StarWind Virtual SAN®
Virtual Tape Library used with Microsoft System Center Data Protection Manager 2016

MARCH 2017
TECHNICAL PAPER

Written by Charbel Nemnom
Microsoft MVP – Cloud and Datacenter Management
Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the Technical Papers webpage or in StarWind Forum. If you need further assistance, please contact us.

Copyright ©2009-2017 StarWind Software Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms”.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company's core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient Hyper-Converged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into Hyper-Converged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind Hyper-Converged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.
Contents

Introduction ................................................................................................................................. 4
What is a Virtual Tape Library (VTL) .......................................................................................... 5
Introducing System Center Data Protection Manager 2016 ....................................................... 5
Pre-Configuring the Servers ...................................................................................................... 6
Installing System Center Data Protection Manager 2016 ......................................................... 7
Creating Virtual Tape Library .................................................................................................. 8
DPM-Side Configuration ........................................................................................................... 14
Add tapes to DPM .................................................................................................................... 18
Configuring protection group for DPM ..................................................................................... 21
Restoring data from tape .......................................................................................................... 29
Copying protected data to tape ............................................................................................... 33
Configuring tape optimization for DPM ................................................................................... 38
Configuring DPM for the short erase tape feature .................................................................. 43
Understanding tape reports in DPM ....................................................................................... 45
Conclusion ............................................................................................................................... 46
**Introduction**

Tapes have been the definite archive media for many years and will probably continue to be used for this purpose for many years to come. There are many reasons why you may want to use tapes versus cloud, like meeting compliance and security requirements, accommodating backup latency issues, or you are just not ready to move your data to the public Cloud.

For many companies, there is no interest in backing up the production data to an actual tape. The reason is that they only need the *Grandfather-father-son rotation* or granularity, tapes are also sensitive to magnetic fields and condensation and the transfer speed is slow. The same things can be accomplished using a virtual tape library, also known as VTL, which could be a hardware box or software that you install on your backup server.

StarWind Virtual Tape Library (VTL) is an appliance and can also be software-only (as part of StarWind VSAN functionality) that eliminates the need for physical tapes by emulating industry-standard tape hardware, keeping all data on inexpensive, fast and high-capacity spinning disks. It is designed for SMB and Enterprises, who either look to get rid of backup tapes completely, or are willing to accelerate backup process and add an extra level of protection. Even with explosive data growth, StarWind VTL fits the backup into backup window by accelerating it, so the process does not overlap with production time. Optionally, it creates additional copy of backup data on the intermediate HDD for better safety. As a result, tape backup becomes affordable, fast and convenient.

This guide is intended for experienced StarWind users and Windows system administrators and IT professionals who would like to configure StarWind Virtual SAN solution. It provides detailed instructions on how to create the Virtual Tape Library device that will run on top of the Windows Server 2016 and integrate with Microsoft System Center Data Protection Manager 2016.

A full set of up-to-date technical documentation can always be found [here](#), or by pressing the Help button in the StarWind Management Console.

For any technical inquiries please visit our [online community](#), [Frequently Asked Questions](#) page, or use the [support form](#) to contact our technical support department.
What is a Virtual Tape Library (VTL)

A virtual tape library simulates a media changer and a number of tape drives. Instead of using physical tapes, the VTL software or hardware writes the backed-up data to individual files that represent a tape. Different vendors use different file setups and extensions.

The advantage of using VTL versus actual tape is to gain granularity of the tape while benefit the speed of a disk-based backup and restore. This also enables you to customize your storage for the VTL software or hardware. You can either choose to have a lot of storage but lack the speed or the opposite.

A VTL solution is installed and configured the same way as a physical tape library, and from a DPM perspective, you can manage it the same way regarding its short-term and long-term retention policy.

Introducing System Center Data Protection Manager 2016

System Center Data Protection Manager 2016 (SCDPM) is the latest release by Microsoft and with it comes a lot of improvements and new features. DPM is well recognized in the industry for protection of Microsoft workloads and environments. With DPM 2016, you can back up the most common workloads in a modern data center today. DPM can backup various business workloads such as the following which might be running on physical machines, Hyper-V, VMware, or in Microsoft Azure:

- Exchange Server
- SQL Server
- SharePoint Server
- Microsoft Dynamics
- Windows Server
- Hyper-V VMs
- System States and Active Directory
- Windows clients
- Files and folders
- VMware VMs (Supported starting with DPM 2012 R2 Update Rollup 11 or later, DPM 2016 support is coming very soon).

