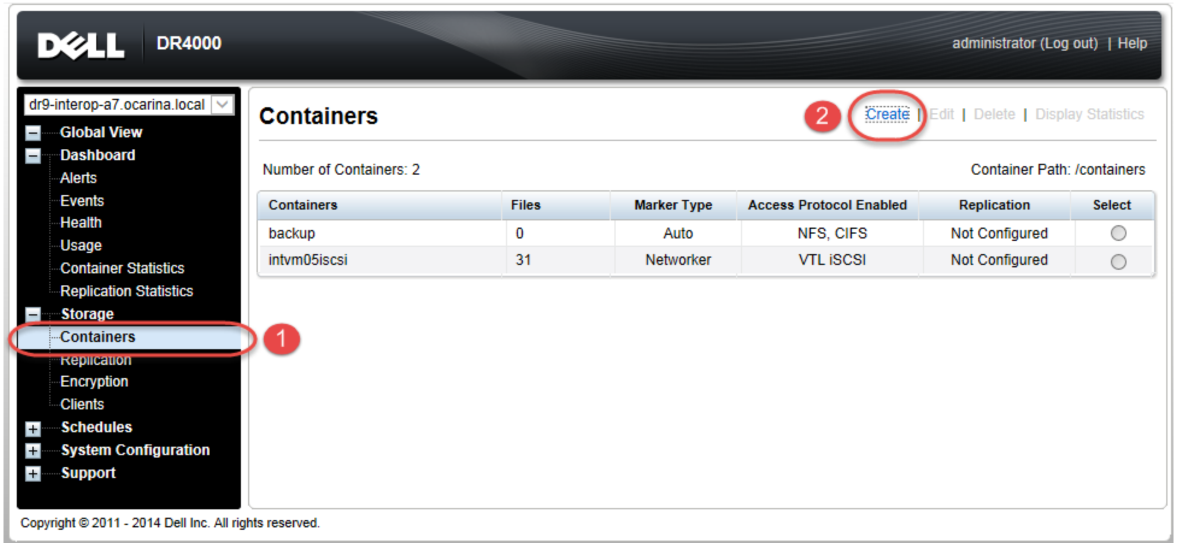
Enter Active Directory Info

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.



Containers

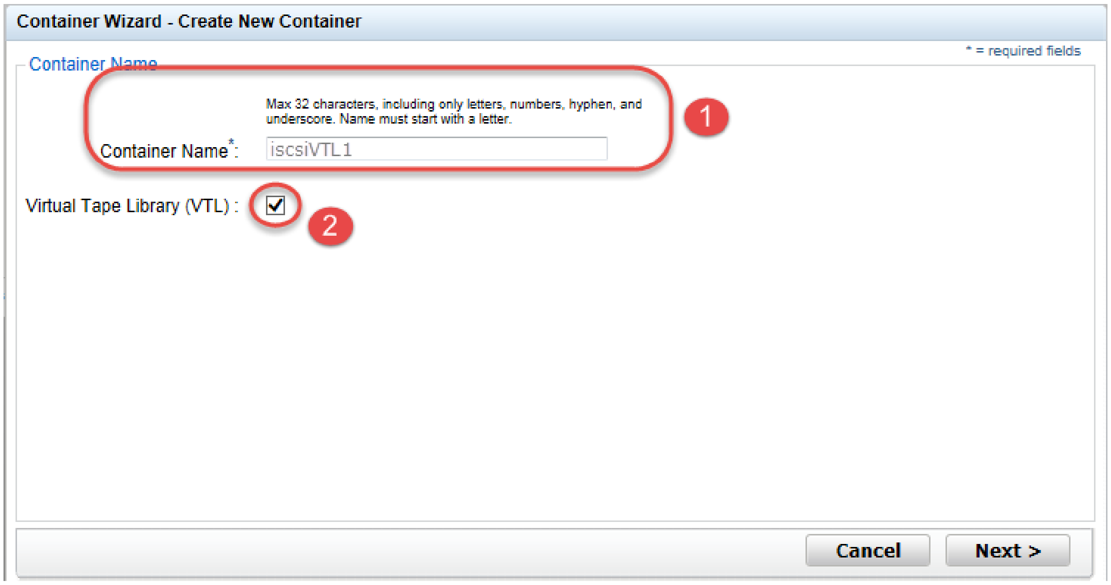
Number of Containers: 2

Container Path: /containers

Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
backup	0	Auto	NFS, CIFS	Not Configured	○
intvm05iscsi	31	Networker	VTL iSCSI	Not Configured	○

Copyright © 2011 - 2014 Dell Inc. All rights reserved.

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



Container Wizard - Create New Container

* = required fields

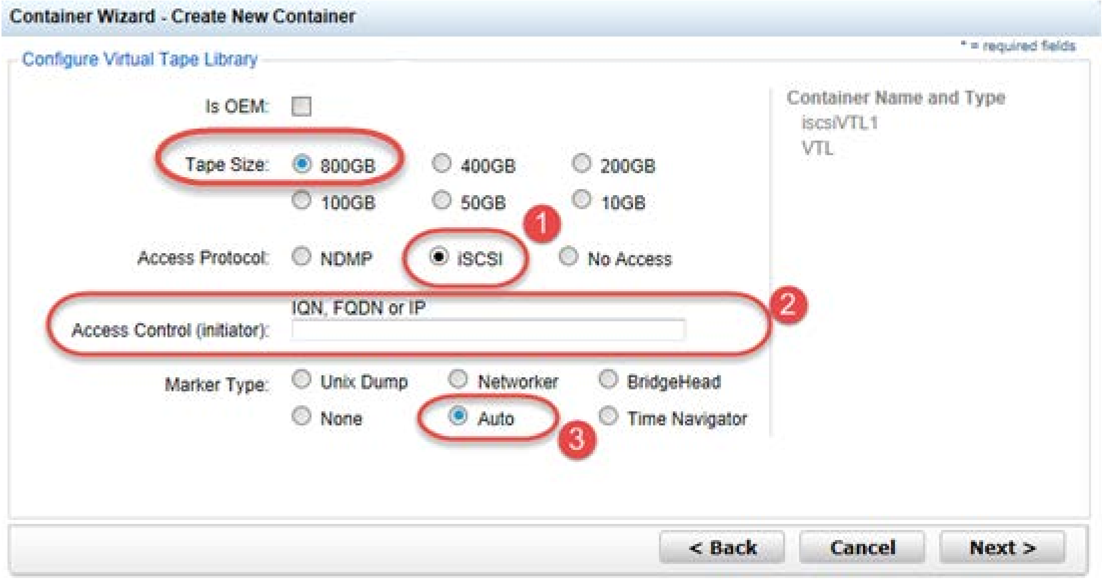
Container Name

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

Container Name*: iscsiVTL1

Virtual Tape Library (VTL) : ☑

3. 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

* = required fields

Is OEM: □

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

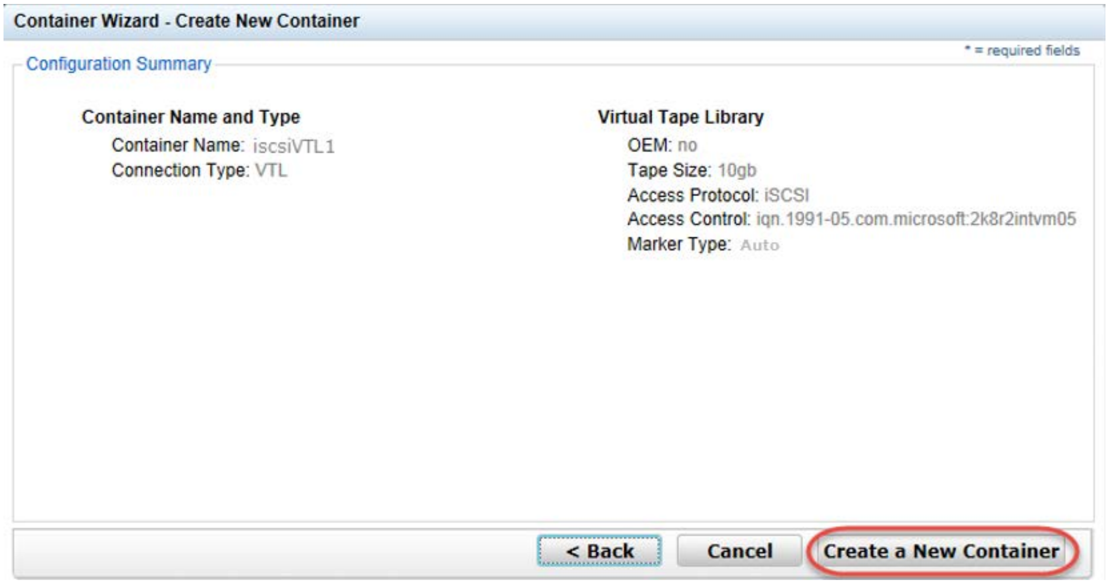
Access Protocol: ○ NDMP ● iSCSI ○ No Access

Access Control (initiator): IQN, FQDN or IP

Marker Type: ○ Unix Dump ○ Networker ○ BridgeHead ○ None ● Auto ○ Time Navigator

Container Name and Type
iscsiVTL1
VTL

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



Container Wizard - Create New Container

Configuration Summary

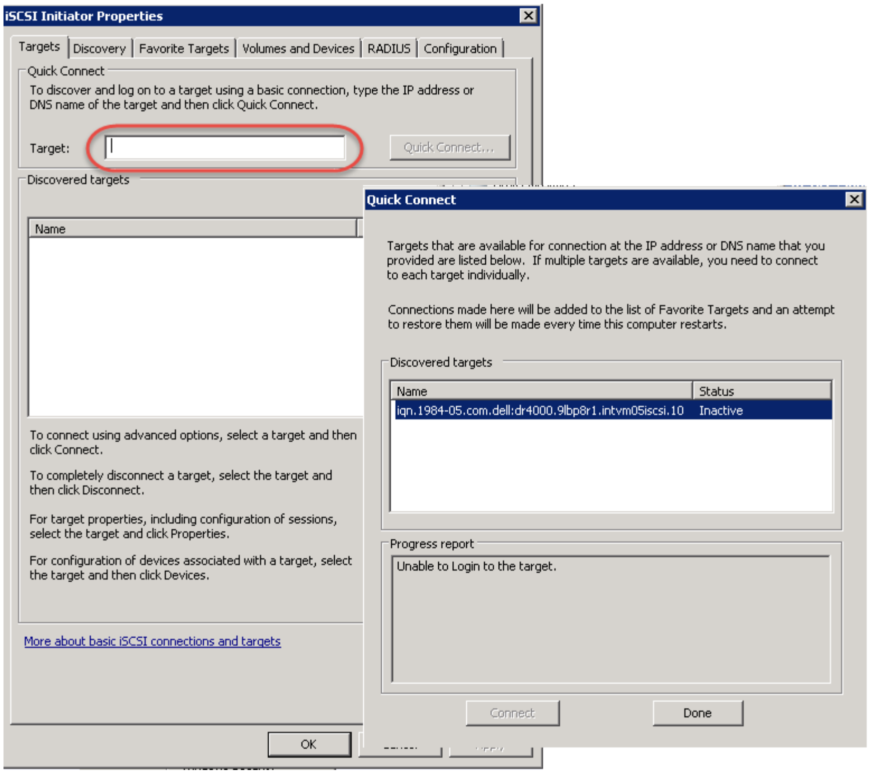
* = required fields

Container Name and Type
Container Name: iscsiVTL1
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

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.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

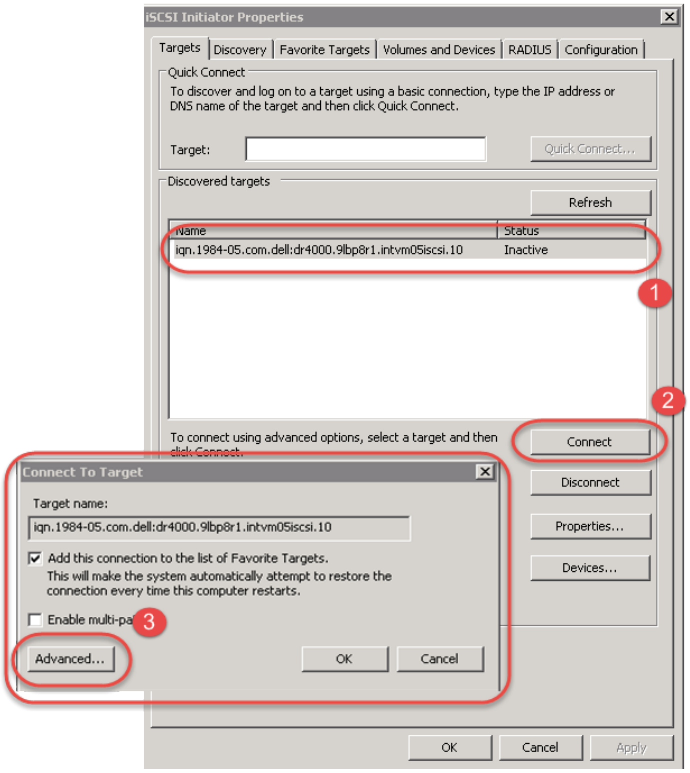
Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.

Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.

Name	Status
iqn.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Inactive

Unable to Login to the target.

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.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Name	Status
iqn.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Inactive

To connect using advanced options, select a target and then click Connect.

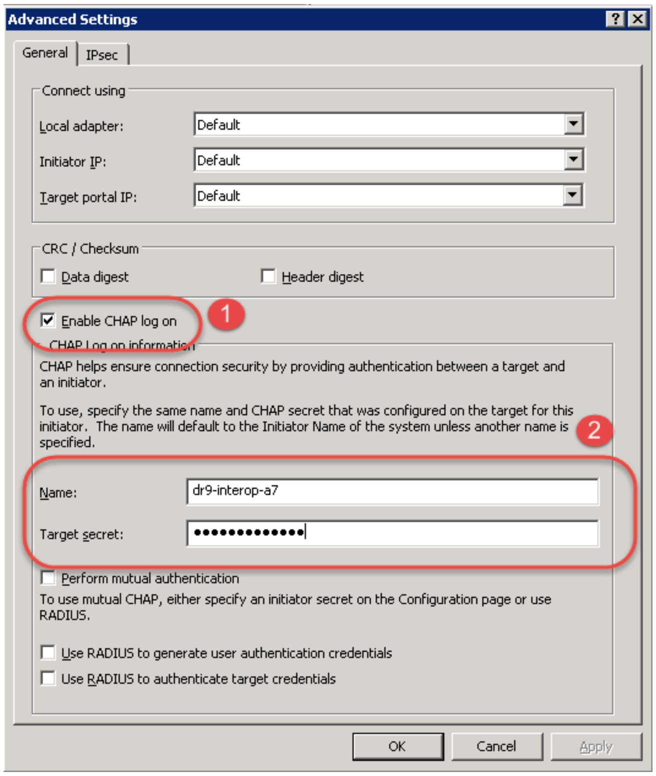
Target name:

iqn.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-pa

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.



Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

□ Data digest □ Header digest

☑ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: dr9-interop-a7

Target secret: ••••••••••••••

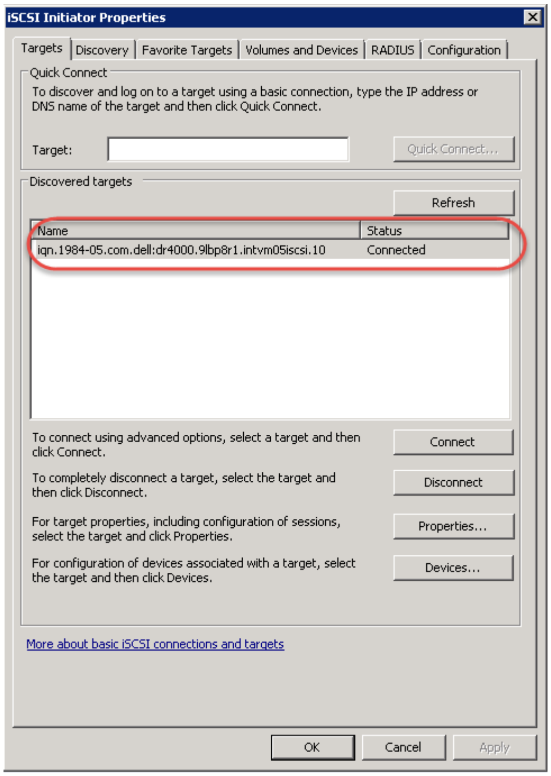
□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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



Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.1984-05.com.dell:dr4000.9lbp8r1.intvm05iscsi.10	Connected

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

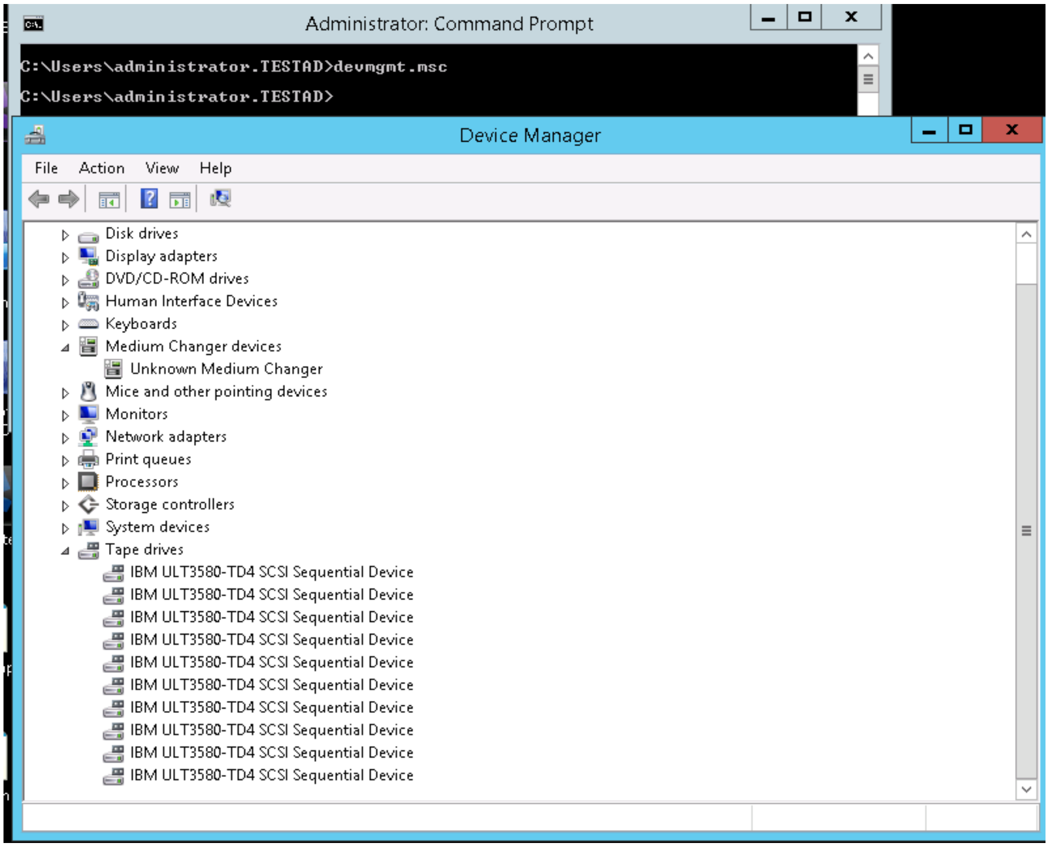
For configuration of devices associated with a target, select the target and then click Devices.

