DXi-Series Configuration and Best Practice Guide

Microsoft Data Protection Manager™

Quantum: 6-67789-01 Rev B

BPG00017A-02

Table of Contents

DXi-Series Configuration and Best Practices Guide for Data Protection Manager from Microsoft

This guide seeks to help Quantum customers who own DXi-Series systems (DXi4000-Series, DXi6000-Series, and DXi8000-Series), and who also use Microsoft's Data Protection Manager (DPM) get the most out of their investment. It is also intended to help Quantum field sales teams by providing guidance to enhance the installation and integration of Data Protection Manager with Quantum DXi-Series systems. This guide includes advice and best practices for using Quantum DXi-Series systems with DPM.

How to use this Guide

This document assumes the reader has basic expertise with Microsoft Data Protection Manager 2010, and/or 2012 as well as basic networking and SAN experience. It also assumes that the reader has a Quantum DXi installed in a working Data Protection Manager environment.

This document provides key recommendations and useful information for quickly setting up a DXi system with Data Protection Manager. It expands on these recommendations and discusses the features and performance tuning considerations.

This document is organized by storage target access method to be employed with Data Protection Manger. In order to utilize Data Protection Manager, the DXi model must be configured for use as a VTL. Data Protection Manager does NOT support Network Attached Storage (CIFS or NFS) as storage target device.

Shortcuts to Quick Start Activities

To go directly to any of the following sections, click that section's name.

Documentation and References

The following is a list of documents, references and links where the user can find additional information regarding specific activities and products. Access to many of the documents below requires a valid serial number. Please have that available when following the hyperlinks to the Quantum documents.

Online documentation for Quantum

http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/Index.aspx#

DXi-Series Management Console

The DXi-Series Management console allow for configuration and monitoring of your storage solution. Refer to the following documents for more information on DXi-Series Management:

- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4700 User's Guide

DXi Replication

Refer to the following documents for DXi-to-DXi Replication setup:

- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4700 User's Guide

Online documentation for Data Protection Manager

Data Protection Manager 2012 Documentation

Refer to the following documents for Getting started, System requirements, Operations Guide and Troubleshooting and Error Codes.

- Getting Started with System Center 2012 - Data Protection Manager
- System requirements
- Operations Guide
- Troubleshooting Guide
- Data Protection Manager Error Codes

Downloadable Documentation

You can download a copy of technical documentation from this site: http://technet.microsoft.com/en-us/library/aa991542. Always use the TechNet library for the most up-to-date information.

Data Protection Manager 2010 Documentation

Refer to the following documents for Administrator Console, System requirement, Client, Setup Help Troubleshooting Guide.

- Data Protection Manager 2010 Administrator Console

- Data Protection Manager 2010 System Requirements
- Data Protection Manager 2010 Client
- Data Protection Manager 2010 Setup Help
- Data Protection Manager 2010 Troubleshooting Guide

Best practices for Data Protection Manager Installation

Best practices include tips and recommendations to help you install or upgrade Microsoft Data Protection Manager 2012 more effectively. For more information about installing Microsoft Data Protection Manager, see the **Data Protection Manager Online Guide**. The following best practices are for preparing to install or upgrade Data Protection Manager. Refer to Microsoft for additional information http://technet.microsoft.com/en-us/library/aa991542

- Back up your server before you install or upgrade any new software.
- Before starting your installation, read the installation instructions at Deploying Data Protection Manager.
- Data Protection Manager supports upgrading from Data Protection Manager 2010. Ensure that QFE3 [KB2581742] has been applied on all Data Protection Manager servers and protected computers (http://www.microsoft.com/en-us/download/details.aspx?id=27218)
- Document your current configuration and settings before you upgrade Data Protection Manager 2010. You can verify that your configuration remains the same after the upgrade is complete.
- If Data Protection Manager Installation fails when trying to configure Reporting with the following error - **The password is shorter than required. (The password could also be too long, be too recent in its change history, not have enough unique characters, or not meet another password policy requirement.)** You have to format the computer and rerun Setup.
- Do not change the installation folder for Data Protection Manager to the root drive. Always install Data Protection Manager inside a folder.
- After installing Operations Manager Agent on the Data Protection Manager server, the following registry key settings are recommended for the data source discoveries to work properly:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Modules\Global\PowerShell] "ScriptLimit"=dword:0000000f

Restart the Health Service (Display name: 'System Center Management') after changing the registry settings. This must be repeated on every Data Protection Manager server that you are monitoring with Operations Manager.