In earlier article, we covered the latest features of System Center Data Protection Manager 2016, you can read all about it [here](#).

The protected data by DPM can be backed-up to disks for short-term retention, to tapes for short-term and long-term retention, and to Microsoft Azure for long-term retention.
Pre-Configuring the Servers

**Figure 1.** shows the reference network diagram of the configuration described in this guide. StarWind server running VTL device and Hypervisor running VMs and DPM are connected directly, but it is possible to wire them through switches as optional.
Installing System Center Data Protection Manager 2016

You can install SCDPM in different ways. Please refer to below articles where we described in details how to install System Center Data Protection Manager 2016, you can choose the installation method that suits your needs:

- [How to install SCDPM 2016 on Windows Server 2016 and SQL Server 2016](#)
- [How to Automate the installation of SCDPM 2016 on Windows Server 2016](#)
- [How to Deploy SCDPM 2016 using SCVMM 2016 on Windows Server 2016](#)

System Center Data Protection Manager 2016 can protect Windows Server 2016 private cloud deployments efficiently and seamlessly. In Windows Server 2016, Microsoft introduced Resilient Change Tracking (RCT) technology. RCT allows backup applications (such as DPM) to find out which blocks of a file have changed since an earlier point in time. DPM 2016 rely now on RCT technology to check the virtual hard disk file that have changed and only read the changed blocks instead of tracking the VM changes using the file system driver. However, when you deploy DPM 2016 agent on any Windows Server 2016 Hyper-V (host or cluster), DPM will still install the file system driver for you, which gives you the flexibility to migrate VMs from Windows Server 2012 R2 to Windows Server 2016 and keep protecting those VMs for you seamlessly. Best of all, the RCT technology is transparent, and does not need any configuration or management from your side.

For more information about Resilient Change Tracking (RCT) in Windows Server 2016 including the backup architecture and the difference between different versions, I strongly recommend to check my recent published book about [Windows Server 2016 Hyper-V Cookbook - Second Edition](#).

In this guide, we will focus on the StarWind virtual tape library (VTL) management, and how System Center Data Protection Manager 2016 can leverage it.
Creating Virtual Tape Library

1. Launch StarWind Management Console and connect to the server. Right click on the server and select **Add Device (advanced)** from the pop-up menu.

2. The Add Device Wizard appears. Choose **Tape Device** item.

Select Device Type you want to create or export as iSCSI Target

- [ ] Hard Disk Device
- [x] Tape Device
- [ ] Optical Disc Drive

Click **Next** to continue.
3. Choose **Virtual Tape** item.

   Add Device Wizard

   **Select Disk Device Type**

   - **Virtual Tape**
     Virtual Tape based on File Images stored on Disk
   - **Physical Tape**
     Export existing physical Tape Device as iSCSI Target
   - **Physical Tape Auto-Loader/Changer**
     Export existing physical Tape Auto-Loader/Changer Device as iSCSI Target

Click **Next** to continue.

4. Enter the path and the name to **virtual Device Header File**.

   Add Device Wizard

   **Virtual Tape Library Location**

   - **Create a New Virtual Tape Library**
     - Name: **SCDPM-VTL01**
     - Location: **My Computer\**
   - **Use an Existing Virtual Tape Library**
     - Location: 

Click **Next** to continue.
5. Select the **Device Model to emulate** a tape drive. Based on DPM compatible list of tape libraries, the **HP MSL2024** and **HP MSL8096** both are supported. For this example, we will select **HP MSL8096** because it’s more performant than **HP MSL2024**. Please note that **ADIC** is not supported by DPM.

   ![Select Device Model to emulate](image)

   Click **Next** to continue.

6. Specify the **Target Alias**. Target Name will be generated automatically.

   ![Target Parameters](image)

   Click **Next** to continue.
7. At **Creation page** click **Create** and view the creation progress.

8. After creation you will see **Device Creation completed** page.

   Click **OK**.
9. The VTL loader is created successfully. Right click on the device and select **Create Tape...** from the pop-up menu.