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`

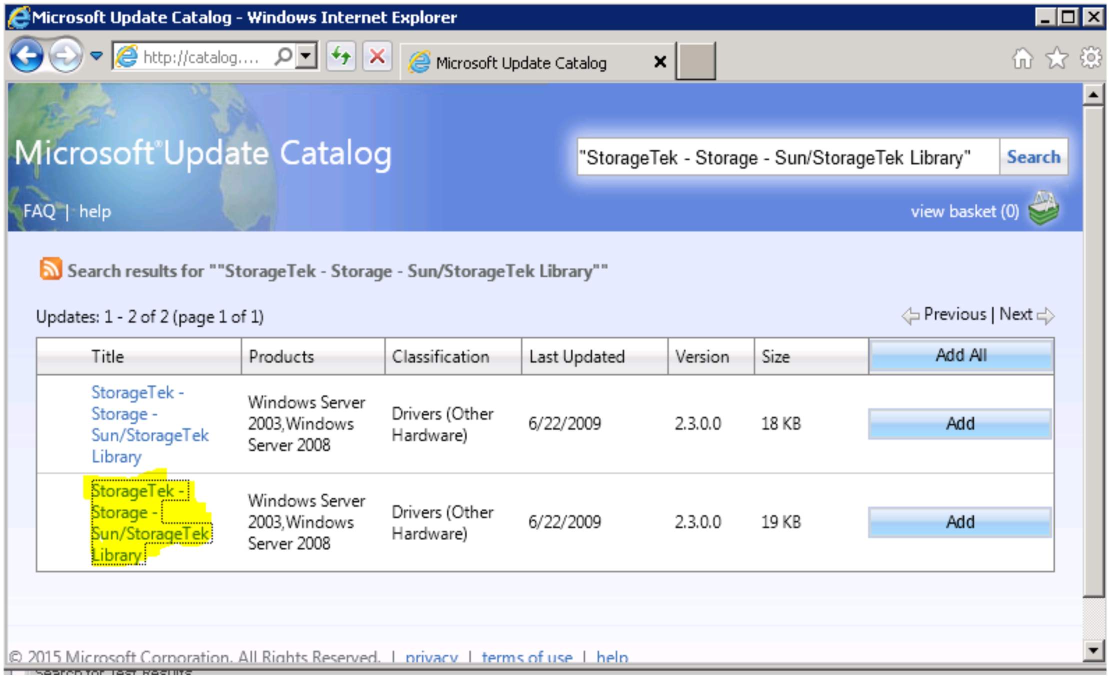
   The DR Series system iSCSI VTL will be listed in the Device Manager as shown in the following screenshot.



```
C:\Users\administrator.TESTAD>devmgmt.msc

C:\Users\administrator.TESTAD>
```

- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Human Interface Devices
- Keyboards
- Medium Changer devices
  - Unknown Medium Changer
- Mice and other pointing devices
- Monitors
- Network adapters
- Print queues
- Processors
- Storage controllers
- System devices
- Tape drives
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device
  - IBM ULT3580-TD4 SCSI Sequential Device

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"



Microsoft Update Catalog - Windows Internet Explorer

Microsoft Update Catalog

"StorageTek - Storage - Sun/StorageTek Library" Search

FAQ | help view basket (0)

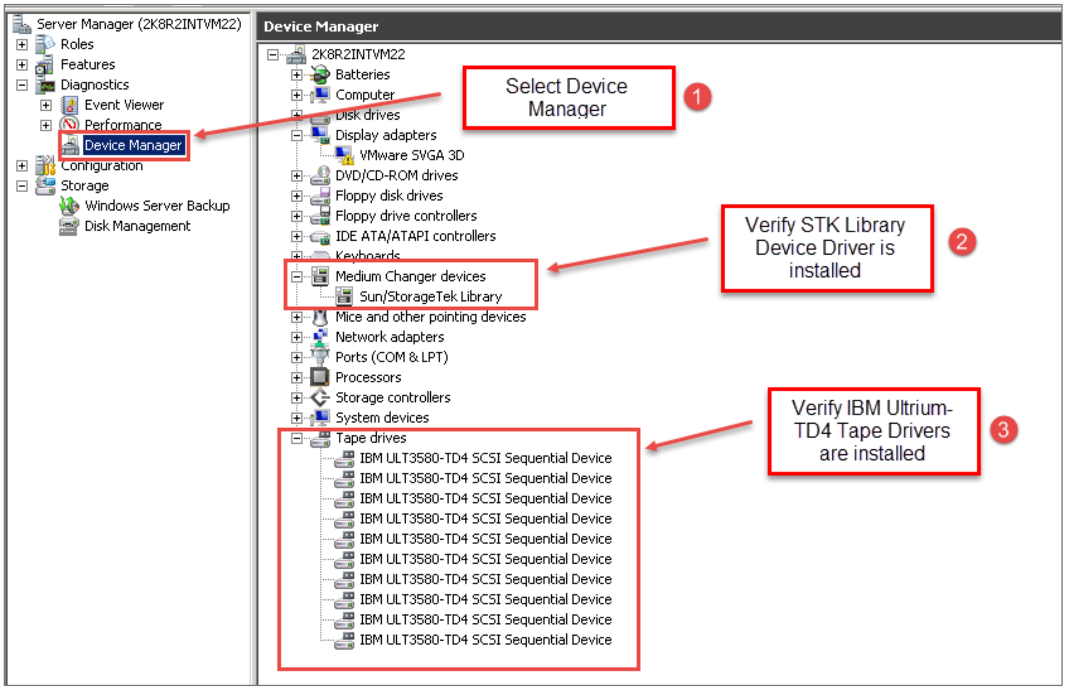
Search results for ""StorageTek - Storage - Sun/StorageTek Library""

Updates: 1 - 2 of 2 (page 1 of 1) Previous | Next

Title	Products	Classification	Last Updated	Version	Size	Add All
StorageTek - Storage - Sun/StorageTek Library	Windows Server 2003,Windows Server 2008	Drivers (Other Hardware)	6/22/2009	2.3.0.0	18 KB	Add
StorageTek - Storage - Sun/StorageTek Library	Windows Server 2003,Windows Server 2008	Drivers (Other Hardware)	6/22/2009	2.3.0.0	19 KB	Add

© 2015 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | help

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.



Server Manager (2K8R2INTVM22)
Roles
Features
Diagnostics
Event Viewer
Performance
Device Manager
Configuration
Storage
Windows Server Backup
Disk Management
Device Manager
2K8R2INTVM22
Batteries
Computer
Disk drives
Display adapters
VMware SVGA 3D
DVD/CD-ROM drives
Floppy disk drives
Floppy drive controllers
IDE ATA/ATAPI controllers
Keyboards
Medium Changer devices
Sun/StorageTek Library
Mice and other pointing devices
Network adapters
Ports (COM & LPT)
Processors
Storage controllers
System devices
Tape drives
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device
IBM ULT3580-TD4 SCSI Sequential Device

Select Device Manager 1

Verify STK Library Device Driver is installed 2

Verify IBM Ultrium-TD4 Tape Drivers are installed 3

4. 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

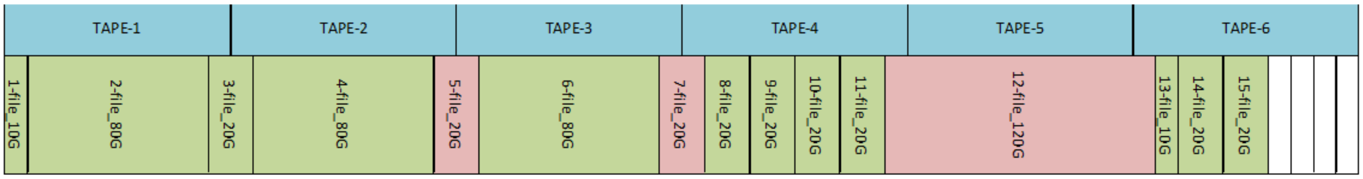
   - Windows 2008 R2 SP1 - IBMTape.x64_w08_6250
   - Windows 2012 R2 - IBMTape.x64_w12R2_6248_WHQL_Cert

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

5. 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.

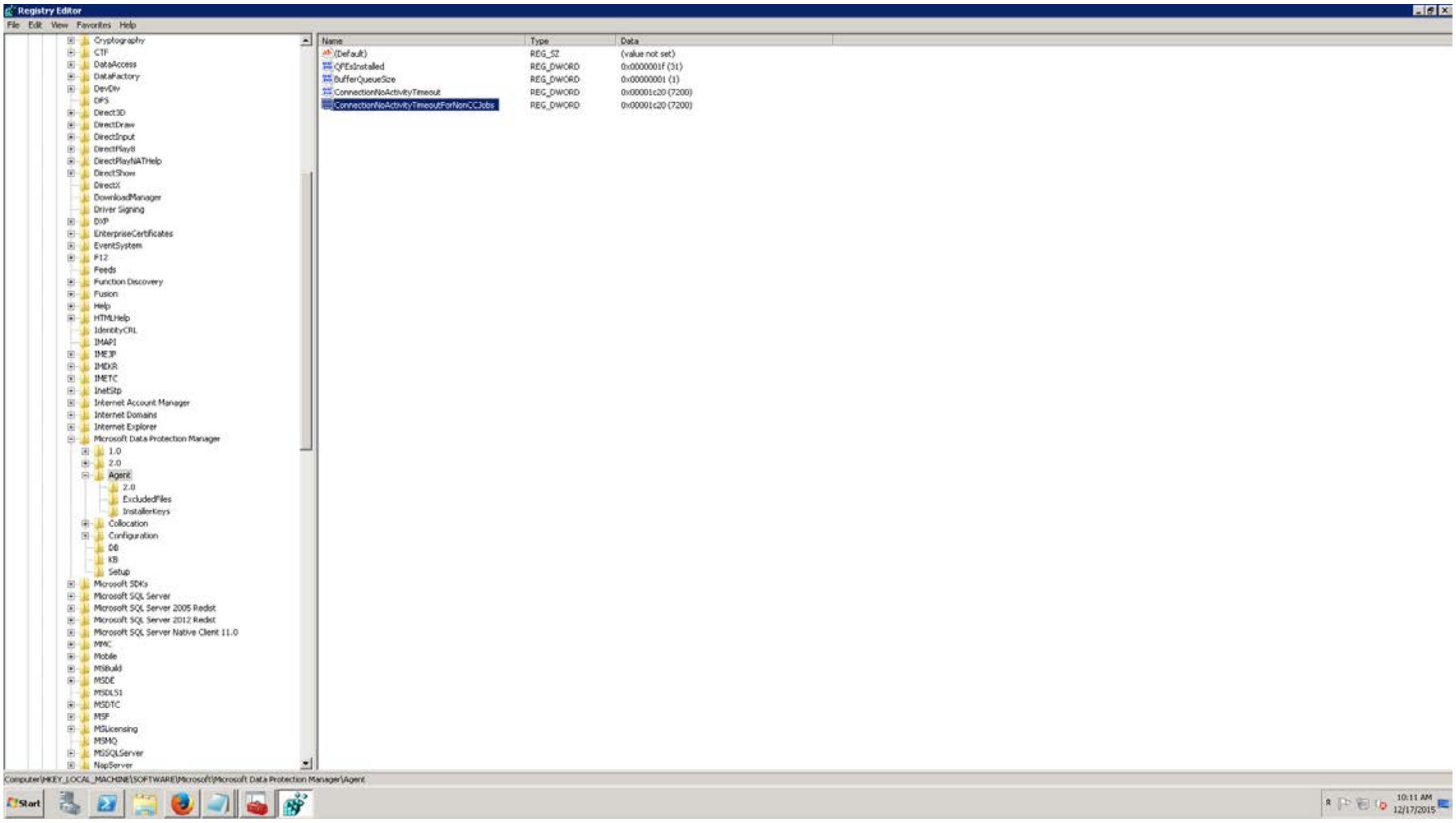
Registry Setting	Value to add/edit
Set BufferQueueSize	1
Set ConnectionNoActivityTimeout and ConnectionNoActivityTimeoutForNonCCJobs	7200
TapeSize	Add this parameter
Storport key	Add for each tape
BusyRetryCount	Add for each tape
TUR	Disable
Service_Name	Add the AutoRun value

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**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
QFEsInstalled	REG_DWORD	0x0000001f (31)
BufferQueueSize	REG_DWORD	0x00000001 (1)
ConnectionNoActivityTimeout	REG_DWORD	0x00001c20 (7200)
ConnectionNoActivityTimeoutForNonCCJobs	REG_DWORD	0x00001c20 (7200)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent

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`

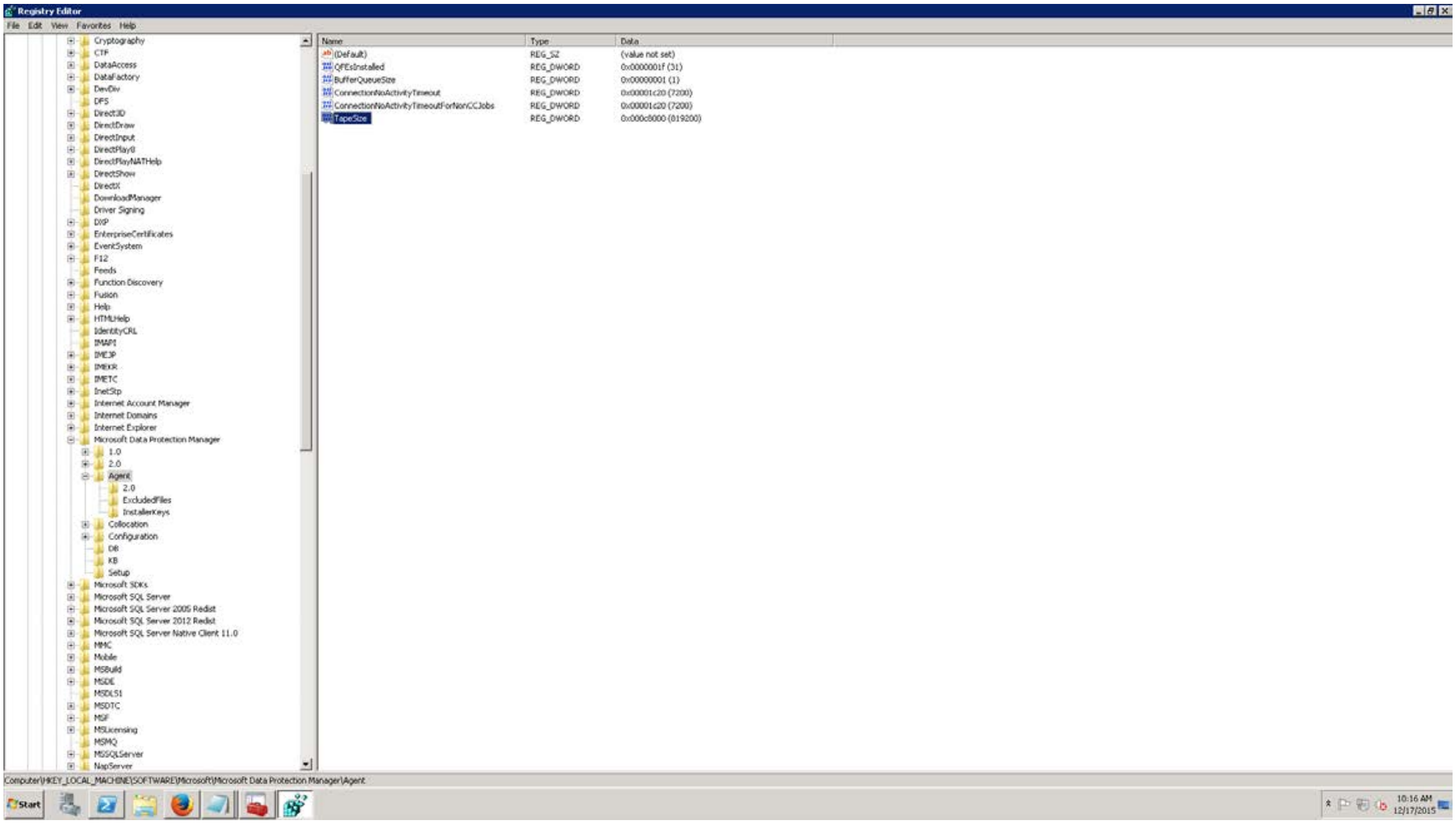
2. In the Registry Editor, go to the following path:
   `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent`

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.



Name	Type	Data
(Default)	REG_SZ	(value not set)
QFEsInstalled	REG_DWORD	0x0000001f (31)
BufferQueueSize	REG_DWORD	0x00000001 (1)
ConnectionNoActivityTimeout	REG_DWORD	0x00001c20 (7200)
ConnectionNoActivityTimeoutForNonCCJobs	REG_DWORD	0x00001c20 (7200)
TapeSize	REG_DWORD	0x000c8000 (819200)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent

3.4.3 Adding the Storport key and BusyRetryCount parameter for each tape

Follow these steps.