- Monitor your disk space regularly to prevent disk space problems. Data Protection Manager's space requirements may vary depending on usage and installed options. The requirements in the Administrator's Guide do not include space estimates for additional program additions.
- Consult any of the following resources on the Help and Documentation menu if you have questions or difficulties:
  - Use the ***Setup Help Guide*** for comprehensive information about MS Data Protection Manager 2012 installation.
  - Use the MS Data Protection Manager Help documentation as listed in the previous section for topic-based documentation.

- You cannot set end-user recovery options from the remote Administrator Console; this must be done on the Data Protection Manager Administrator Console.

- Data Protection Manager supports protection and recovery for VMM - System Center 2012 only. VMM 2008 R2 is not supported.

- Data Protection Manager does not support protection and recovery for SQL Server 2012 if the *AlwaysOn* feature is enabled.

- The **Copy to tape** option in the Recovery wizard is only available to the Data Protection Manager administrator. The Recovery administrator and Tape administrator do not have permissions to use it.

- If the Express Full backups for SQL Server databases are transferring large amounts of data (almost the size of the primary MDF file), you must install the update KB2471430 (kb2471430) on the SQL Server. This typically happens after you have run DBCC CHECKDB on a Windows 2008 server.

- Data Protection Manager's database cannot be on a clustered or mirrored instance of SQL Server.

- If you are upgrading to Data Protection Manager 2012 from Data Protection Manager 2010, you have to set up tape collocation again.

- While you will be able to upgrade from Data Protection Manager 2010 to Data Protection Manager 2012, Data Protection Manager servers can share a tape library (provided it's recognized by device manager in Windows correctly) you can't have Data Protection Manager 2010 and 2012 servers talking to the same tape library,

- A combination of short-term protection to disk and long-term protection to tape provides the best possible recovery opportunities. It *does* use tape quite well; individual protection groups can't share a single tape or set of tapes. This means that Data Protection Manager 2010 may not be as efficient as it could be when it comes to using tapes. Data Protection Manager 2012 will allow administrators to collocate multiple protection groups to one tape or set of tapes. In other words, tapes can be shared which increases the products overall efficiency.

Summary of Tuning Parameters for Microsoft Data Protection Manager

For Backup Administrators that are well-versed on Microsoft Data Protection Manager and Quantum DXi systems, a summary of suggested parameters/values is present in the following table. As with any modifications to a system that impacts performance and/or tuning, your results may vary and are not guaranteed.

Parameter or Option	**Setting**
Compression	While MS DPM supports compression, to obtain effective deduplication rates, you should NOT compress your backup data before sending it to a DXi appliance.
Encryption	While MS DPM supports encryption, to obtain effective deduplication rates, you should NOT encrypt your backup data before sending it to a DXi appliance.
Reclamation setting	It is recommended to schedule daily reconciliation and reclamation to manage the available space.
Deduplication	Deduplication is a new feature in Windows Server 2012. The implementation of deduplication is volume-based. Data Protection Manager (DPM) supports protection for Windows Server 2012 volumes that have deduplication enabled. To obtain effective deduplication rates, you should NOT deduplicate your backup data before sending it to a DXi appliance.
VTL Options	**Settings**
VTL sign-on string	Microsoft Data Protection Manager will support WHQL certified Libraries and Tape drives as seen in Windows Device Manager. Recommend using VTL Emulate of Scalar i6000
Drive sign-on string	Emulate as per the Data Protection Manager HCL: • Scalar i6k: HP LTO4 • Scalar i6k: HP LTO4
Miscellaneous Options	**Recommendations**
Server Resources	Memory Requirements for All Operating Systems: • 12 GB • 16 GB if you are using deduplication • At least 32 GB for heavily used servers.

Consult the ***Data Protection Manager Online Guide*** for comprehensive information about Microsoft Data Protection Manager 2012 if you have question or difficulties.

Configuring MS Data Protection 2012 with DXi-Series

Configuring MS Data Protection Manager with DXi VTL

Creating a backup image on a virtual tape is no different than creating a backup image on a physical tape. The backup functionality is unchanged.

Data Protection Manager seamlessly integrates with a DXi-Series disk backup system using the VTL interface. Once installed and configured, Data Protection Manager can manage the backups through the DXi and can take advantage of the DXi system's capabilities, such as data deduplication and replication.

VTL Device Path Considerations

One of the key components to ensure that SAN-connected physical and virtual tape libraries are detected properly by backup servers is "serialization." Serialization provides a unique identifier for each device in a physical or virtual tape library to automate device association from multiple backup servers. These identifiers, returned by the VTL devices are separate from the "element address" that defines the position of devices in the library. The element address used by the library's robot or medium changer to manage the tape drives.