10. Select the **Tape Type** (size) and click **OK**. In this example, we will select **LTO-6 Ultrium 6/16T (2500GB)** ~2.45TB. The recommended type to use is **LTO-5** and **LTO-6** tapes. You can also customize the **Tape Capacity Size** in case you don't have enough usable space (i.e. **LTO-6** with 1000GB). You cannot customize with more than the maximum tape capacity (Less Than or Equal To 2500GB is supported). As a best practice, we would suggest creating more tapes with smaller sizes instead of larger sizes (more on that in Configuring tape optimization for DPM section).
11. StarWind VTL will not provision a 2.5TB fixed file on the host, instead it will create a thin empty header file with 2KB in size. The file will grow as soon as DPM start writing on the tape.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0F80001.VTape</td>
<td>2/12/2017 9:00 AM</td>
<td>VTAPE File</td>
<td>2 KB</td>
</tr>
<tr>
<td>D0F80001.VTdat</td>
<td>2/12/2017 9:00 AM</td>
<td>VTDAT File</td>
<td>0 KB</td>
</tr>
<tr>
<td>D0F80001.VTidx</td>
<td>2/12/2017 9:00 AM</td>
<td>VTIDX File</td>
<td>0 KB</td>
</tr>
<tr>
<td>D0F80002.VTape</td>
<td>2/12/2017 6:27 PM</td>
<td>VTAPE File</td>
<td>2 KB</td>
</tr>
<tr>
<td>D0F80002.VTdat</td>
<td>2/12/2017 6:27 PM</td>
<td>VTDAT File</td>
<td>0 KB</td>
</tr>
<tr>
<td>D0F80002.VTidx</td>
<td>2/12/2017 6:27 PM</td>
<td>VTIDX File</td>
<td>0 KB</td>
</tr>
<tr>
<td>D0F80003.VTape</td>
<td>2/12/2017 6:27 PM</td>
<td>VTAPE File</td>
<td>2 KB</td>
</tr>
<tr>
<td>D0F80003.VTdat</td>
<td>2/12/2017 6:27 PM</td>
<td>VTDAT File</td>
<td>0 KB</td>
</tr>
<tr>
<td>D0F80003.VTidx</td>
<td>2/12/2017 6:27 PM</td>
<td>VTIDX File</td>
<td>0 KB</td>
</tr>
</tbody>
</table>

12. The Tape is created and placed into the first slot of VTL. The HP MSL8096 that we have in this example supports 4 drive slots and 96 storage slots, since we already created one tape with 2500GB, we can still create up to 95 more tapes. The Drive Slots means that data can be written and read from 4 tapes simultaneously. This will boost performance.
**DPM-Side Configuration**

1. Launch the Microsoft iSCSI initiator from the DPM Server. Switch to **Discovery** tab. Click **Discover Portal** and enter the IP address of StarWind server with VTL created.

   ![Image of Discovery tab](image1.png)

2. Switch to **Targets** tab and connect the target. Make sure you select “Microsoft iSCSI Initiator” under Advanced Settings. It’s recommended to put the iSCSI traffic on different network, so make sure to choose the **Initiator IP** and the **Target IP** accordingly.

   ![Image of Targets tab](image2.png)
3. Open **Device Manager** and see the Medium Changer devices is shown as “**Unknown Medium Changer**”. The VTL that we created in the previous step supports 4 drive slots, for this reason we can see 4 **Tape drives** in Device Manager named “**Hewlett Packard LTO Ultrium-5 drive**”.

4. It’s recommended to install the latest update driver from HP. The driver for **HP MSL8096** can be downloaded here [HPE StoreEver Tape Drivers for Microsoft Windows](#). The current version that support Windows Server 2016 is **4.2.0.0**.

*RECOMMENDED* **HPE StoreEver Tape Drivers for Microsoft Windows**

By downloading, you agree to the terms and conditions of the [Hewlett Packard Enterprise Software License Agreement](#).  

**Note:** Some software requires a valid warranty, current Hewlett Packard Enterprise support contract, or a license fee.
5. Extract the driver downloaded in Step 4 and launch `cpqsetup.exe`

6. Select All and click **Install**.
7. Once the drivers are installed, you can see the Medium Changer devices is shown now as “Hewlett Packard MSL G3 Series library (x64 based)”. 

8. We are ready now to add tape(s) to DPM library.
**Add tapes to DPM**

1. DPM automatically detects tape devices that are attached to it and they are displayed in the **Libraries** workspace of the **Management** view.