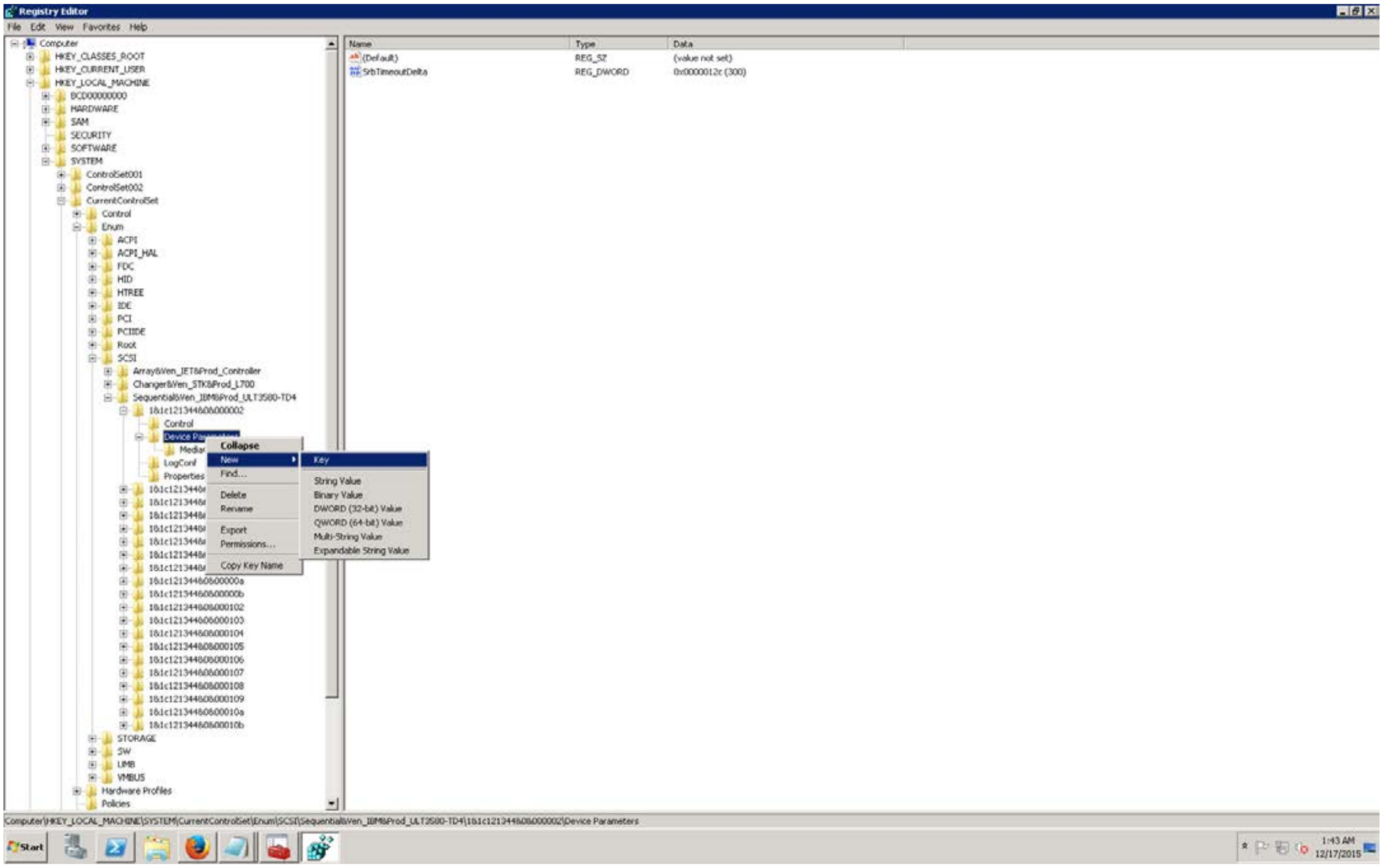
1. To add the Storport key, go to the following path:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI\<DEVICEID>\<INSTANCE>\DeviceParameters`

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.

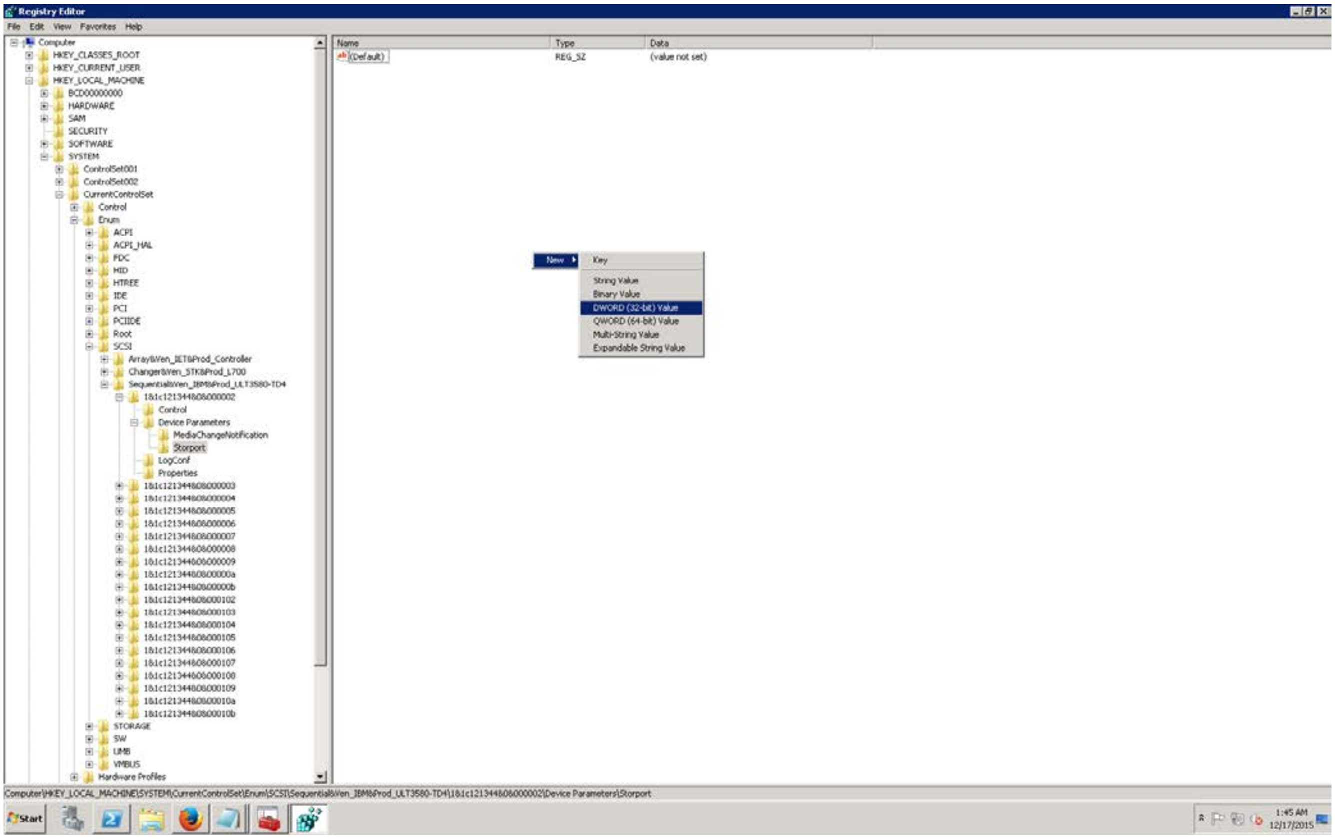
3. Right-click **DeviceParameters**, select **New > Key**, and change NewKey as **Storport.**



Name	Type	Data
(Default)	REG_SZ	(value not set)
SrbTimeoutDelta	REG_DWORD	0x0000012c (300)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SCSI\Sequential&Ven_IBM&Prod_ULT3580-TD4\1&1c121344&0&000002\Device Parameters

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



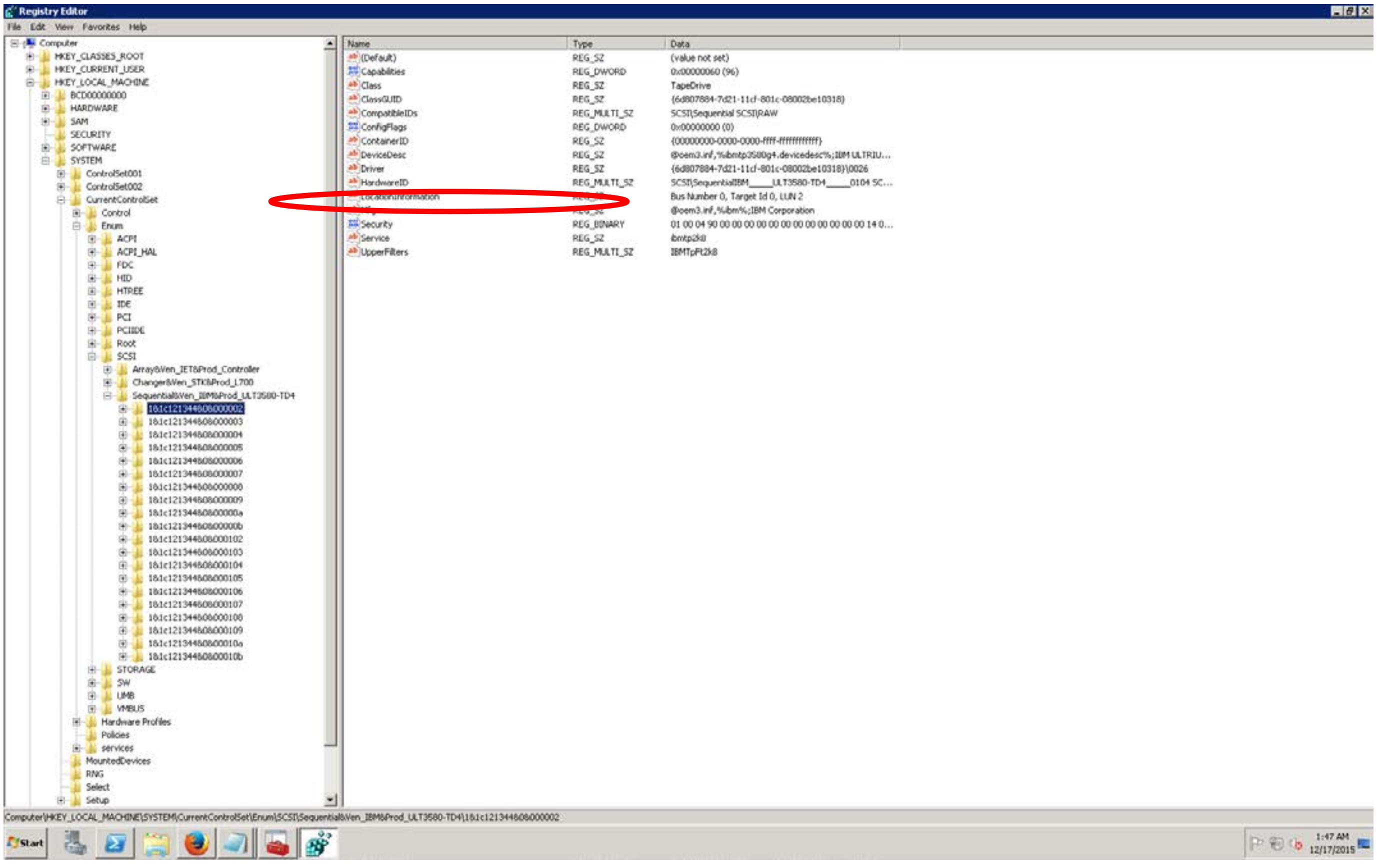
Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SCSI\Sequential&Ven_IBM&Prod_ULT3580-TD4\1&1c121344&0&000002\Device Parameters\Storport