Serialization allows the servers running the data protection application (the media servers) to coordinate tape drive configuration by aligning the device serial number with the device's element address. If the Device Configuration Manager does not serialize the devices listed, do not commit the changes, and check the VTL online state. The DXi VTL partition must be online for this to function properly.

Install/Configure Library device driver(s) as required by Data Protection Manager

Always ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and for the HBA(s). Microsoft certified drivers should be loaded for the tape drive for best performance.

If the device is presenting itself properly to the operating system, then it should be supplying the operating system with an inquiry string.

Data Protection Manager must be configured using the VTL interface with a DXi-Series disk backup system. Installing and configuring the DXi and Data Protection Manager server for VTL operations consists of the following major steps:

1. **Configure the DXi for VTL**
2. **Configure Data Protection Manager with Library and Tape Drives**
3. **Configure Data Protection Manager Library Sharing**
4. **Test Backup to DXi VTL storage target device**

Configure the DXi for VTL

A virtual tape library (VTL) is a data storage virtualization technology used for backup and recovery. A VTL presents itself as a tape library with tape drives for use with existing backup software. Virtualizing disk storage as tape allows integration of VTLs with existing backup software and existing backup and recovery processes and policies. The benefits of such virtualization include storage consolidation and faster data restores.

In the Remote Management Console, under the **Configuration** tab, the **VTL** page allows you to configure a DXi to present its storage capacity as VTL (virtual tape library) partitions that are

compatible with Data Protection Manager. You can add virtual tape drives and storage slots to VTL partitions, and you can create and work with virtual tape cartridges. You can also map partitions to hosts.

Partitioning lets you divide the DXi virtual tape drives and storage elements into separate partitions, usable by separate host computers. The **Partitions** page contains a list of assigned tape drives, as well as listing all user-defined partitions that are currently configured on the system. This page also lets you add, edit, and delete partitions.

The **Summary** page displays the maximum number of partitions, the total number of tape drives, and the number of assigned tape drives. The **Summary** page also provides a list of configured partitions on the system. Click the link in the **Name** column to edit the specific partition.

Caution: Ensure that your Data Protection Manager system is properly configured for the correct number of tape drives emulated in the DXi system partition. Failure to do so may cause Data Protection Manager to malfunction or cease to operate.

Note: If you are planning to replicate partitions to another DXi system, you must ensure that every partition name and barcode number on the system is unique. You can NOT have duplicate partition names or barcode numbers on a DXi system or on a system receiving a replicated partition.

The **Create Media** page allows you to create virtual media for a specific partition. Once created, these virtual cartridges are available for backing up data. You can configure the media type, capacity, starting barcode, and initial location on this page.

Note: It is possible to oversubscribe space on the DXi system. The sum total of capacity for all media could be more than the physical capacity of the system. See ***Oversubscription of Space on the DXi*** in the following Best Practices section for more information on this subject.

Configure Data Protection Manager with Library and Tape Drives

To configure the Data Protection Manager Library and tape drives, follow these steps:

1. Before Data Protection Manager can recognize the tape library, you must add the following firewall exceptions:

   C:\Program Files\Microsoft System Center 2012\DPM\SQL\MSSQL10_50.MSDPMV4RC\MSSQL\Binn\sqlservr.exe

   C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe

   C:\Program Files\Microsoft System Center 2012\DPM\DPM\bin\DPMLA.exe

When a DXi is configured as a VTL it will present itself to Data Protection Manager as a standard tape library with drives and cartridges under Windows **Device Manager**.

2. In the Data Protection Manager Administrator Console perform a Rescan operation. When you perform a Rescan operation, Data Protection Manager examines the tape libraries or stand-alone tape drives that are attached to the Data Protection Manager server and updates the information

that is displayed on the Libraries area of the Management workspace in Data Protection Manager Administrator Console. The **Libraries** area displays each stand-alone tape drive, and each tape library and its drives. The **Rescan** operation might take several minutes to complete.

Note: If a library job is already in progress when the Rescan operation begins, the Rescan operation can fail.

3. You use the **Rescan** operation on the **Libraries** area to check for and refresh the state of all new tape libraries and stand-alone tape drives when you make changes to your hardware.

Note: If the tape drives listed on the Libraries area in Data Protection Manager Administrator Console do not match the physical state of your tape drives, see Managing Tapes in Data Protection Manager Help. For example, if drives from a tape library are listed as stand-alone tape drives, or if a stand-alone tape drive displays incorrectly as a drive in a tape library, you need to remap the tape drive information. For more information about remapping tape drives, see Managing Tapes.

Caution: If you are sharing the tape library across multiple Data Protection Manager servers, add the exceptions on all of them.