2. If the tape isn’t displayed, you can detect it manually with the **Rescan** button. This might take a few minutes.

3. After you rescan, check that the details displayed in **Device Manager** and in the tape library are the same. You will see one tape library with 4 drives and 96 available slots (tapes).
4. If you want to add more tapes, select the tape library in the Libraries workspace of the Management view, and then click Add+

5. The I/E port door named “Hewlett Packard MSL G3 Series library” will be open, so you can create more tapes using StarWind management console as described in the previous section. Do NOT press OK. See the next step.
6. Once the tapes are created using StarWind management console, press **OK**. DPM will detect the newly added tapes as shown in the next screenshot.

![Add Tapes Using VE port](image)

Press **OK**.

7. Before we start using the newly added tapes, we need to **Identify** the “Unknown” tapes so they become “Free” and ready to be used.

![System Center 2016 DPM Administrator Console](image)

8. After short period, the tapes will be available and marked as “**Free**”.

![System Center 2016 DPM Administrator Console](image)
Configuring protection group for DPM

1. Assuming you have already deploy DPM agent on your servers. Open DPM Management Console in the Protection workspace of the Management view, and then click New+

2. Select the option desired for backup (Servers / Clients).

Click Next to continue.
Choose the data to protect.

Click **Next** to continue.
4. System Center Data Protection Manager 2016 will provide you two protection methods in Protection Group Wizard when modifying or creating a new protection group. These are:

- Short-term protection (Disk / Tape).
- Long-term protection (Tape).

Select your Protection Method. In this example, we will select tape for short-term protection as well as long-term protection.

Click **Next** to continue.
5. System Center Data Protection Manager 2016 will provide you three additional steps in Protection Group Wizard when modifying or creating a new protection group. These are:

- Specify short-term goals
- Specify long-term goals
- Select library and tape details

Specify your desired Short-Term Goals. In this example, we will specify the retention range 12 Weeks (3 months), this is the maximum short-term protection you can specify. We will choose the frequency of backup as Daily. You can specify Weekly and Biweekly as well. The backup mode is Only full backup. Because Microsoft is doing this by NOT using incremental technology when writing data to a tape; instead, the DPM server will allocate two tapes per Protection Group and write a full backup to the tape. This will result in a longer backup time, but you will gain speed when performing a restore as you are not using the incremental restore chain of tapes.

Click Next to continue.
6. Specify your desired **Long-Term Goals**. In this example, we will specify the retention range 3 Years (maximum is 99 years). We will choose the frequency of backup as **Quarterly**. You can specify **Daily**, **Weekly**, **Biweekly**, **Monthly**, **Half yearly** and **Yearly**. The short-term goal was set in the previous step to maximum 3 months, it makes sense to go with quarterly. In this case, we will have 1 recovery point every 3 months. You need to check your company policy and specify the retention range accordingly.

Click **Next** to continue.
Select the **Library and Tape Details**. In this example, we have only one tape library “Hewlett Packard MSL G3 Series library (x64 based)”. Since this tape library support up to 4 slots, we will increase the allocated drives to 4. This means that data can be written and read from 4 tapes simultaneously to increase performance. Select the **Compress data** option for short-term and long-term protection, this feature is useful which basically allow to write sequential data on the tape, therefore the tape backup will be much more efficient.

Click **Next** to continue.
8. Review the Summary and click Create Group.

![Create New Protection Group]

9. You can create a manual recovery point if you don't want to wait for the backup schedule. You can do this in the Protection workspace of the Management view, right click on the protected item and select Create recovery point... You can choose Short term tape protection or Long term tape protection.

![Create recovery point]

If you choose Long term tape protection, the latest recovery point on short-term tape will be backed up to tape.
10. Open the **Libraries** workspace of the **Management** view, and see the protection group named “Tape Protection Group 01” is assigned to slot 5 and 6, the Data Written was around 15GB which match the actual data. In this example, we created two recovery points, hence the data was written twice on two different tapes respectively.

11. If you look at the StarWind VTL storage file system, you can see that the data was written to **D0F80005.VTdat** (Slot 5) and **D0F80006.VTdat** (Slot 6) respectively.
Restoring data from tape

This section will provide you with the steps to recover protected data from tape.

1. Make sure that your tape library is online and does not report any errors; this can be done by verifying the alerts in the Monitoring view of the DPM console or in the Libraries workspace of the Management view of the DPM console.