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>



```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ControlSet001
      ControlSet002
      CurrentControlSet
        Control
        Enum
          ACPI
          ACPI_HAL
          FDC
          HID
          HTREE
          IDE
          PCI
          PCIIDE
          Root
          SCSI
            Array&Ven_IET&Prod_Controller
            Changer&Ven_STK&Prod_L700
            Sequential&Ven_IBM&Prod_ULT3580-TD4
              1&1c121344808000002
              1&1c121344808000003
              1&1c121344808000004
              1&1c121344808000005
              1&1c121344808000006
              1&1c121344808000007
              1&1c121344808000008
              1&1c121344808000009
              1&1c12134480800000a
              1&1c12134480800000b
              1&1c121344808000102
              1&1c121344808000103
              1&1c121344808000104
              1&1c121344808000105
              1&1c121344808000106
              1&1c121344808000107
              1&1c121344808000108
              1&1c121344808000109
              1&1c12134480800010a
              1&1c12134480800010b
          STORAGE
          SW
          UMB
          VMBUS
        Hardware Profiles
        Policies
        services
      MountedDevices
      RNG
      Select
      Setup
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000060 (96)
Class	REG_SZ	TapeDrive
ClassGUID	REG_SZ	{6d807884-7d21-11cf-801c-08002be10318}
CompatibleIDs	REG_MULTI_SZ	SCSI\Sequential SCSI\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffffff}
DeviceDesc	REG_SZ	@oem3.inf,%ibmtp3580g4.devicedesc%;IBM ULTRIU...
Driver	REG_SZ	{6d807884-7d21-11cf-801c-08002be10318}\0026
HardwareID	REG_MULTI_SZ	SCSI\SequentialIBM_____ULT3580-TD4_____0104 SC...
LocationInformation	REG_SZ	Bus Number 0, Target Id 0, LUN 2
Mfg	REG_SZ	@oem3.inf,%ibm%;IBM Corporation
Security	REG_BINARY	01 00 04 90 00 00 00 00 00 00 00 00 00 00 00 00 14 0...
Service	REG_SZ	ibmtp2k8
UpperFilters	REG_MULTI_SZ	IBMTpFlt2k8

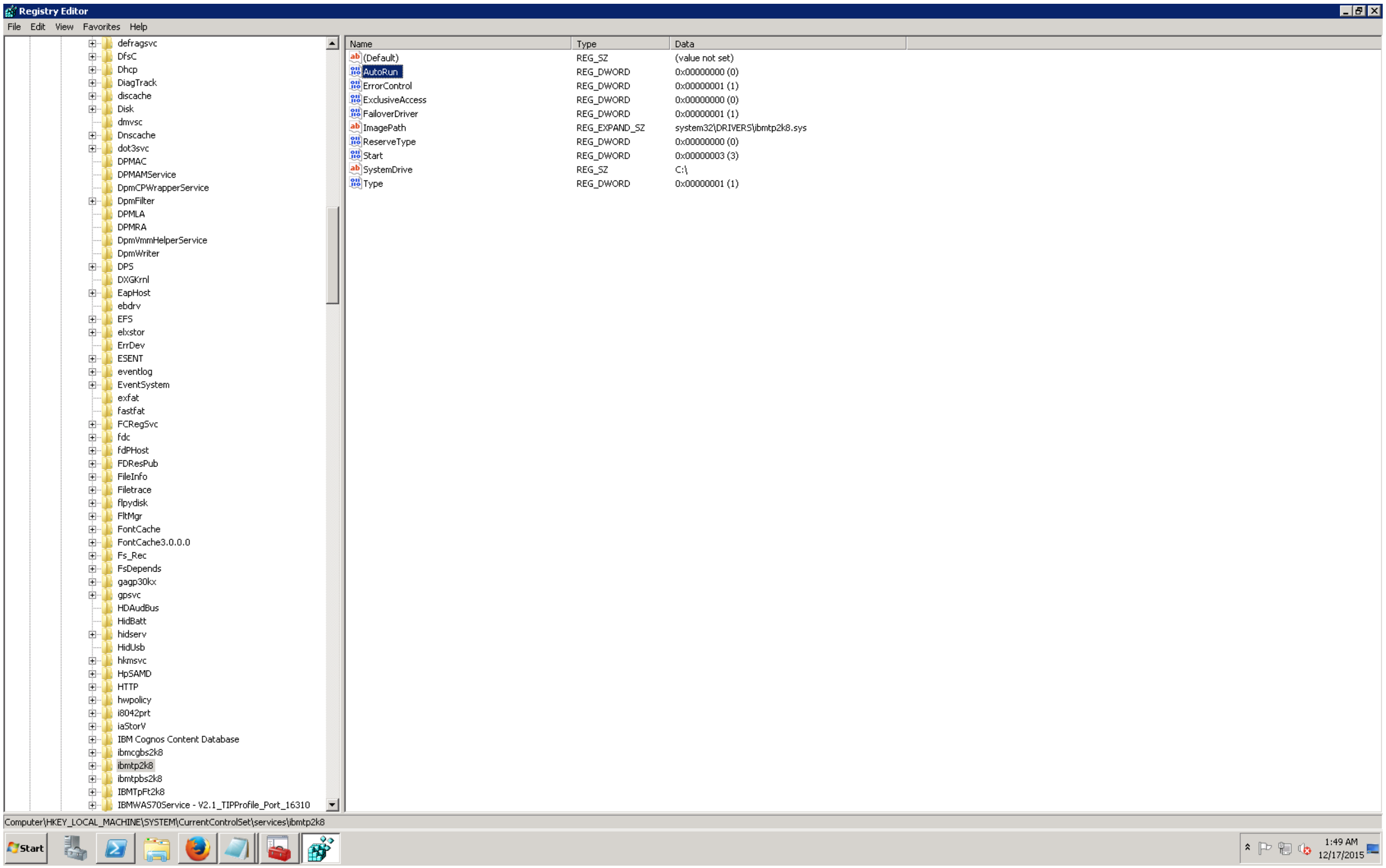
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SCSI\Sequential&Ven_IBM&Prod_ULT3580-TD4\1&1c121344808000002

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

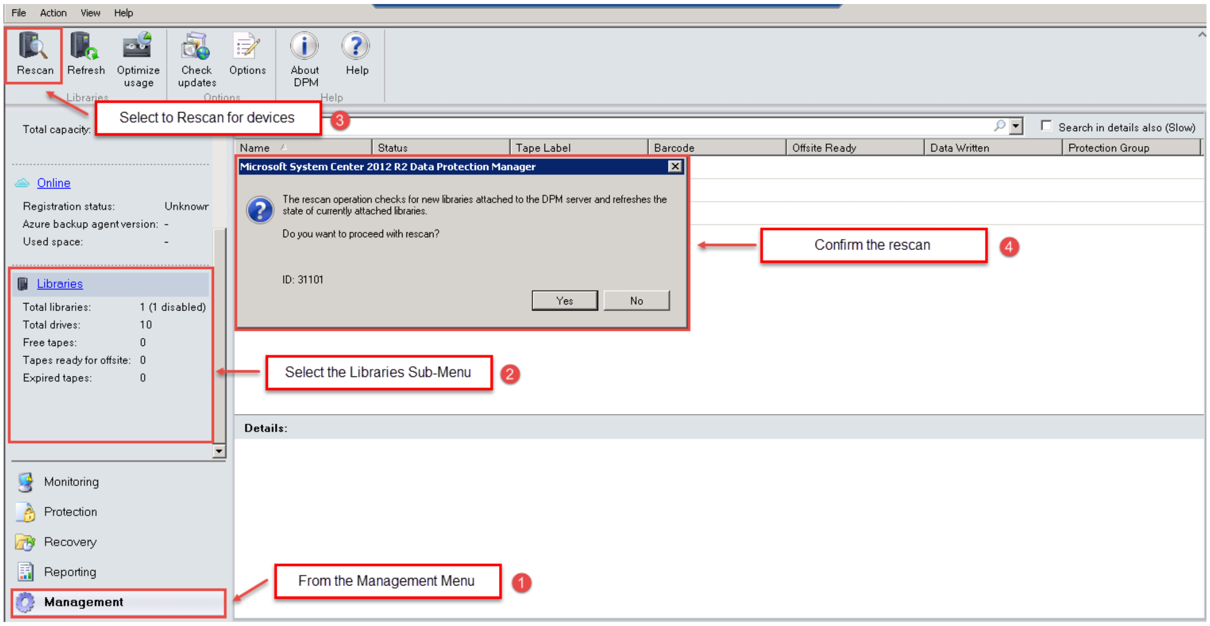


Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoRun	REG_DWORD	0x00000000 (0)
ErrorControl	REG_DWORD	0x00000001 (1)
ExclusiveAccess	REG_DWORD	0x00000000 (0)
FailoverDriver	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	system32\DRIVERS\ibmtp2k8.sys
ReserveType	REG_DWORD	0x00000000 (0)
Start	REG_DWORD	0x00000003 (3)
SystemDrive	REG_SZ	C:\
Type	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ibmtp2k8

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**.



Total capacity:

Online

Registration status: Unknowr

Azure backup agent version: -

Used space: -

Libraries

Total libraries: 1 (1 disabled)

Total drives: 10

Free tapes: 0

Tapes ready for offsite: 0

Expired tapes: 0

Microsoft System Center 2012 R2 Data Protection Manager

The rescan operation checks for new libraries attached to the DPM server and refreshes the state of currently attached libraries.

Do you want to proceed with rescan?

ID: 31101

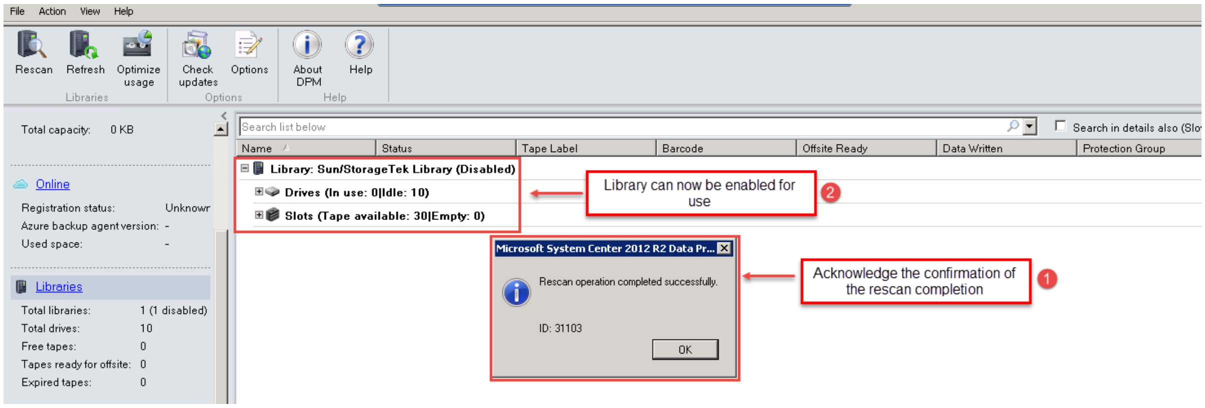
1 From the Management Menu

2 Select the Libraries Sub-Menu

3 Select to Rescan for devices

4 Confirm the rescan

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.



Total capacity: 0 KB

Online

Registration status: Unknowr

Azure backup agent version: -

Used space: -

Libraries

Total libraries: 1 (1 disabled)

Total drives: 10

Free tapes: 0

Tapes ready for offsite: 0

Expired tapes: 0

Library: Sun/StorageTek Library (Disabled)

Drives (In use: 0|Idle: 10)

Slots (Tape available: 30|Empty: 0)

Microsoft System Center 2012 R2 Data Pr...

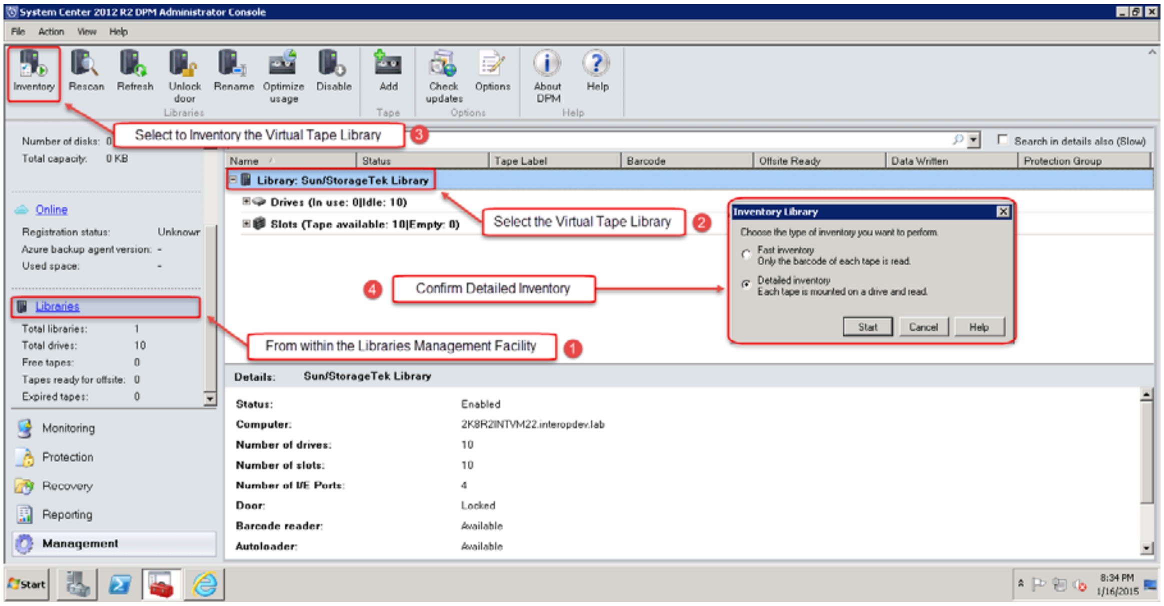
Rescan operation completed successfully.

ID: 31103

1 Acknowledge the confirmation of the rescan completion

2 Library can now be enabled for use

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.



1. From within the Libraries Management Facility
2. Select the Virtual Tape Library
3. Select to Inventory the Virtual Tape Library
4. Confirm Detailed Inventory

Number of disks: 0
Total capacity: 0 KB

Online
Registration status: Unknown
Azure backup agent version: -
Used space: -

Libraries
Total libraries: 1
Total drives: 10
Free tapes: 0
Tapes ready for offsite: 0
Expired tapes: 0

☐ Search in details also (Slow)

Name	Status	Tape Label	Barcode	Offsite Ready	Data Written	Protection Group
Library: Sun/StorageTek Library						
Drives (In use: 0|Idle: 10)						
Slots (Tape available: 10|Empty: 0)						

Inventory Library