4. You can temporarily disable a tape library in Data Protection Manager to perform maintenance or repairs. When you are ready to return the tape library to operation, you must enable it. In Data Protection Manager Administrator Console, go to the **Management** view, and then open the **Libraries** workspace. In the **Display** pane, select the tape library or stand-alone tape drive that is disabled. Click **Enable** or **Disable library**.

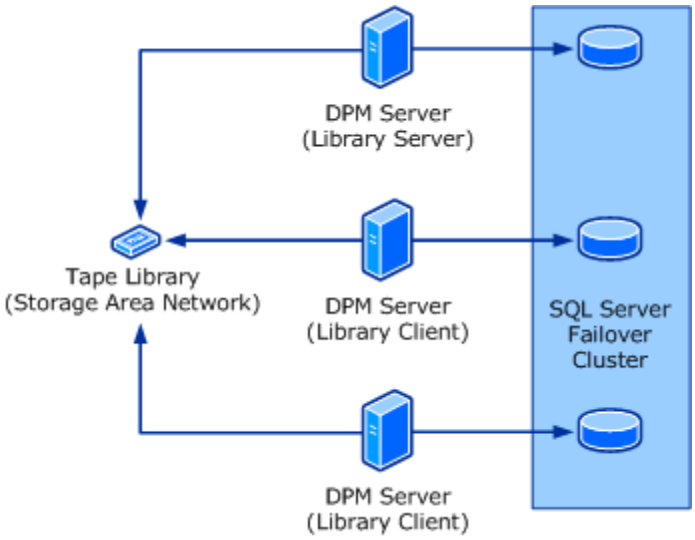
5. Inventory the VTL to identify new tapes and have them recognized by Data Protection Manager. In Data Protection Manager Administrator Console, go to the **Management** view. In the **Libraries** workspace, select a **library**. Click **Inventory**. In the **Inventory** dialog box, select **Fast inventory** or **Detailed inventory**, and then click Start. DXi VTL tapes have virtual bar codes.

   A *fast inventory* involves reading the bar code of each tape in the library. Data Protection Manager can perform a fast inventory for tapes that have bar codes in a tape library that has a bar code reader.

   A *detailed inventory* involves reading the header area of a tape in the library to identify the on-media identifier (OMID) on each tape. Data Protection Manager must perform a detailed inventory when a tape does not have a bar code or the tape library does not have a bar code reader.

Configure Data Protection Manager Library Sharing

With System Center 2012 – Data Protection Manager (DPM), you can share a single tape library across multiple Data Protection Manager servers. The following illustration shows the topology of a shared library.



- The tape library is typically a collection of tape drives that automatically mount and dismount tape media.

Note: The tape library must be in a storage area network (SAN) environment.

- The *library server* is a computer on which Data Protection Manager is installed, the library-sharing command has been run, and the medium changer is enabled.

  A *library client* is a computer on which Data Protection Manager is installed, the library-sharing command has been run, and the medium changer is not enabled.

Note: Data Protection Manager recommends that the system configuration of the library server computer and all library client computers be as similar as possible, and that you do not configure any protection groups on the library server.

All Data Protection Manager Servers using a shared library must use a similar SQL Server setup for hosting Data Protection Manager databases. For example, they should all use a local instance of the Data Protection Manager database or all of them should use a remote instance. You should not have some Data Protection Manager servers using local instance and others using a remote instance.

To configure the Data Protection Manager library sharing, follow these steps:

1. On the computer that will be the library server for the shared library, enable the medium changer by using Device Manager.

2. On each library client computer, ensure that the medium changer is not enabled.

3. Enable Named Pipes protocol for the SQL Server instances of the library server and library client computers. Then restart the SQL service.

4. Run the following commands to configure the Data Protection Manager servers to use a shared library:

   - On each library client computer, open an elevated Command Prompt window, and then run the following commands:

     cd <*system drive*>:\Program Files\Microsoft DPM\DPM\Setup

AddLibraryServerForDpm.exe –DpmServerWithLibrary<*FQDN of library server*>
where <*FQDN of library server*> is the fully qualified domain name of the library server.

- On the library server computer, open an elevated Command Prompt window, and then run the following commands one time for each library client. For example, if your library server supports three library clients, you must run this command three times on the library server.

  cd <*system drive*>:\Program Files\Microsoft DPM\DPM\Setup

  AddLibraryServerForDpm.exe – ShareLibraryWithDpm<*FQDN of library client*>
  where <*FQDN of library client*> is the fully qualified domain name of the library client.

5. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

Important: Do not run these commands on the library server.