2. In the DPM console, go to Recovery and choose the data source you would like to recover.

3. Mark the data source and choose the data and time for the restore. Right-click on the data source and choose Recover… to start the Recovery wizard.

4. In the Review Recovery Selection wizard, review the data source that is chosen for recovery and click on Next > to continue.

5. In the Select Recovery Type wizard, you will choose how to recover your data. When you recover data from tape you can:
   - Recover to original instance
   - Recover as virtual machine to any host (Only available if you are restoring a VM)
   - Copy to a network folder
   - Copy to tape
6. If you select **Copy to a network folder**, you need to have a DPM agent deployed and a data source that is protected by the DPM server for the server to be listed as a recovery destination.

7. If you choose **Copy to tape**, see the next section for more information.

8. In this example, we will cover how to recover as virtual machine to any host. Select **Recover as virtual machine to any host** option and click on **Next >** to continue.

9. In the **Specify Destination** wizard, specify where you want to recover the virtual machine. Click on **Next >** to continue.
10. In the **Specify Recovery Options** wizard, you can configure specific options for the recovery. The first thing to verify is the **Recovery library** name. It is important to choose the library that hosts all the tapes that are needed for the recovery. In this example, we have only one tape drive named “Hewlett Packard MSL G3 Series library (x64 based)”.

11. Click through to complete the wizard. In the **Summary** step, you can verify the recovery settings, click on **Recover** to start the process of recovering the virtual machine to a different host.
12. In the **Recovery Status** wizard, you can follow the progress of the job.

![Recovery Status](image)

**Note:**

When you restore data from a tape, DPM uses a scratch before it gives the data to the selected data source. It is very important that your DPM %systemdrive% server has more than 10 GB of free disk space.

DPM supports item-level recovery (ILR), which allows you to perform a specific recovery of files, folders, volumes, and virtual hard disks from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server. However, ILR is not supported when you restore from tapes, you can only restore an entire VM or a single virtual hard disk.
Copying protected data to tape

This section will provide you with the steps to export backup data from disk to tape to archive, for portability, or other reasons.

1. In the DPM console, go to Recovery and choose the data source you would like to recover.

2. Mark the data source and choose the data and time for the recovery. Right-click on the data source and choose Recover... to start the Recovery wizard.

3. In the Review Recovery Selection wizard, review the data source that is chosen for recovery and click on Next > to continue.

4. In the Select Recovery Type wizard, choose Copy to tape and click on Next > to continue.
5. In the **Specify Library** wizard, you can define which tape library you should use for **Primary library** and **Copy library** if you have multiple libraries present in your DPM server. In the **Tape options** section, you can specify a custom **Tape label** that could provide an easier way to determine the actual contents of the tape. Choose the **Compress** option, so the data will be compressed that is written to the tape. Click **Next** to continue.

6. Click through to complete the wizard. In the **Summary** step, you can verify the recovery settings, click on **Recover** to start the process of copying it to tape.
7. In the **Recovery Status** wizard, you can follow the progress of the job.

   ![Recovery Status wizard](image1)

   **Recovery Status**
   
   **Steps:**
   - Review recovery selection
   - Select recovery type
   - Specify library
   - Specify recovery options
   - Summary
   - Recovery status

   **Recovery status:** Successful
   - **Start time:** 2/14/2017 6:28:57 AM
   - **End time:** 2/14/2017 5:31:05 AM
   - **Data transferred:** 15,308.50 MB

8. If you want to restore the data that has being copied to the tape as described above. Open the **Libraries** workspace in the **Management** view and select the tape where the data was imported (copied). Right click and select **View tape contents**.

   ![Libraries workspace](image2)
9. The **View Tape Contents** window will open. Select the desired content that you want to restore, and click **Copy**...