Choose the type of inventory you want to perform.

○ Fast inventory
Only the barcode of each tape is read.

● Detailed inventory
Each tape is mounted on a drive and read.

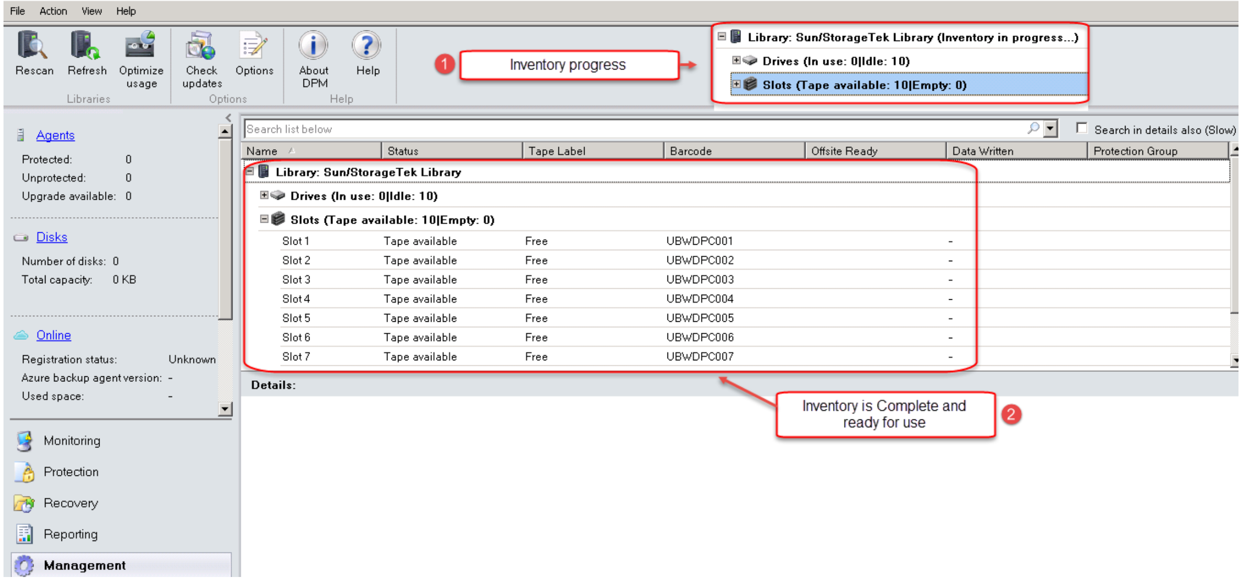
Start Cancel Help

Details: Sun/StorageTek Library

Status: Enabled
Computer: 2K8R2INTVM22.interopdev.lab
Number of drives: 10
Number of slots: 10
Number of I/E Ports: 4
Door: Locked
Barcode reader: Available
Autoloader: Available

8:34 PM
1/16/2015

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



1. Inventory progress
2. Inventory is Complete and ready for use

Library: Sun/StorageTek Library (Inventory in progress...)
Drives (In use: 0|Idle: 10)
Slots (Tape available: 10|Empty: 0)

Agents
Protected: 0
Unprotected: 0
Upgrade available: 0

Disks
Number of disks: 0
Total capacity: 0 KB

Online
Registration status: Unknown
Azure backup agent version: -
Used space: -

Search list below
☐ Search in details also (Slow)

Name	Status	Tape Label	Barcode	Offsite Ready	Data Written	Protection Group
Library: Sun/StorageTek Library						
Drives (In use: 0|Idle: 10)						
Slots (Tape available: 10|Empty: 0)						
Slot 1	Tape available	Free	UBWDPC001	-		
Slot 2	Tape available	Free	UBWDPC002	-		
Slot 3	Tape available	Free	UBWDPC003	-		
Slot 4	Tape available	Free	UBWDPC004	-		
Slot 5	Tape available	Free	UBWDPC005	-		
Slot 6	Tape available	Free	UBWDPC006	-		
Slot 7	Tape available	Free	UBWDPC007	-		

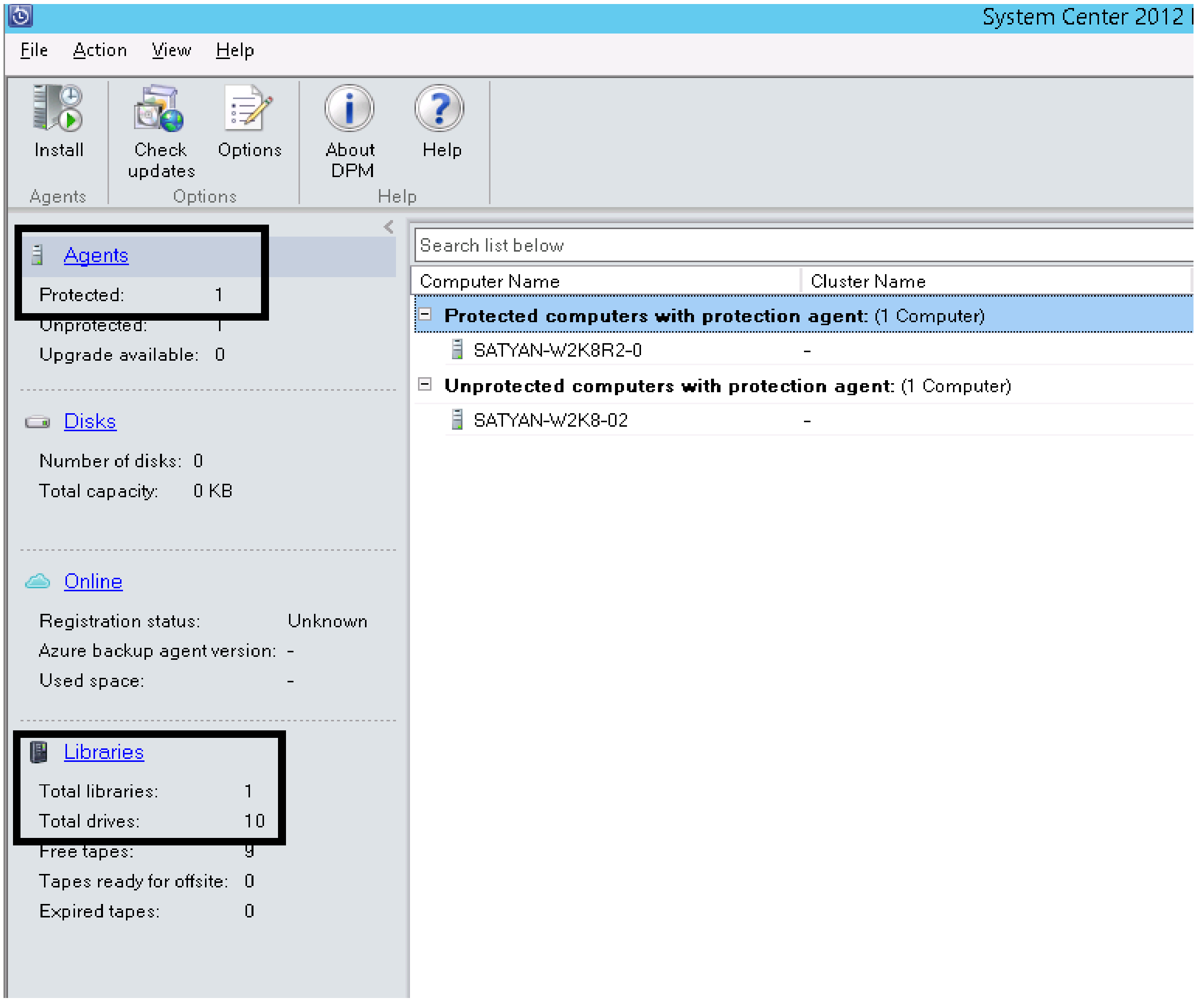
Details:

5. You should reboot the system for registry settings to take effect.

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.



Agents

Protected: 1

Unprotected: 1

Upgrade available: 0

Disks

Number of disks: 0

Total capacity: 0 KB

Online

Registration status: Unknown

Azure backup agent version: -

Used space: -

Libraries

Total libraries: 1

Total drives: 10

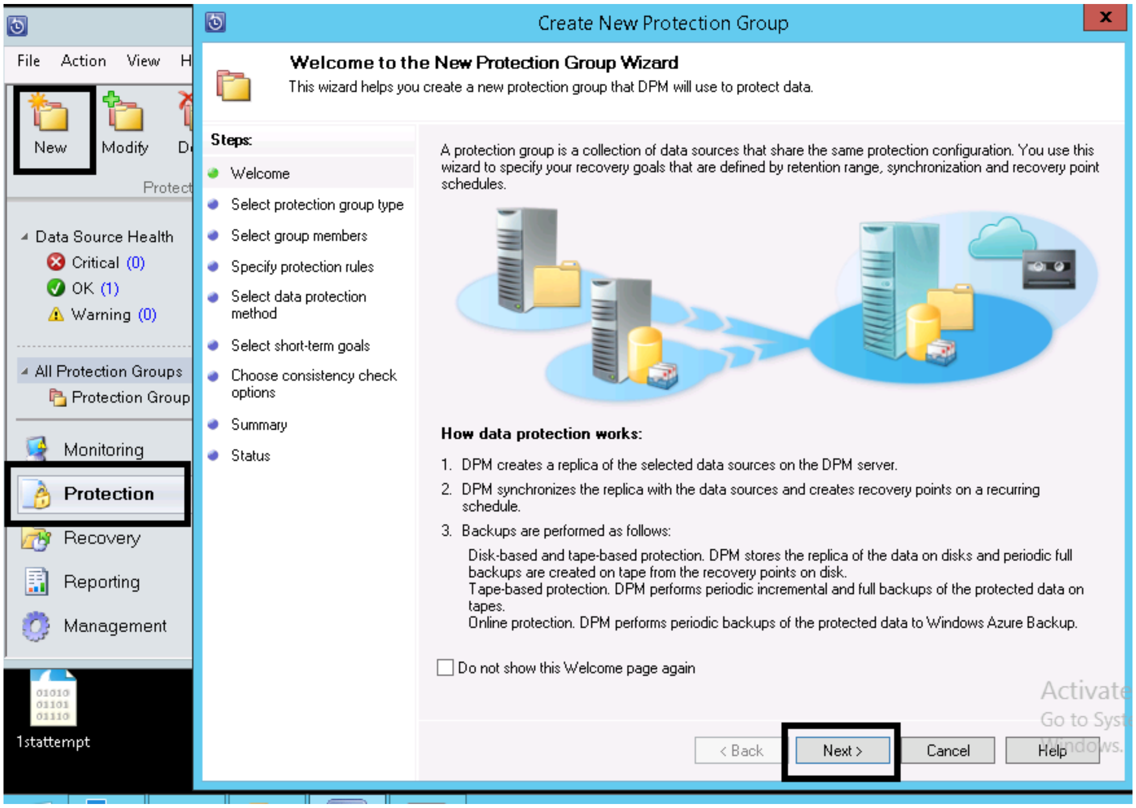
Free tapes: 9

Tapes ready for offsite: 0

Expired tapes: 0

Computer Name	Cluster Name
Protected computers with protection agent: (1 Computer)	
SATYAN-W2K8R2-0	-
Unprotected computers with protection agent: (1 Computer)	
SATYAN-W2K8-02	-

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



Welcome to the New Protection Group Wizard

This wizard helps you create a new protection group that DPM will use to protect data.

A protection group is a collection of data sources that share the same protection configuration. You use this wizard to specify your recovery goals that are defined by retention range, synchronization and recovery point schedules.

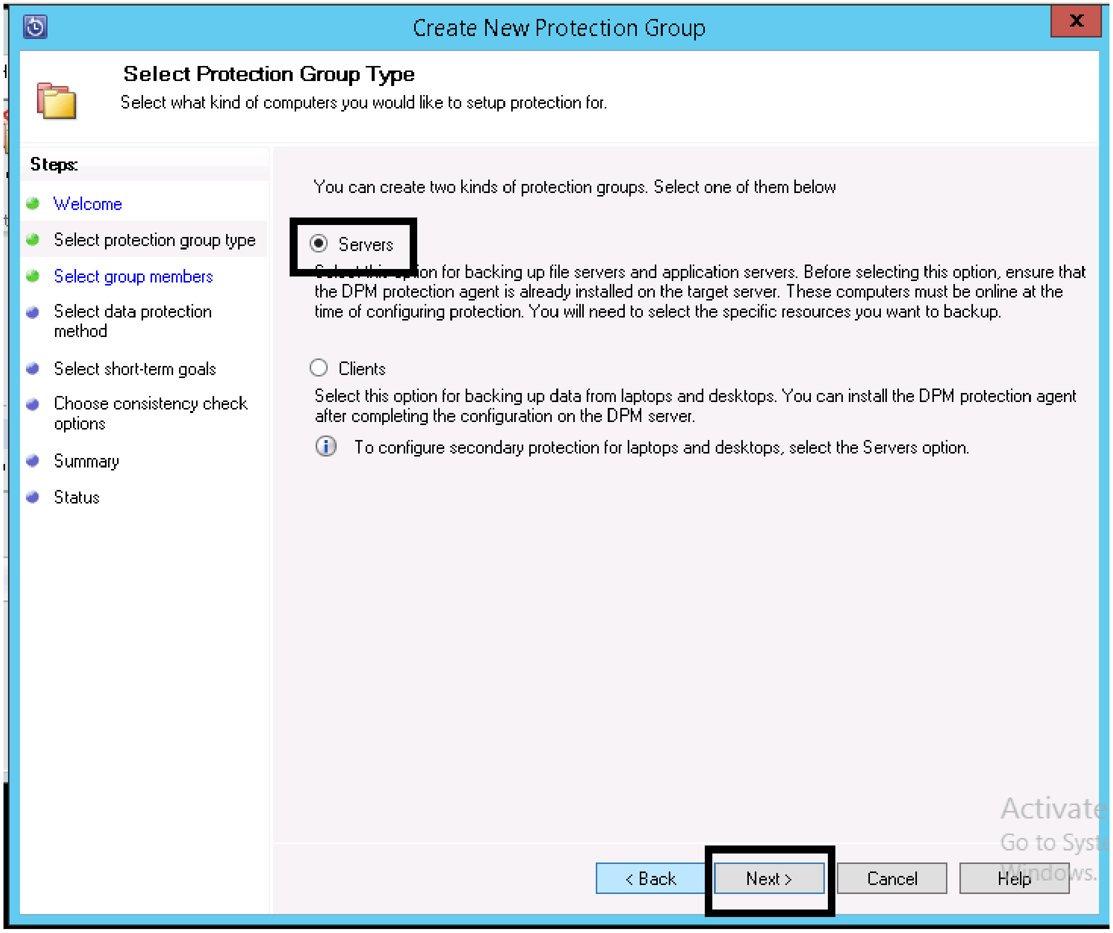
How data protection works:

1. DPM creates a replica of the selected data sources on the DPM server.
2. DPM synchronizes the replica with the data sources and creates recovery points on a recurring schedule.
3. Backups are performed as follows:

   Disk-based and tape-based protection. DPM stores the replica of the data on disks and periodic full backups are created on tape from the recovery points on disk.
   Tape-based protection. DPM performs periodic incremental and full backups of the protected data on tapes.
   Online protection. DPM performs periodic backups of the protected data to Windows Azure Backup.

☐ Do not show this Welcome page again

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



Create New Protection Group

Select Protection Group Type

Select what kind of computers you would like to setup protection for.

Steps:
Welcome
Select protection group type
Select group members
Select data protection method
Select short-term goals
Choose consistency check options
Summary
Status

You can create two kinds of protection groups. Select one of them below

● Servers

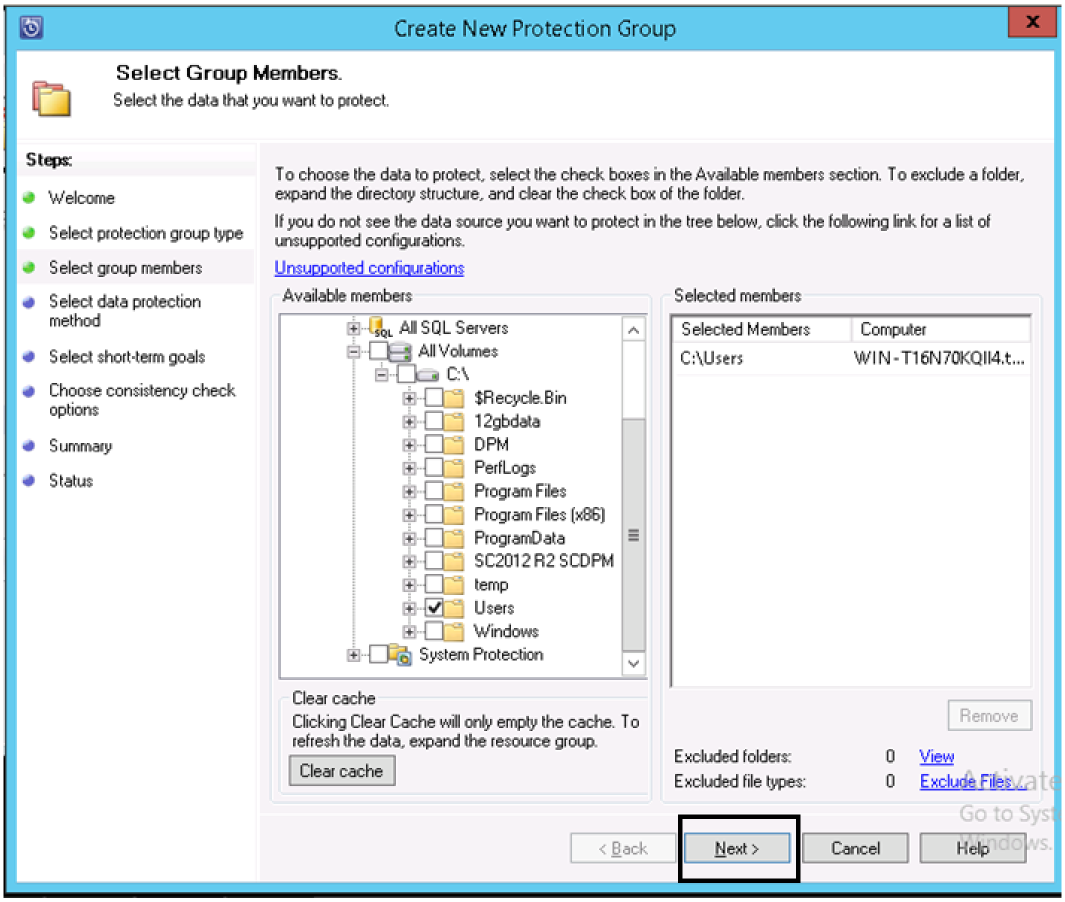
Select this option for backing up file servers and application servers. Before selecting this option, ensure that the DPM protection agent is already installed on the target server. These computers must be online at the time of configuring protection. You will need to select the specific resources you want to backup.

○ Clients

Select this option for backing up data from laptops and desktops. You can install the DPM protection agent after completing the configuration on the DPM server.

To configure secondary protection for laptops and desktops, select the Servers option.

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



Select Group Members.

Select the data that you want to protect.

To choose the data to protect, select the check boxes in the Available members section. To exclude a folder, expand the directory structure, and clear the check box of the folder.

If you do not see the data source you want to protect in the tree below, click the following link for a list of unsupported configurations.