Note: Before you run the following commands, on all library client computers ensure that both the SQL Server (DPM2012) and SQL Server Agent (MSDPM2012) services use a domain user account as the logon account, not a local account, which is the default configuration, and that the domain account that is used is a member of the local Administrator group on all of the computers that are sharing the library.

cd <*system drive*>:\Program Files\Microsoft DPM\DPM\Setup

SetSharedDpmDatabase -DatabaseName <**SqlServer\Instance\DatabaseName**> [-DoNotMoveData]
where <*SQLServer**Instance**Databasename*> is the database name of the library server.

Tip: You can find this information in the About Data Protection Manager window as Data Protection Manager's SQL Server. You can copy this information from there using your mouse.

- In Data Protection Manager Administrator Console on the library server, perform a **Rescan**, and then perform a **Rescan** or **Refresh** on each of the library client computers.

Note: The quickest way to see all media on all of the Data Protection Manager servers is to perform a rescan on each followed by a detailed inventory. Next, on any one of the servers, mark a number of media as free and then perform a refresh on the other servers.

After you have configured library sharing, you can use the shared tape library as if it were attached to each Data Protection Manager server.

To promote another Data Protection Manager server to library server, use the following procedure to promote another server to library server:

1. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   cd <*system drive*>:\Program Files\Microsoft DPM\DPM\Setup

   SetSharedDpmDatabase.exe –RemoveDatabaseSharing

   AddLibraryServerForDpm.exe –DpmServerWithLibrary<*FQDN of the library server*>-remove
   where <*FQDN of library server*> is the fully qualified domain name of the old library server.

Note: Ensure that the Data Protection Manager Administrator Console is functioning correctly on each library client.

2. On the computer that you want to promote as the new library server, enable the medium changer in Device Manager.

3. On the computer that you want to promote as the new library server, open an elevated Command Prompt window, and then run the following commands one time for each of the library client computers:

   cd <*system drive*>:\Program Files\Microsoft DPM\DPM\Setup

   AddLibraryServerForDpm.exe –ShareLibraryWithDPM<*FQDN of client library*>
   where <*FQDN of client library*> is the fully qualified domain name of the library client.

4. On each library client computer, open an elevated Command Prompt window, and then run the following commands:

   cd <*system drive*>:\Program Files\Microsoft DPM\Setup
   SetSharedDpmDatabase -DatabaseName <**SqlServer\Instance\DatabaseName**> [-DoNotMoveData]
   where <*SQLServer**Instance**Databasename*> is the database name of the library server.

Tip: You can find this information in the About Data Protection Manager window as Data Protection Manager's SQL Server. You can copy this information from there using your mouse.

Test Backup to DXi VTL storage target device

After you have completed the configuration, you can and should test the configuration by performing a backup jobs and monitoring it results.

Configuring MS Data Protection 2012 for Backup (D2D)

In many organizations, disk-to-disk-to-tape backup is replacing the traditional disk-to-tape backup systems that have been the standard for disaster recovery for many years. A big part of that reason is Microsoft's new server product, Microsoft System Center Data Protection Manager (DPM).DPM can be configured to use disk-based, tape-based, and cloud-based backup systems.

- Disk-Based Backup: disk-based backup is used for short-term data protection operations and allows rapid backup and restore of protected data.
- Tape-Based Backup: although protected data is not initially written to tape, DPM allows backed-up data to be copied to tape for the purposes of meeting long-term data retention and archiving requirements.
- Cloud-Based Backup: DPM can be configured to back up data across the Internet to a disaster recovery facility at a separate data center.

Data Protection Manager 2012 will still not support long-term protection on disk. You still need to use a third-party virtual tape library product if you want to achieve this goal.

In a disk-to-disk backup, data is copied not to a backup tape but instead to a share point on one of the servers on your network. The tape portion of the disk-to-disk-to-tape backup comes in when the network share containing the backup is backed up to tape.

Disk-based storage, also called D2D (disk-to-disk), which is a type of backup in which *data from one computer is stored on the hard disk of another computer*. This contrasts with the more traditional method of backing up data from one computer to a storage media such as tape, which is also called D2T (disk-to-tape). For extra protection, the two methods can be combined in a D2D2T (disk-to-disk-to-tape) configuration, which provides the rapid recovery benefits of disk-based storage in the short term and archive storage for critical data using tape-based storage in the long term.

Best Practices for MS Data Protection Manager with DXi VTL

Deduplication Data Consideration

Deduplication results can be negatively impacted by compression, encryption, software deduplication, and multiplexing. These functions all change the data stream in a way that obscures patterns in the data content. They will reduce the performance and deduplication from any downstream appliance, including DXi systems. To obtain effective deduplication rates, you should NOT encrypt, deduplicate, compress, or multiplex your backup data before sending it to a DXi appliance.