![View Tape Contents Window]

10. Specify the **Alternate Recovery Destination**, and then click **OK** to continue.

![Specify Alternate Recovery Destination Window]
11. The selected data will be copied to the location specified. You can monitor the progress of the copy job(s) on the Jobs tab in the Monitoring view area.

```
Completed (Total jobs: 356)

-   -   -   -   -
ws2016-hv03.vrt.lab   Copy data - tape   2/14/2017 2:02:27 PM

Details:

Type: Copy data - tape
Status: Completed
End time: 2/14/2017 2:05:02 PM
Start time: 2/14/2017 2:02:27 PM
Time elapsed: 00:02:35
Data transferred: 15,303.19 MB (16051798016 bytes)
Source details: -
Target details: D:\ on W52016-HV01.VRT.LAB
Library: Hewlett Packard MSL G3 Series library (vd4 based)
Tape Label (Barcode): DPM_Recovered_RTC_W52016-HV02.VRT.LAB:00000001 (D0F80004)
```

Please note that the data will remain on the tape after the restore. If you want to erase the tape, please see Configuring DPM for the short erase tape feature section.
Configuring tape optimization for DPM

This section will cover how to set up tape colocation and optimization for DPM.

When Microsoft released System Center Data Protection Manager 2007, they introduced a new feature called co-location. By enabling this feature, DPM 2016 allows you to choose which protection groups can be co-located on the same tape regardless of retention goals. This have a large impact on how long a tape can used for backup jobs.

As a side note: If you don't optimize and co-locate your protection groups, you will not be able to continuously backup once all tapes in your tape library are used at least once. The collocation set is needed for Scheduled backups and for Ad-Hoc backups in order to use the same tapes.

To enable co-location for your protected workloads on tapes, there are some key points that you should be aware of. DPM uses protection group sets to optimize tape usage. A protection group set is a set of protection groups for which the backups will be co-located on tape. You use the tape optimization feature to allow multiple protection groups to share a tape to store their backups. The first thing you need to configure is to create new sets of tape optimization by using DPM console and then associate protection groups to the set.

1. Open DPM console and click on Libraries workspace in the Management view. In the DPM console, you will now be able to click on the Optimize usage button in the top-left section of the DPM console.
2. The **Tape Optimization Setup** window will open; click on the **Create** button to create your **Tape Optimization Set**.

3. When you click on **Create**, a new window will appear, which will present you the choice to choose the desired **Protection Group** that could be chosen for tape optimization. Select the checkboxes next to the name of the Protection Groups field that you would like to co-locate, and click on **OK**.
4. Uncheck Don't allow backups of different retention periods co-locate on the same tape.

If you select this feature, DPM will ensure that datasets of different retention ranges will not be backed up to the same tape. In our example in this guide, we have daily backups with retention range 12 weeks and quarterly backups with retention range 3 years. So, if you select this option, once a tape is used for a daily backup (whose retention range is 12 weeks), it will not be used for any quarterly backup (whose retention range is 3 years). Similarly, once a tape is used for a quarterly backup, it will not be used for a daily backup.

But since we are using StarWind Virtual Tape Library (VTL), you can decide if this is desired scenario in your case. Ideally for physical tapes, for each short-term tape full backup, a new tape will be used in DPM by design. And for each long-term tape full backup, a new tape will be used as well. The incremental backups will always go onto the same tape.

As mentioned earlier, for VTL scenarios, we would suggest creating more tapes with smaller sizes. Generally, the collocation feature is used to use same tapes for backing up data sources of different protection groups. Thus, we will leave “Don't allow backups of different retention periods to co-locate on same tape” unchecked.
You can also configure advanced configurations for the tape co-location options by clicking on the Advanced button in the Tape Optimization Setup window.

You can control two options:

- **The Write period**

  You can configure **Write period**, that is, the number of days, weeks, months, or years for which the tape will be available for writing. When the period expires, the tape will be marked Offsite Ready.

  If you give large value for write period, tape will not be marked offsite ready and will be used for the next backups for large period of time. This is our case with Virtual Tape Library, because, it is assumed that at some point, physical tapes are meant to be stored offline/offsite and kept.

  As an example, if you give write period as 5 days, and Tape No.1 is used for first short-term backup on Sunday, the same tape can be used for short-term backups on Monday, Tuesday, Wednesday, and Thursday. After Thursday write period of 5 days has elapsed and it will be marked offsite ready. In this case the first recovery point which is taken on Sunday, will be lying in tape even though it will be expired (Expiration tolerance 5 days) before latest recovery point taken on Thursday. DPM will not overwrite a full tape until all recovery points on that tape expire.

- **The Expiry tolerance**

  The **Expiration tolerance** defines the maximum time a recovery point can lie expired on an active tape. This could also be set to any number of days, weeks, months, or years depending on your configuration.
If you give expiry tolerance a very large value you will be maintaining recovery points even when they are expired. In this case your daily backups and quarterly backups can go to same tape, and since in this example we have given large expiry tolerance (3 years), the expired daily backups would still be present along with quarterly backups.