Unsupported configurations

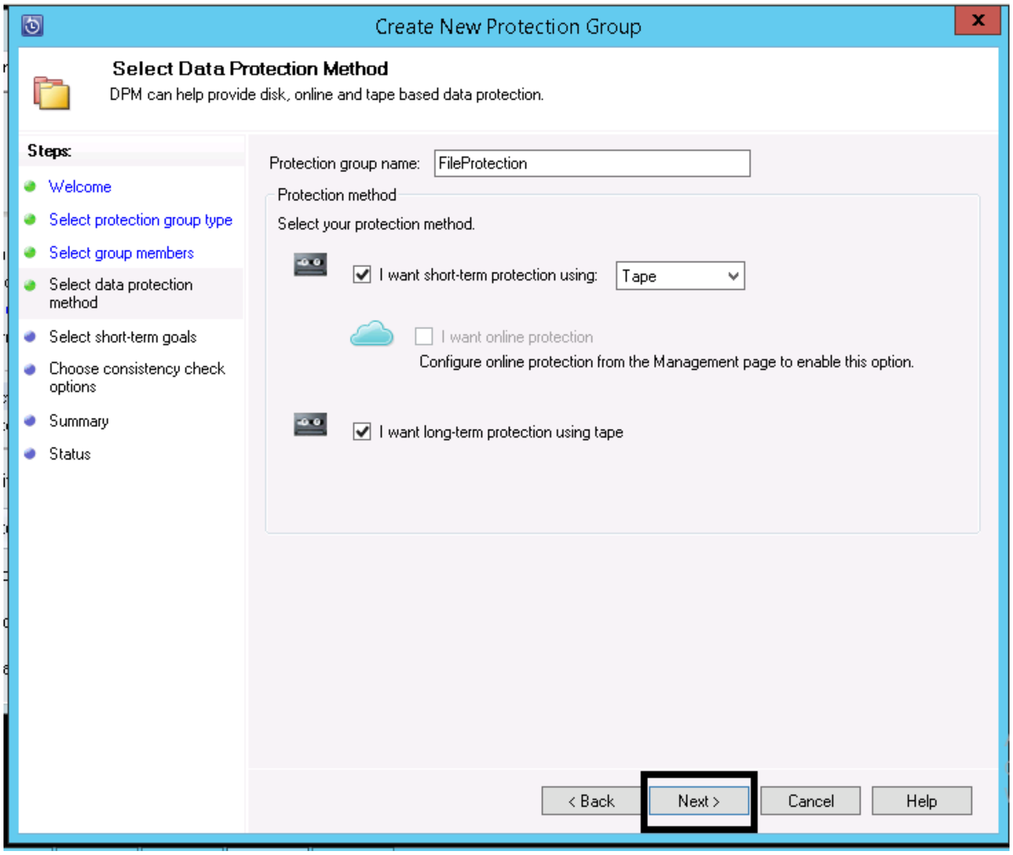
☑ Users

Selected Members	Computer
C:\Users	WIN-T16N70KQII4.t...

Clicking Clear Cache will only empty the cache. To refresh the data, expand the resource group.

Excluded folders:	0	View
Excluded file types:	0	Exclude Files...

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**.



Create New Protection Group
Select Data Protection Method
DPM can help provide disk, online and tape based data protection.
Steps:
Welcome
Select protection group type
Select group members
Select data protection method
Select short-term goals
Choose consistency check options
Summary
Status
< Back
Next >
Cancel
Help

Protection group name: FileProtection

Protection method

Select your protection method.

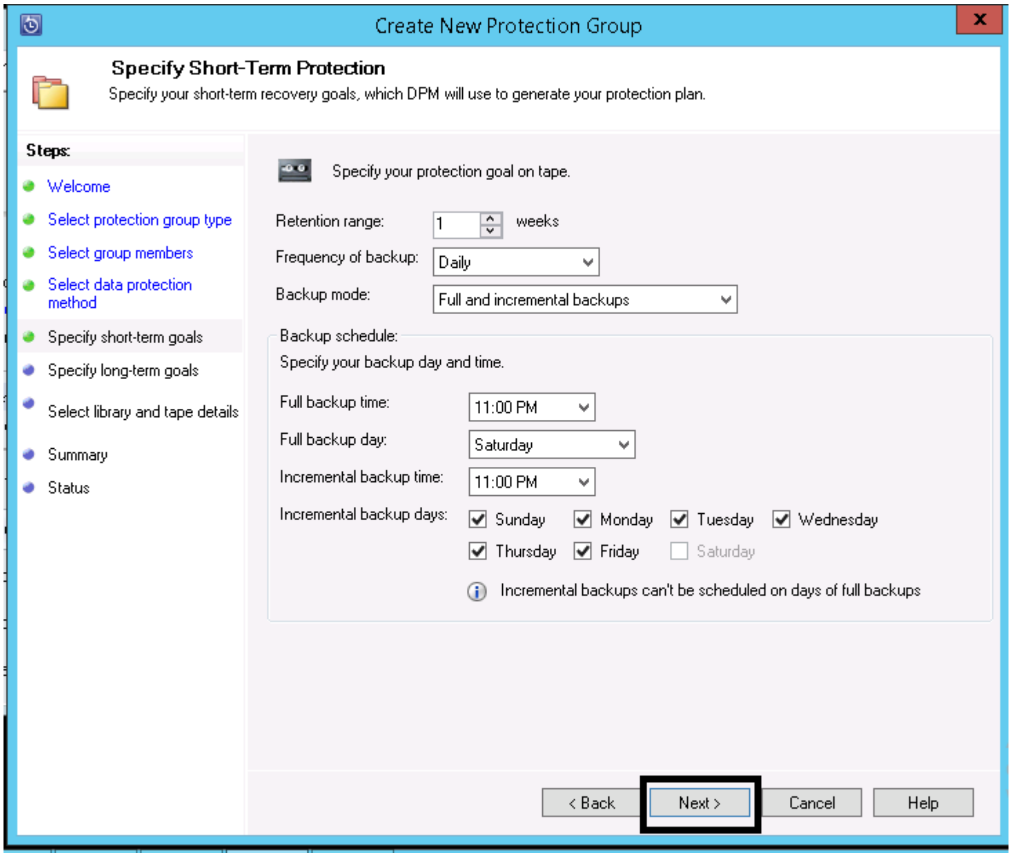
☑ I want short-term protection using: Tape

□ I want online protection

Configure online protection from the Management page to enable this option.

☑ I want long-term protection using tape

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



Create New Protection Group

Specify Short-Term Protection

Specify your short-term recovery goals, which DPM will use to generate your protection plan.

Steps:

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Specify short-term goals
- Specify long-term goals
- Select library and tape details
- Summary
- Status

Specify your protection goal on tape.

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

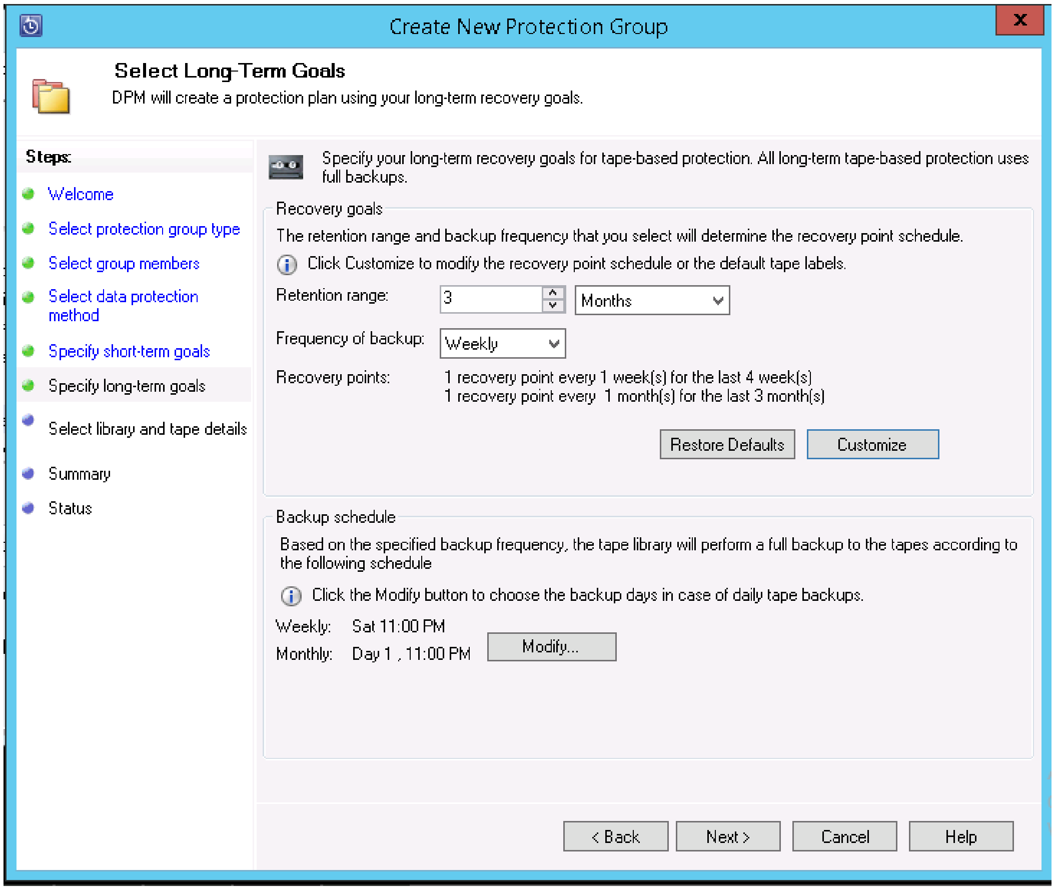
Full backup day: Saturday

Incremental backup time: 11:00 PM

Incremental backup days: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday

Incremental backups can't be scheduled on days of full backups

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



Create New Protection Group

Select Long-Term Goals

DPM will create a protection plan using your long-term recovery goals.

Specify your long-term recovery goals for tape-based protection. All long-term tape-based protection uses full backups.

Recovery goals

The retention range and backup frequency that you select will determine the recovery point schedule.

Click Customize to modify the recovery point schedule or the default tape labels.

Retention range: 3 Months

Frequency of backup: Weekly

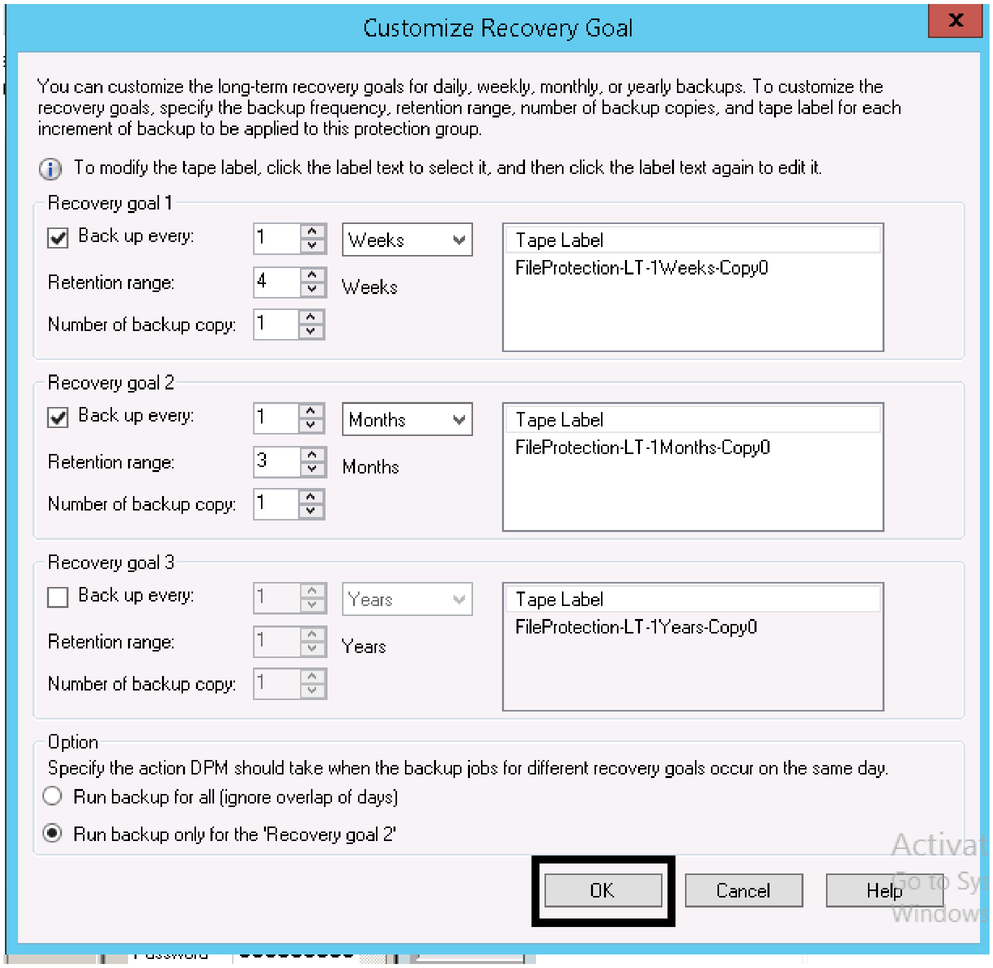
Recovery points: 1 recovery point every 1 week(s) for the last 4 week(s)
1 recovery point every 1 month(s) for the last 3 month(s)

Backup schedule

Based on the specified backup frequency, the tape library will perform a full backup to the tapes according to the following schedule

Click the Modify button to choose the backup days in case of daily tape backups.

Weekly: Sat 11:00 PM
Monthly: Day 1 , 11:00 PM



Customize Recovery Goal

You can customize the long-term recovery goals for daily, weekly, monthly, or yearly backups. To customize the recovery goals, specify the backup frequency, retention range, number of backup copies, and tape label for each increment of backup to be applied to this protection group.

To modify the tape label, click the label text to select it, and then click the label text again to edit it.

Recovery goal 1
☑ Back up every: 1 Weeks
Retention range: 4 Weeks
Number of backup copy: 1
Tape Label: FileProtection-LT-1Weeks-Copy0

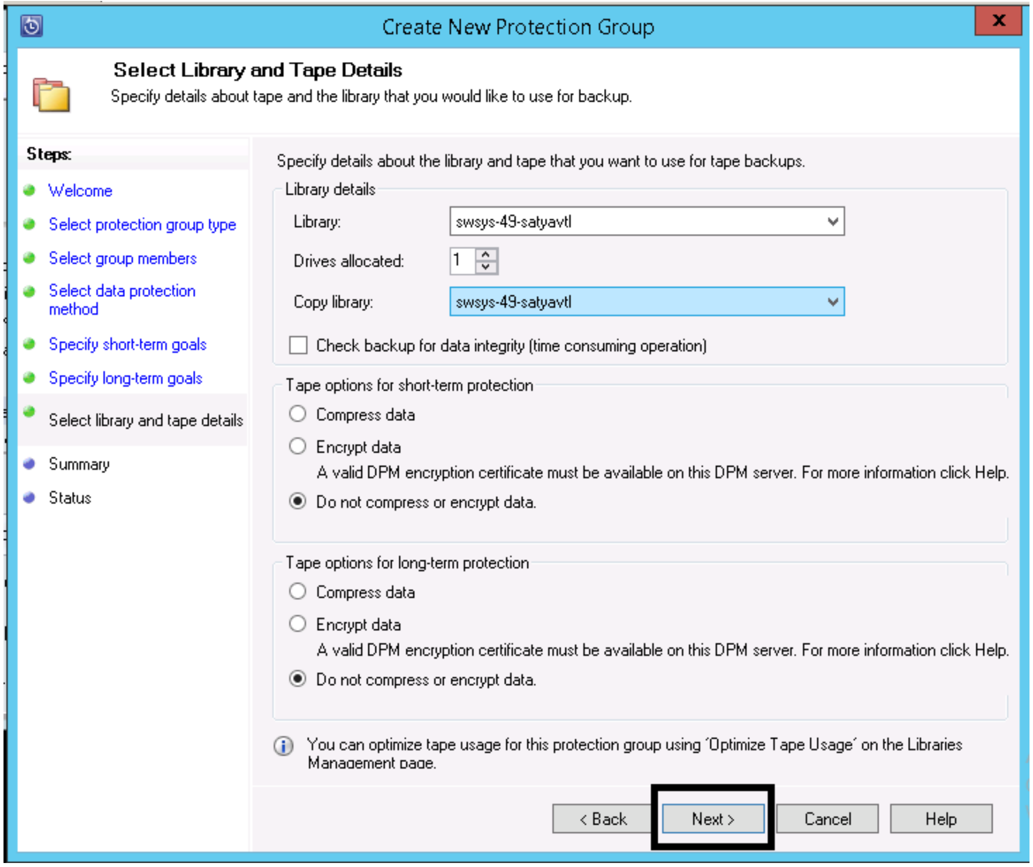
Recovery goal 2
☑ Back up every: 1 Months
Retention range: 3 Months
Number of backup copy: 1
Tape Label: FileProtection-LT-1Months-Copy0

Recovery goal 3
□ Back up every: 1 Years
Retention range: 1 Years
Number of backup copy: 1
Tape Label: FileProtection-LT-1Years-Copy0

Option
Specify the action DPM should take when the backup jobs for different recovery goals occur on the same day.
○ Run backup for all (ignore overlap of days)
● Run backup only for the 'Recovery goal 2'

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.



Create New Protection Group

Select Library and Tape Details

Specify details about tape and the library that you would like to use for backup.

Specify details about the library and tape that you want to use for tape backups.

Library details

Library: swsys-49-satyavtl

Drives allocated: 1

Copy library: swsys-49-satyavtl

□ Check backup for data integrity (time consuming operation)

Tape options for short-term protection

○ Compress data

○ Encrypt data

A valid DPM encryption certificate must be available on this DPM server. For more information click Help.

● Do not compress or encrypt data.

Tape options for long-term protection

○ Compress data

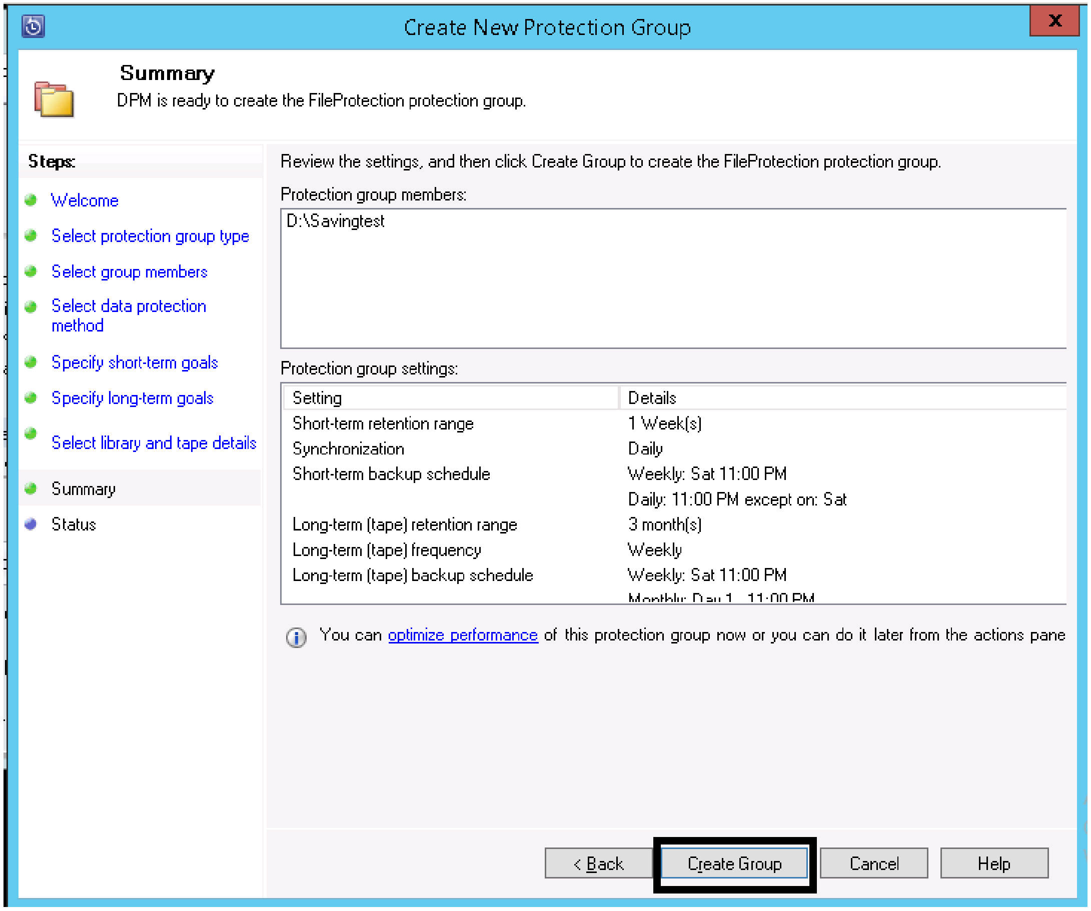
○ Encrypt data