The use of multiplexing was intended for slow source data, and for the minimum transfer rate required by physical tape drives. Multiplexing backup streams was intended to provide more efficient use of a limited number of physical tape drives. Since the virtual tape drives in DXi systems are not susceptible to performance losses from slow data transfer rates, the number of virtual tape drives can easily be increased in quantity without any time penalty for repositioning. It is not necessary to use multiplexing with the DXi systems. Additionally, multiplexing adds additional header information to the data and reduces the deduplication ratio.

Good Candidates for Data Deduplication

Data deduplication can work well with VMware, large databases , PowerPoint presentations, Word documents, Excel spreadsheets, SQL, Oracle , Exchange databases and source code

Not So Good Candidates for Data Deduplication

Data deduplication does not work well with in-line compressed data, SQL with LiteSpeed (in-line compression), Oracle with multi-channel RMAN (in-line multiplex), Exchange 2010, compressed video, compressed audio and compressed JPG images.

For long-term archiving, it is recommended to vault the data to a physical tape device.

Number of Concurrent Tape Drives in Use

Each DXi model has a maximum number of virtual tape drives that can be configured. Each model also has a maximum aggregate throughput rate, which will be divided relatively equally between the virtual tape drives in use. This does not prohibit a single tape drive from using all available bandwidth. The media server typically determines individual tape drive performance.

It is not a good idea to configure the maximum number of virtual tape drives and perform I/O through all of them concurrently. Better performance can be achieved by using a subset of those virtual tape drives at the same time. Quantum expects the customer configuration to distribute those virtual tape drives among multiple media servers, to simplify initial installation by providing dedicated resources to each media server.

Quantum also recommends that backups be staggered, so that only a subset of drives is in use at one time. During a backup, the data transfer rate is primarily controlled by the media server, because the DXi system does not restrict the ingest data rate. This creates the opportunity for one or more media servers to burst data at a higher rate, leaving less bandwidth for the remaining virtual tape drives. Conversely, it supports the coexistence of fast data streams with slow streams, for maximum use of the available bandwidth.

Keep in mind that increasing the number of concurrently active virtual tape drives does not increase the aggregate DXi bandwidth. It could also result in a failed backup job due to a timeout from a bandwidth-starved operation.

The recommended maximum number of concurrently active virtual tape drives for various maximum aggregate bandwidths is listed in the table below.

DXi Model	Max VTDs*	Max # of Concurrently Active VTDs	Max Aggregate Bandwidth
DXi4701	64	32	1650 MB/s (5.9 TB/Hr)
DXi6700	80	80	972 MB/s (3.5TB/Hr)
DXi6701 / DXi6702	256	80	1,580 MB/s (5.7TB/Hr)
DXi6802	256	80	3,299 MB/s (11.9 TB/Hr)
DXi8500**	160	160	1,777MB/s (6.4TB/Hr)
DXi8500***	512	160	3,047MB/s (11.0 TB/Hr)

* Virtual Tape Drives; max # defined in the system
** DXi8500 w/64GB RAM & 2TB drives
*** DXi8500 w/128 GB RAM & 3TB drives

Tape Cartridge Capacity Considerations

Space on a given tape cartridge cannot be reused until after all backup data on that cartridge has expired. The greater the capacity of a cartridge, the longer it will typically take for all data on that cartridge to expire. Expired data continues to take up space on the virtual tape cartridge, as well as in the DXi, until that cartridge is overwritten, relabeled, or erased. This means that lower cartridge capacities are more desirable so that tapes will be returned the Data Protection Manager scratch pool for reuse and overwritten sooner.

There is virtually no relationship between the configured capacity of a virtual tape cartridge and the tape drive emulation that has been configured for the partition:

- Backup/restore operation will span the number of tapes required, ignoring the configured capacity.
- Vaulting/duplicating operations performed by the backup application will ignore the virtual capacity when writing to another cartridge, whether virtual or physical.
- DXi-Series devices limit the maximum capacity permitted by the tape drive emulation; the minimum is 5GB.

The capacity utilization is tracked in COMPRESSED GB, and the data is stored in compressed form. That is, 100GB of data that is 2:1 compressible will be reported as occupying 50GB of virtual tape cartridge space.

Oversubscription of Space on the DXi

Deduplication will reduce the amount of space used on the physical system by the virtual tapes. Users are advised to monitor for Low Space conditions on the DXi and free up virtual media before reaching this threshold. A best practice would be to trigger the Space Reclamation process *before* the DXi reaches approximately 80 percent full.