When done, click OK and then click Close to continue.
Configuring DPM for the short erase tape feature

By default, when you erase a tape by using System Center Data Protection Manager (SCDPM), it performs a long erase, this is always a time-consuming process, and it is a very common scenario regardless of the tape type you are using. A faster way is to perform a short erase.

1. Login to your DPM server and open registry editor.

2. Enter the DWORD UseShortErase in the registry and reboot the DPM server. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent

3. Add the value of 00000000 in a DWORD.

4. Short erase is faster but it does NOT erase the data from the tape. If you have a policy in your company that dictates all data from the tape must be erased and unrecoverable, then you shouldn’t use this option. To revert to long erases, please remove this registry key.

5. If you want to erase a tape. Open the Libraries workspace in the Management view and select the desired tape for erase. Right click and select Erase tape.
6. Click **Yes** to erase the selected tape.

7. After short period, the tape will be available to reuse and marked as **Free**. If the “UseShortErase” feature was not enabled, this process will take more time to complete.
Understanding tape reports in DPM

DPM provide you with the information that you will need to keep track of your tapes, so you can manage them more effectively.

In the DPM console, click on **Reporting** view. You have two different tape reports that are very useful:

- Tape Management
- Tape Utilization

The **Tape Management** report provides you information regarding how to manage tape rotation and lists all the libraries that are below the free tape threshold. It’s important to know that data is collected per library and is aggregated for all libraries.

The **Tape Utilization** report will give you the data needed to find the trends that will help you in capacity planning.
Conclusion

Tape is here to stay, because it offers affordable capacity and outstanding long-term vaulting capabilities. Being better in terms of price and capacity than traditional physical tapes including modern high capacity SATA spindles and able to last for decades, it's often included into regulatory requirements for some companies.

StarWind VTL merges with existing infrastructure and fits the backup process into a much smaller backup window. Additionally, it creates a redundant snapshot copy and meets regulatory requirements with decreased backup cost and enhanced performance.

Backup and recovery have been a natural part of the business continuity plan for many years.
By combining StarWind virtual tape library and System Center Data Protection Manager 2016 gives you a unique opportunity to save on storage cost, and protect your critical data against malware, ransomware, and intrusion attacks.

We hope this guide gave you a solid foundation on how to protect your data using System Center Data Protection Manager 2016 and StarWind VTL.

We highly encourage you to deploy and evaluate the current release of DPM 2016 and StarWind VTL. We welcome your comments and feedback.
Charbel Nemnom

Microsoft MVP Charbel Nemnom is an accomplished technical professional with over 13 years of broad IT project management and infrastructure experience serving on and guiding technical teams to optimize performance of enterprise systems. He has practical knowledge of complex systems builds, network design and virtualization. Charbel has extensive experience in various systems, focusing on Microsoft Cloud Platform, Hyper-V, Datacenter Management, Cloud Computing, security, data protection, and many types of monitoring tools as well as a solid knowledge of technical reporting.

Charbel Nemnom
Web-site: http://charbelnemnom.com/
Twitter: https://twitter.com/@CharbelNemnom
Linkedin: https://www.linkedin.com/in/cnemnom

StarWind

<table>
<thead>
<tr>
<th>US Headquarters</th>
<th>EMEA and APAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-617-449-7717</td>
<td>+44 20 3769 1857 (UK)</td>
</tr>
<tr>
<td>1-617-507-5845</td>
<td>+49 302 1788 849 (Germany)</td>
</tr>
<tr>
<td></td>
<td>+33 097 7197 857 (France)</td>
</tr>
<tr>
<td></td>
<td>+7 495 975 94 39</td>
</tr>
<tr>
<td></td>
<td>(Russian Federation and CIS)</td>
</tr>
<tr>
<td></td>
<td>1-866-790-2646</td>
</tr>
</tbody>
</table>

Support Portal: https://www.starwind.com/support
Support Forum: https://www.starwind.com/forums
Sales: sales@starwind.com
General Information: info@starwind.com

StarWind Software, Inc. 35 Village Rd., Suite 100, Middleton, MA 01949
©2017, StarWind Software Inc. All rights reserved.