A valid DPM encryption certificate must be available on this DPM server. For more information click Help.

● Do not compress or encrypt data.

You can optimize tape usage for this protection group using 'Optimize Tape Usage' on the Libraries Management page.

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



Create New Protection Group

Summary

DPM is ready to create the FileProtection protection group.

Review the settings, and then click Create Group to create the FileProtection protection group.

Protection group members:

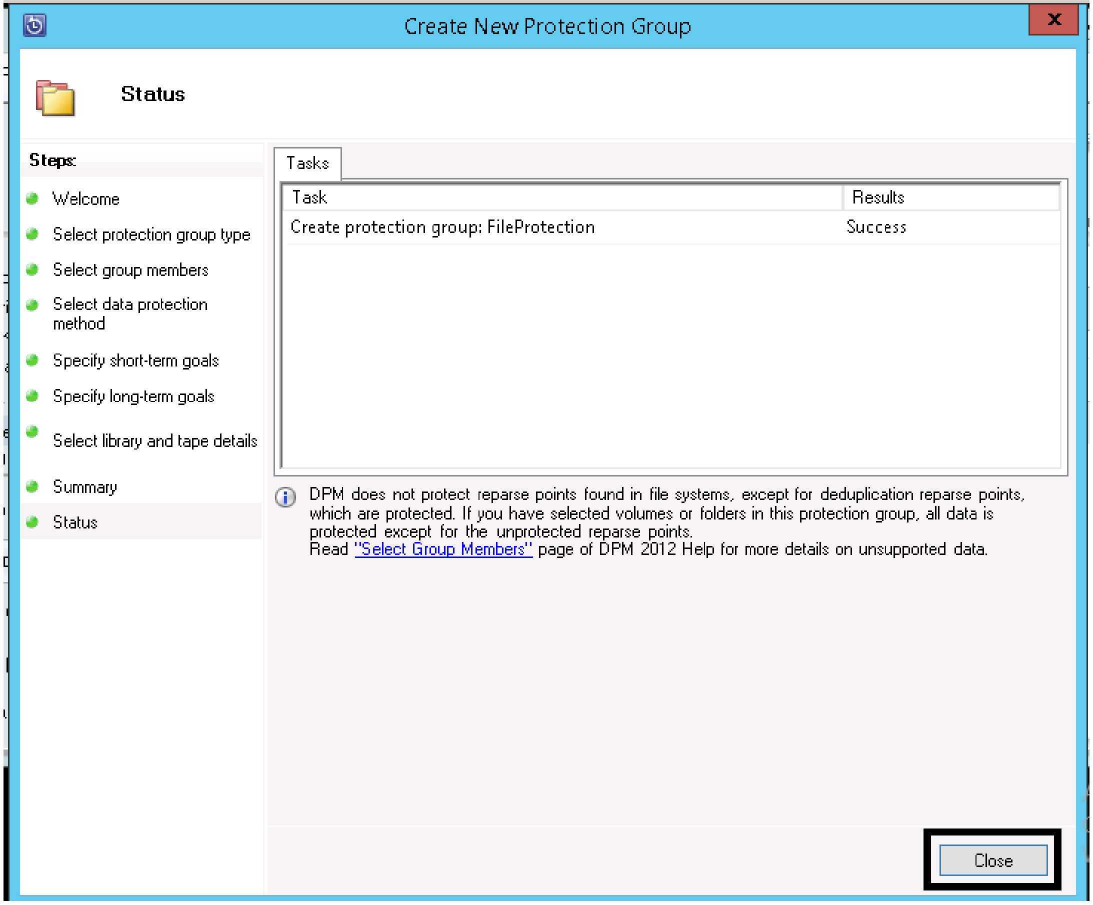
D:\Savingtest

Protection group settings:

Setting	Details
Short-term retention range	1 Week(s)
Synchronization	Daily
Short-term backup schedule	Weekly: Sat 11:00 PM Daily: 11:00 PM except on: Sat
Long-term (tape) retention range	3 month(s)
Long-term (tape) frequency	Weekly
Long-term (tape) backup schedule	Weekly: Sat 11:00 PM Monthly: Day 1 , 11:00 PM

You can optimize performance of this protection group now or you can do it later from the actions pane

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

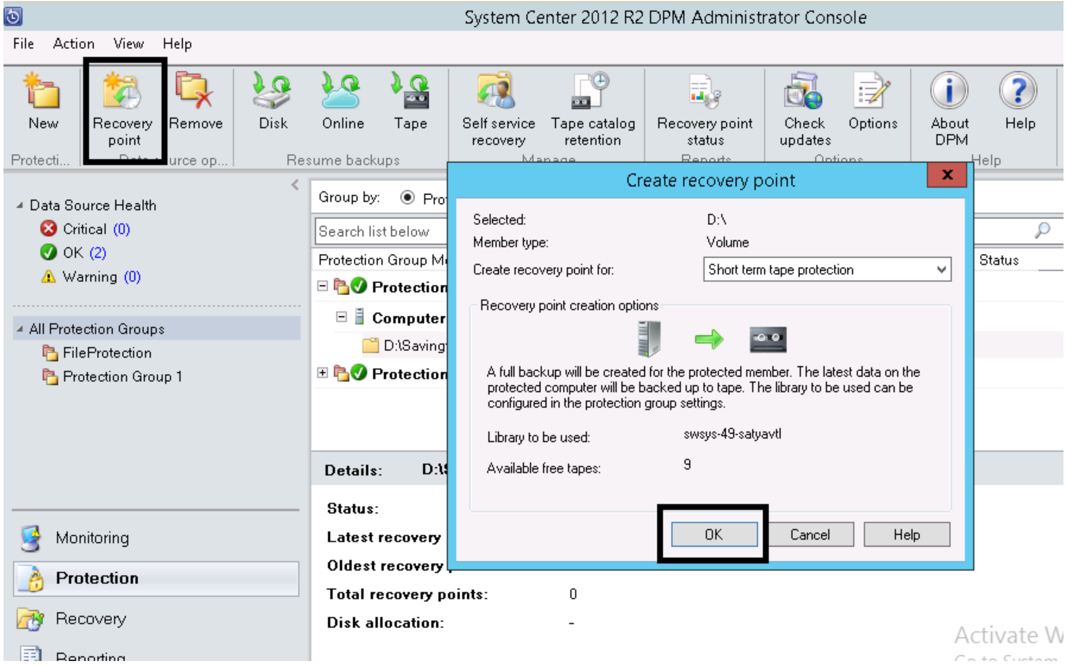


Create New Protection Group
Status
Steps:
Welcome
Select protection group type
Select group members
Select data protection method
Specify short-term goals
Specify long-term goals
Select library and tape details
Summary
Status
Tasks

Task	Results
Create protection group: FileProtection	Success

DPM does not protect reparse points found in file systems, except for deduplication reparse points, which are protected. If you have selected volumes or folders in this protection group, all data is protected except for the unprotected reparse points.
Read "Select Group Members" page of DPM 2012 Help for more details on unsupported data.

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**.



Details: D:\

Status:

Latest recovery

Oldest recovery

Total recovery points: 0

Disk allocation: -

Create recovery point

Selected: D:\

Member type: Volume

Create recovery point for: Short term tape protection

Recovery point creation options

A full backup will be created for the protected member. The latest data on the protected computer will be backed up to tape. The library to be used can be configured in the protection group settings.

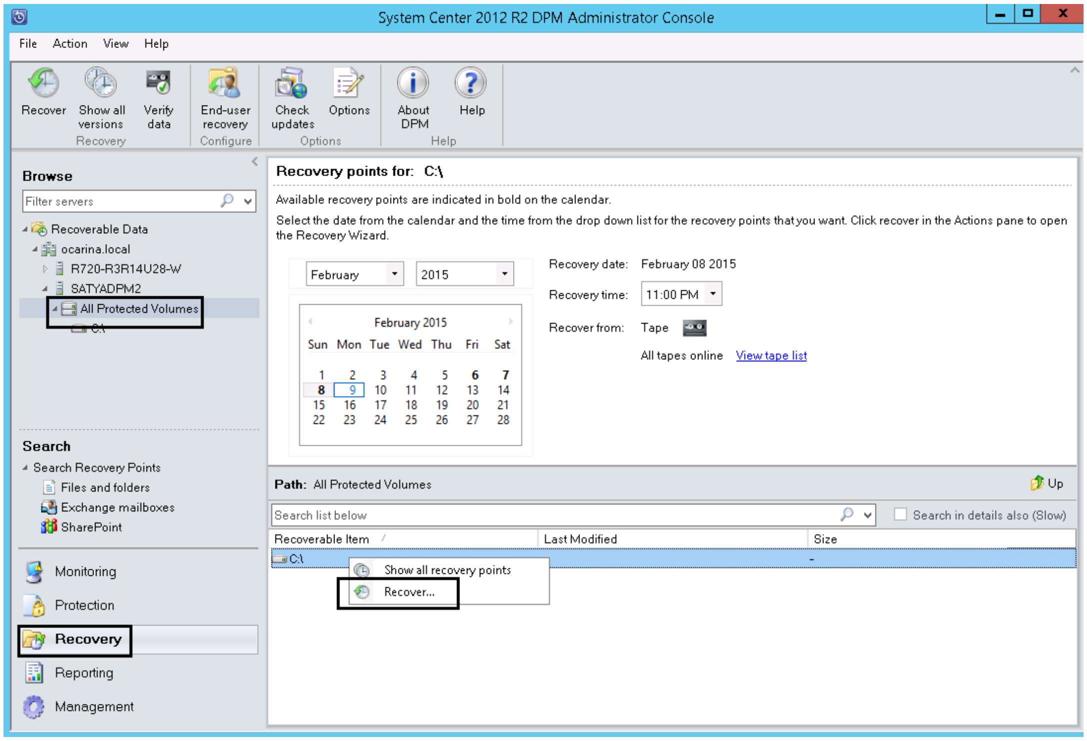
Library to be used: swsys-49-satyavtl

Available free tapes: 9

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.



Available recovery points are indicated in bold on the calendar.

Select the date from the calendar and the time from the drop down list for the recovery points that you want. Click recover in the Actions pane to open the Recovery Wizard.

Recovery date: February 08 2015

Recovery time: 11:00 PM

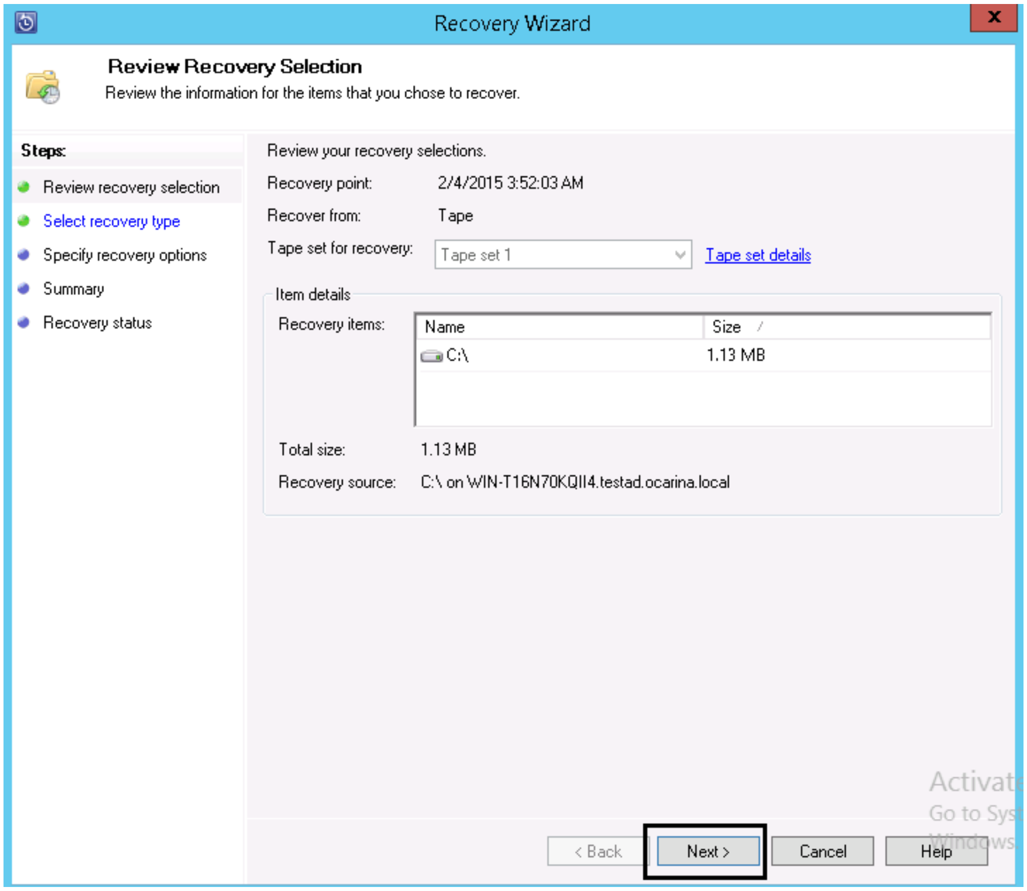
Recover from: Tape

All tapes online

Path: All Protected Volumes

Recoverable Item	Last Modified	Size
C:\		-

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



Review Recovery Selection

Review the information for the items that you chose to recover.

Review your recovery selections.

Recovery point: 2/4/2015 3:52:03 AM

Recover from: Tape

Tape set for recovery: Tape set 1

Item details

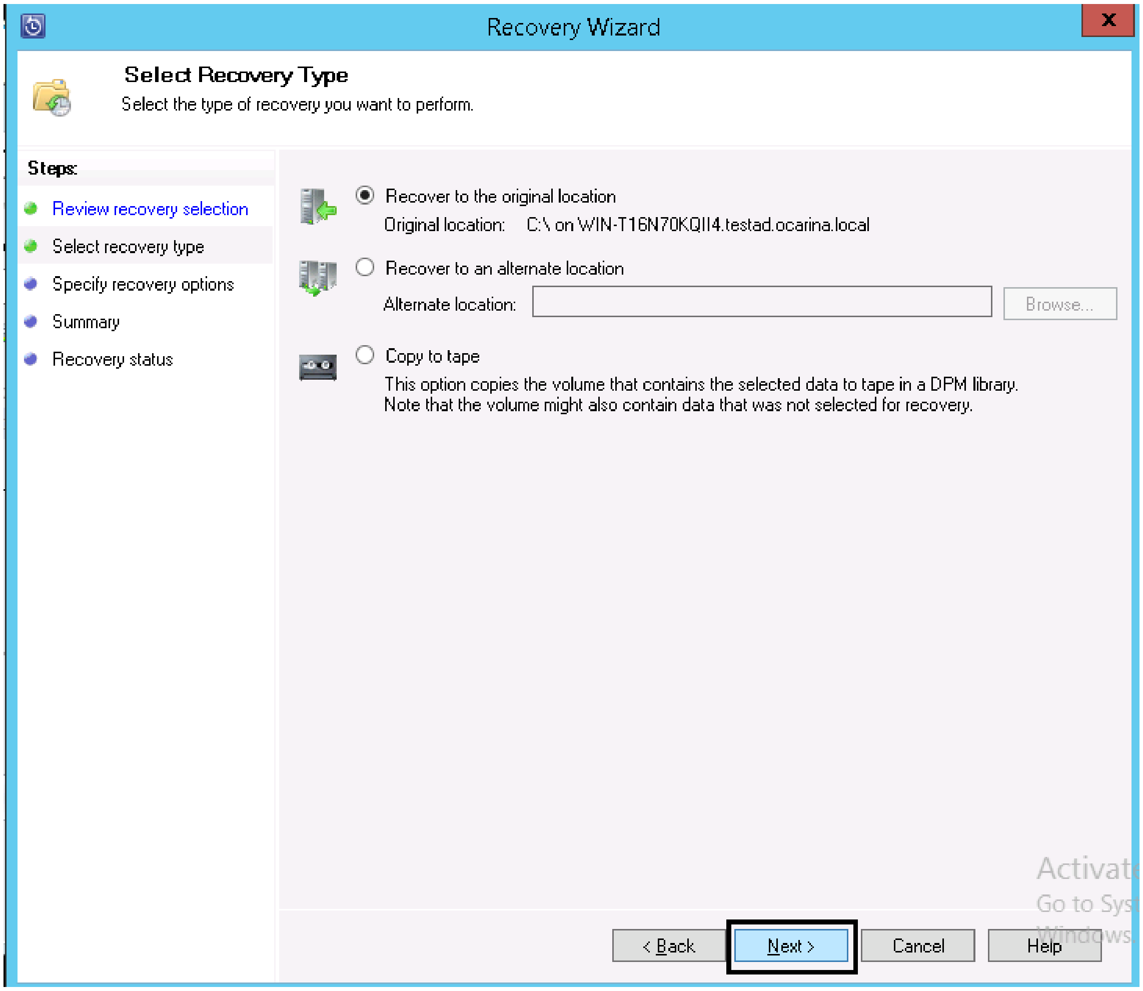
Recovery items:

Name	Size
C:\	1.13 MB

Total size: 1.13 MB

Recovery source: C:\ on WIN-T16N70KQII4.testad.ocarina.local

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



Recovery Wizard

Select Recovery Type

Select the type of recovery you want to perform.

Steps:

- Review recovery selection
- Select recovery type
- Specify recovery options
- Summary
- Recovery status

● Recover to the original location

Original location: C:\ on WIN-T16N70KQII4.testad.ocarina.local

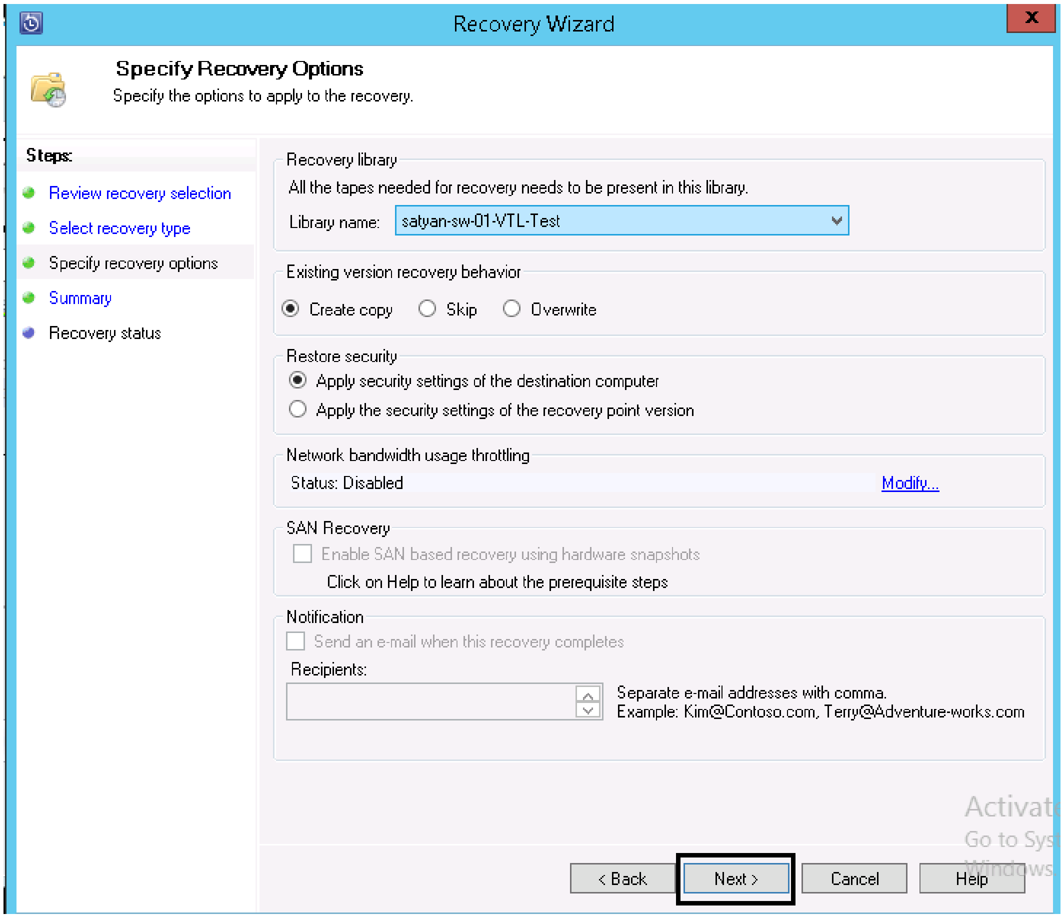
○ Recover to an alternate location

Alternate location:

○ Copy to tape

This option copies the volume that contains the selected data to tape in a DPM library. Note that the volume might also contain data that was not selected for recovery.

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



Recovery Wizard

Specify Recovery Options

Specify the options to apply to the recovery.

Recovery library

All the tapes needed for recovery needs to be present in this library.

Library name: satyan-sw-01-VTL-Test

Existing version recovery behavior

● Create copy ○ Skip ○ Overwrite

Restore security

● Apply security settings of the destination computer

○ Apply the security settings of the recovery point version

Network bandwidth usage throttling

Status: Disabled Modify...

SAN Recovery

□ Enable SAN based recovery using hardware snapshots

Click on Help to learn about the prerequisite steps

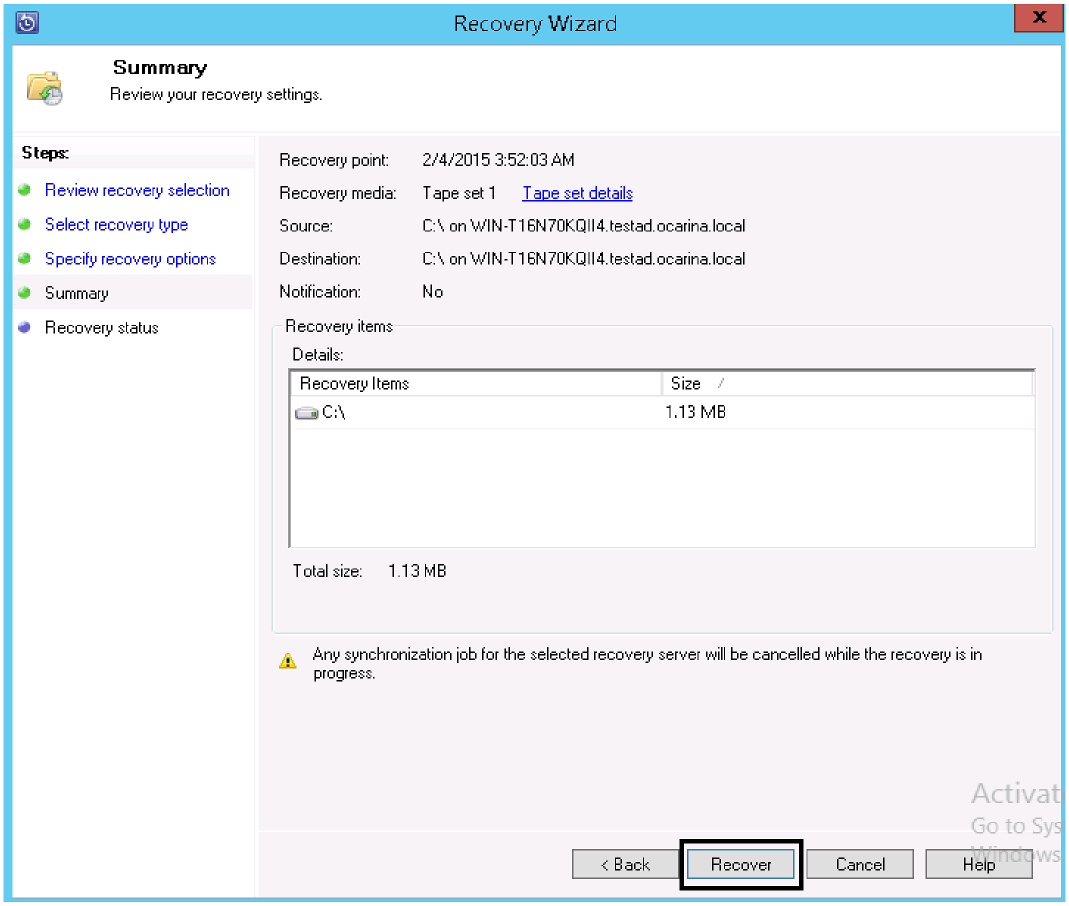
Notification