The **Disk Usage** overview on the **Home** page of the DXi Management GUI displays the following

information about disk usage on the system (Note: values are displayed as an amount and as a percentage of the total capacity in the system):

- **Disk Capacity -** The total usable disk capacity of the DXi.
- **Available Disk Space** - The disk space available for data storage (free space).
- I/O Write Low Threshold state (Yellow) - Free disk space is equal to or less than 500GB + [10GB * (Total system capacity in TB)]
  - **Stop Write state (Red)** - Free disk space is equal to or less than 250GB
  - **Stop I/O state (Red)** - Free disk space is equal to or less than 10GB

Note: For optimal system performance, Quantum recommends keeping the amount of Available Disk Space (free space) at 20% or more.

Note: When disk capacity is low, target replication to the system is paused. In addition, space reclamation is automatically started to free up disk space.

Tape Drive LUN Mapping

It is recommend that mapping the device starting with LUN 0 on each port and **not** skipping any LUNs. A best practice is to zone the VTL devices and the Data Protection Manager Media servers to prevent other servers from taking control of the VTL resources. Additionally, it is recommended to use the HBA driver to bind the devices to a specific address. This helps keep devices in the same order after a reboot. It is also recommended to set the **WWNN = WWPN** for DXi systems. This allows for binding on the HBA to use either WWNN or WWPN.

Quantum DXi-Series VTL devices support reserve and release to accommodate sharing drives. The option allows devices to be shared between Data Protection Manager Media servers. Data Protection Manager 2012 will allow administrators to collocate multiple protection groups to one tape or set of tapes. In other words, tapes can be shared, which will increase the products overall efficiency. The advantage of this is that you will have a pool of drives available to each media server. Other SAN architectures assign drives to each media server and eliminate the shared function. For both conditions, it is a good practice to keep the Data Protection Manager Media server separate from other production servers to eliminate downtime from maintenance. This requires the media servers to have a fast network connection to the source data.

VTL Fibre Channel Performance Tuning

To enhance performance for Data Protection Manager environments, consider using the tuning parameter indicated by the article mentioned below to eliminate interference from the Host System.

According to the Microsoft knowledgebase article “Windows Server 2003 cannot perform backup jobs to tape devices on a storage area network” (http://support.microsoft.com/kb/842411/en-us), you may encounter the following problem:

> “… a conflict in Windows Server 2003 causes a Test Unit Ready (TUR) request issue on SCSI-attached and fiber-attached devices. When this issue occurs, an overflow of TUR requests causes the storage unit not to respond or to respond slowly to SCSI commands. In a SAN environment, any Windows Server 2003-based computer that is zoned to detect the Tape Backup Unit hardware can send TUR requests.” The cause and workaround are

documented in the Microsoft knowledge base article number 842411. Microsoft support link: (http://support.microsoft.com/kb/842411/en-us).

The article referenced above lists the cause of the problem, and a workaround for it.

Handling of Expired Media Data Protection Manager Considerations

When a tape is expired by Data Protection Manager, the event is not directly communicated to the DXi-series device. When trying to use an expired tape in DPM, DPM is not able to use them automatically and will generate an alert for the expired tapes that are being loaded for re-use:

Event Description: The back up to tape job failed for the following reason: (ID 3311)

Event Details:

The tape has been written to by another tape backup application using an unsupported physical block size. DPM supports a physical block of 65536 bytes for writing and a physical block size ranging from 1024 bytes to 65536 bytes for reading. So DPM will not be able to read or overwrite the contents of this tape. (ID 24084 Details: When accessing a new tape of a multivolume partition, the current block size is incorrect (0x80070452))

Go to the Libraries tab in the Management pane, select the tape, and click on Erase tape to erase the content of this tape. After erasing this tape, DPM will be able to use it for backups.

Replication Considerations

For first-time replication setups, it is important to manually replicate the name space once the target system is configured and is online. This facilitates the first replication following the first backup to that share/partition. The replication is only available to NAS shares with deduplication enabled. The DXi supports 128-bit AES encryption for replication. Data is only encrypted while in transit between the replication source and replication target. Data is unencrypted upon arrival at the replication target. Encryption may affect replication performance. You should disable encryption if your WAN is already secured. For more information, please refer to *Quantum DXi-Series Best Practices for Data Replication*.

Space Reclamation

Space management involves two processes: data reconciliation and data reclamation. **Data reconciliation** is used to create a list of what can be removed. It runs automatically every twelve hours, at noon and midnight unless data reclamation is running. **Data reclamation** is the process of deleting the data on the data reconciliation list. It can be scheduled or run manually. There is significant overhead associated with this process and, therefore, it should not be run during periods of high appliance use. In addition, replication, reclamation, and backup stream ingest all consume system resources and should not all be done at the same time.