□ Send an e-mail when this recovery completes

Recipients:

Separate e-mail addresses with comma.
Example: Kim@Contoso.com, Terry@Adventure-works.com

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



Recovery point: 2/4/2015 3:52:03 AM

Recovery media: Tape set 1 Tape set details

Source: C:\ on WIN-T16N70KQII4.testad.ocarina.local

Destination: C:\ on WIN-T16N70KQII4.testad.ocarina.local

Notification: No

Recovery items

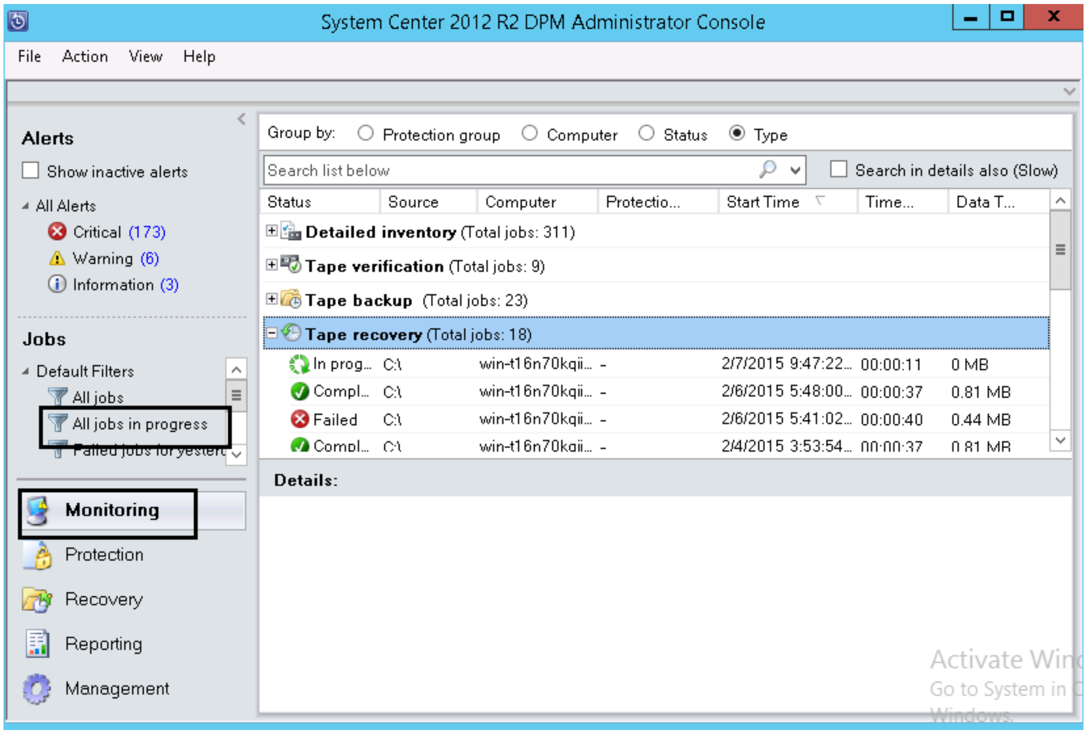
Details:

Recovery Items	Size
C:\	1.13 MB

Total size: 1.13 MB

Any synchronization job for the selected recovery server will be cancelled while the recovery is in progress.

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



Group by: ○ Protection group ○ Computer ○ Status ● Type

Search list below

□ Search in details also (Slow)

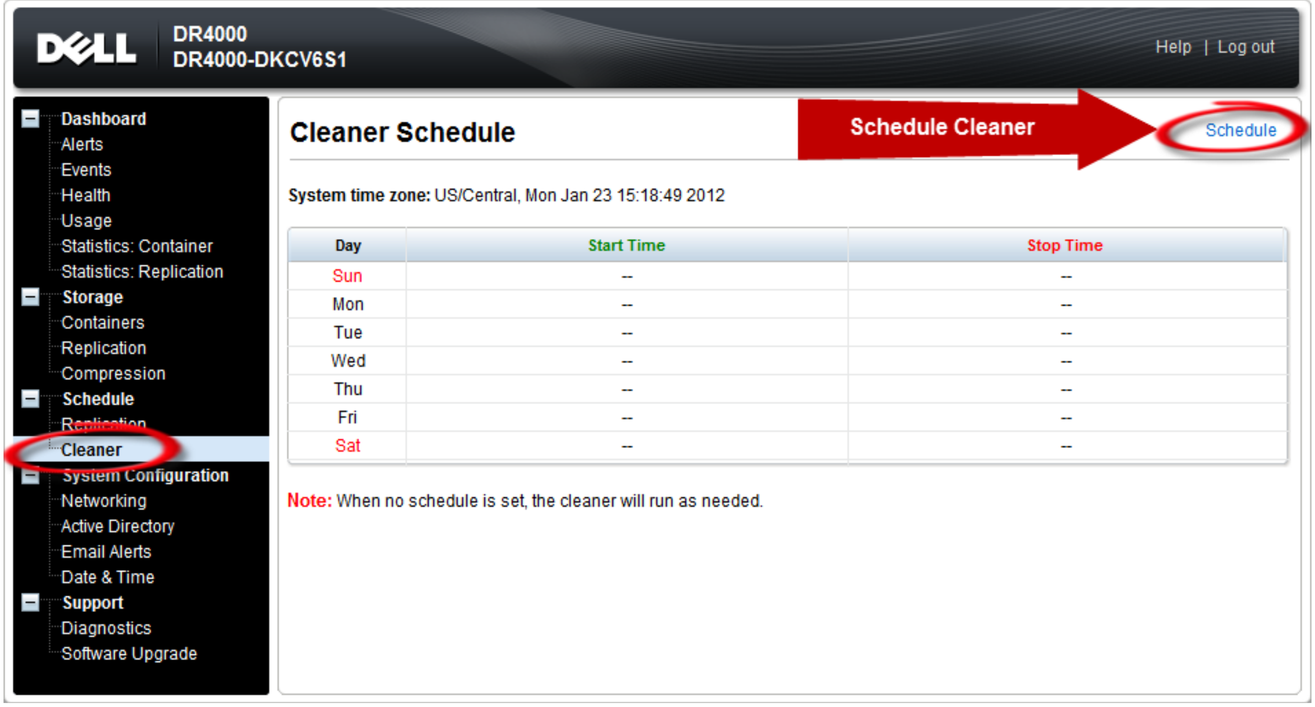
Status	Source	Computer	Protectio...	Start Time	Time...	Data T...
⊞ **Detailed inventory** (Total jobs: 311)						
⊞ **Tape verification** (Total jobs: 9)						
⊞ **Tape backup** (Total jobs: 23)						
⊟ **Tape recovery** (Total jobs: 18)						
In prog...	C:\	win-t16n70kqii...	-	2/7/2015 9:47:22...	00:00:11	0 MB
✓ Compl...	C:\	win-t16n70kqii...	-	2/6/2015 5:48:00...	00:00:37	0.81 MB
☒ Failed	C:\	win-t16n70kqii...	-	2/6/2015 5:41:02...	00:00:40	0.44 MB
✓ Compl...	C:\	win-t16n70kqii...	-	2/4/2015 3:53:54...	00:00:37	0.81 MB

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.



Cleaner Schedule

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

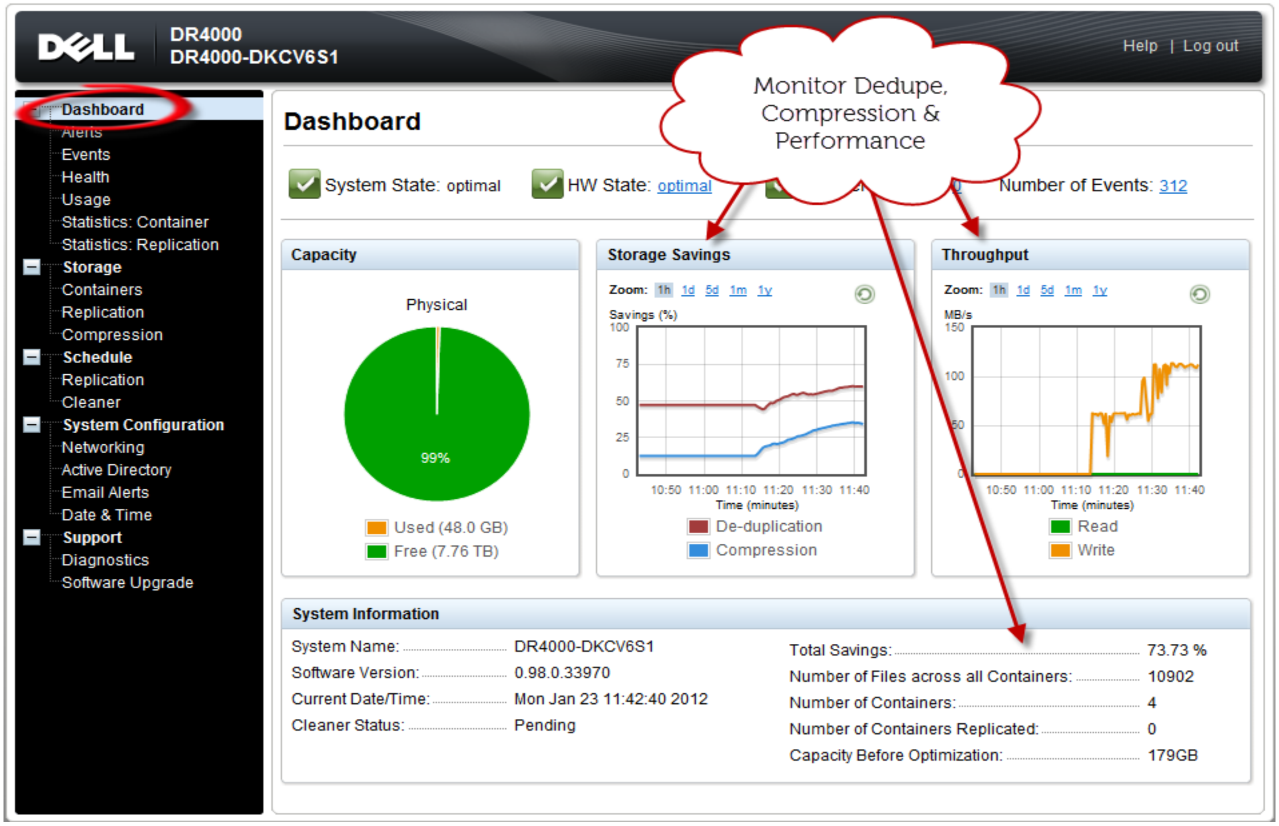
Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--

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.



Monitor Dedupe, Compression & Performance

DR4000
DR4000-DKCV6S1

Dashboard

✓ System State: optimal ✓ HW State: optimal Number of Events: 312

System Information

System Name:	DR4000-DKCV6S1
Software Version:	0.98.0.33970
Current Date/Time:	Mon Jan 23 11:42:40 2012
Cleaner Status:	Pending
Total Savings:	73.73 %
Number of Files across all Containers:	10902
Number of Containers:	4
Number of Containers Replicated:	0
Capacity Before Optimization:	179GB

A Managing VTL protocol accounts and credentials

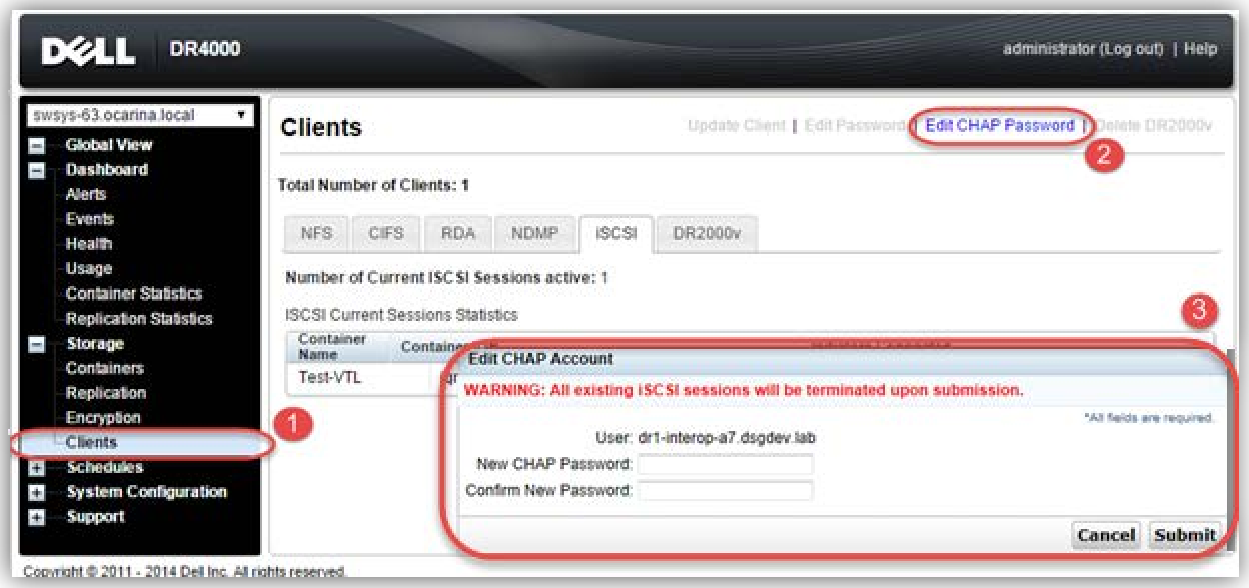
A.1 Managing iSCSI account details

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



Clients

Total Number of Clients: 1

Number of Current ISCSI Sessions active: 1

ISCSI Current Sessions Statistics

Container Name	Containe
Test-VTL	gr

Edit CHAP Account

WARNING: All existing ISCSI sessions will be terminated upon submission.

*All fields are required.

User: dr1-interop-a7.dsgdev.lab

New CHAP Password:

Confirm New Password:

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

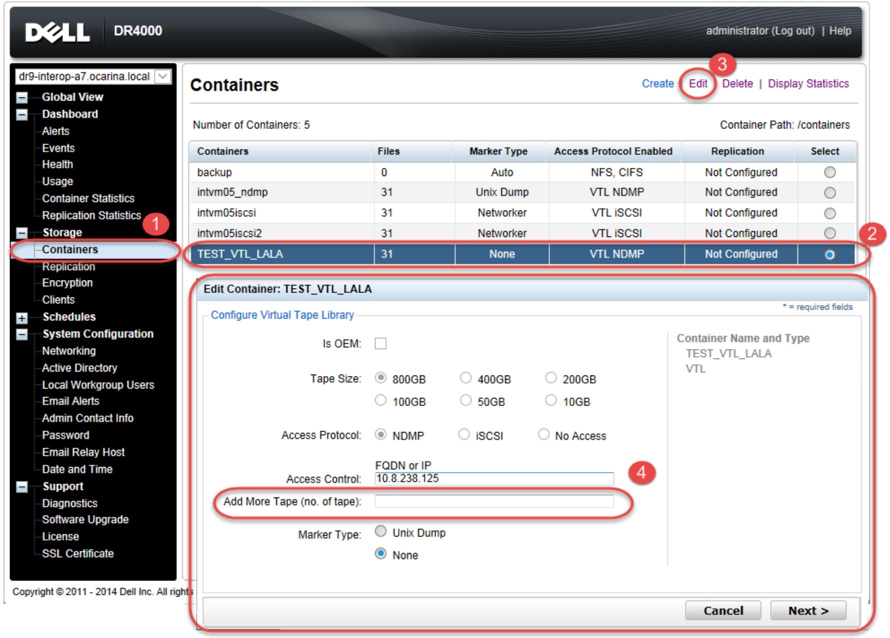
Type	Capacity	Max number of Tapes supported
LTO-4	800GiB	2000

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.



Containers

Number of Containers: 5

Container Path: /containers

Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
backup	0	Auto	NFS, CIFS	Not Configured	○
intvm05_ndmp	31	Unix Dump	VTL NDMP	Not Configured	○
intvm05iscsi	31	Networker	VTL iSCSI	Not Configured	○
intvm05iscsi2	31	Networker	VTL iSCSI	Not Configured	○
TEST_VTL_LALA	31	None	VTL NDMP	Not Configured	●

Edit Container: TEST_VTL_LALA

Configure Virtual Tape Library

* = required fields

Is OEM: □

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

Access Protocol: ● NDMP ○ iSCSI ○ No Access

Access Control: FQDN or IP 10.8.238.125

Add More Tape (no. of tape):

Marker Type: ○ Unix Dump ● None

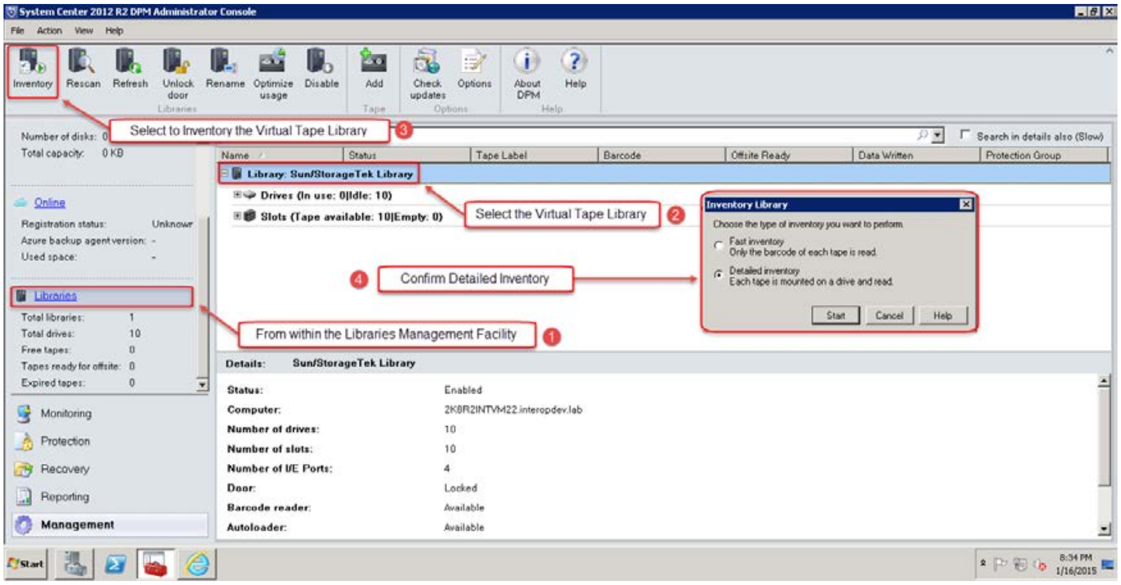
Container Name and Type
TEST_VTL_LALA
VTL

Copyright © 2011 - 2014 Dell Inc. All rights

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.



Select to Inventory the Virtual Tape Library

Select the Virtual Tape Library

Confirm Detailed Inventory

From within the Libraries Management Facility

Number of disks: 0
Total capacity: 0 KB

Registration status: Unknown
Azure backup agent version: -
Used space: -

Total libraries: 1
Total drives: 10
Free tapes: 0
Tapes ready for offsite: 0
Expired tapes: 0

Library: Sun/StorageTek Library
Drives (In use: 0|Idle: 10)
Slots (Tape available: 10|Empty: 0)

Inventory Library
Choose the type of inventory you want to perform.
○ Fast inventory
Only the barcode of each tape is read.
● Detailed inventory
Each tape is mounted on a drive and read.

Details: Sun/StorageTek Library

Status: Enabled
Computer: 2K8R2INTVM22.interopdev.lab
Number of drives: 10
Number of slots: 10
Number of I/E Ports: 4
Door: Locked
Barcode reader: Available
Autoloader: Available

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 though 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.