It is recommended to schedule daily reconciliation and reclamation, to manage the available space. The scheduled time should be configured to start the data reclamation process after daily backups are complete. The default schedule is weekly, and the default time for the data reclamation is set to 12:00 AM on Sunday. These parameters are user configurable; you should configure them for your backup window.

Data Protection Manager Enable Auto Refresh on Server

You can set the auto-refresh interval for the library by using the **Set-DPMGlobalProperty** cmdlet in Data Protection Manager Management Shell. The syntax for the command is as follows:

Set-DPMGlobalProperty -DPMServerName<*DPMServerName*> -LibraryRefreshInterval<*LibraryRefreshInterval*>

Where <*DPMServerName*> is the computer name of the DPM server and <*LibraryRefreshInterval*> is the time interval in minutes.

You must set LibraryRefreshInterval to a value greater than or equal to five (5). Setting it to less than five automatically resets it to zero (0), which means the refresh does not occur.

Note: After you have run the Set-DPMGlobalProperty cmdlet, you must close and then reopen Data Protection Manager Administrator Console for the auto-refresh settings to take effect.

Data Protection Manager Library Server failure

If the library server fails, Data Protection Manager detects the failure and raises an alert. All tape jobs scheduled to run fail, while the library server is down. Data Protection Manager checks at 20-minute intervals to see if the library server is working again. If you cannot resolve the problem on the library server, or do not want to wait for the library server to come back online, you can promote another Data Protection Manager server as the library server.

Data Protection Manager Encryption

DPM supports encrypting data on tape for long-term protection. Encryption can be enabled on all 'Protection Groups'. To obtain effective deduplication rates, you should NOT encrypt your backup data before sending it to a DXi appliance.

Helpful utilities – Guides

The following is a list of documents, references and links where the user can find additional information regarding specific activities and products.

Quantum Web Site

http://www.quantum.com

Guardian Web Site Reference

http://www.quantum.com/ServiceandSupport/Services/GuardianInformation/index.aspx

StorageCare Vision Web Site Reference

http://www.quantum.com/Products/Software/Storagecarevision/Index.aspx

Quantum Service Web Site Reference

http://www.quantum.com/ServiceandSupport/Index.aspx

Call Center Americas:

To contact our world-class support representatives, please refer to the information below:

- Telephone (toll free): 800-284-5101
- Telephone (local): 949-725-2100
- Hours of operation (subject to change without notice): 7 days a week, 24 hours a day with valid contract
- 7x24x4 or 7x24x2 coverage available.
- All other contracts can contact Quantum during normal business days from 5AM to 5PM US Pacific Time.

View our Service-Level Objective:

http://www.quantum.com/ServiceandSupport/ServiceLevelAgreement/Index.aspx

Appendix

Data Protection Manager Management Shell Operations

Some common operations using Data Protection Manager Management shell.

Inventory the Tape Library using Data Protection Manager Management shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] *<String>* **[-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

- Use the following syntax to perform a fast inventory:

  Start-DPMLibraryInventory [-DPMLibrary] *<Library>* **[-FastInventory] [-JobStateChangedEventHandler** *<JobStateChangedEventHandler>***] [-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

- Use the following syntax to perform a detailed inventory:

  Start-DPMLibraryInventory [-DPMLibrary] *<Library>* **-DetailedInventory [-Tape** *<Media[]>***] [-JobStateChangedEventHandler** *<JobStateChangedEventHandler>***] [-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

  For more information, type "**Get-Help Start-DPMLibraryInventory -detailed**" in DPM Management Shell.

Enable a Library using Data Protection Manager Management shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] *<String>* **[-Verbose] [-Debug] [-Error Action** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

- Use the following syntax to enable a library:

  Enable-DPMLibrary [-DPMLibrary] *<Library[]>* **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

For more information, type "**Get-Help Enable-DPMLibrary -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Enable-DPMLibrary -full**" in Data Protection Manager Management Shell.

Disable a Library using Data Protection Manager Management shell

- Use the following syntax to retrieve the library:

  Get-DPMLibrary [-DPMServerName] *<String>* **[-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***]**

- Use the following syntax to disable a library:

  Disable-DPMLibrary [-DPMLibrary] *<Library []>* **[-PassThru] [-Verbose] [-Debug] [-ErrorAction** *<ActionPreference>***] [-ErrorVariable** *<String>***] [-OutVariable** *<String>***] [-OutBuffer** *<Int32>***] [-WhatIf] [-Confirm]**

  For more information, type "**Get-Help Disable-DPMLibrary -detailed**" in DPM Management Shell.

For technical information, type "**Get-Help Disable-DPMLibrary -full**" in Data Protection Manager Management Shell.