Quantum

# DXi-Series Configuration and Best Practices Guide

*For HP Data Protector*

**Quantum: 6-67788-01 Rev C**

**BPG00015A-02**

Quantum
BE CERTAIN

# Table of Contents

# DXi-Series Configuration and Best Practices Guide for HP Data Protector

This guide seeks to help Quantum customers who own DXi-Series systems (DXi4000-Series, DXi6000-Series, DXi8000-Series, and DXi9000-Series), and who also use Data Protector from HP 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 HP Data Protector with Quantum DXi-Series systems. This guide includes advice and best practices for using Quantum DXi-Series systems with Data Protector.

## How to Use This Guide

This document assumes that the reader has basic expertise with HP Data Protector, as well as basic networking and SAN experience. It also assumes that the reader has a Quantum DXi installed in a working Data Protector environment.

This document provides key recommendations and useful information for quickly setting up a DXi system with HP Data Protector. It expands on these recommendations and discusses the features and performance tuning considerations relevant to various storage access methods.

This document is organized according to the various storage target access methods to be employed with HP Data Protector. Depending on the DXi model, the DXi can appear as a Virtual Tape Library (VTL) storage device over Fibre Channel (FC) or as a Disk based target. These access methods are discussed in the following order.

- DXi VTL
- DXi NAS - NFS and/or CIFS

## 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 you 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 documents.

## *Online Documentation for your Quantum product*

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

### DXi-Series Management Console

The DXi-Series Management console helps you configure and use your storage solution. Refer to the following documents for more information on DXi-Series Management:

- DXi9000 User's Guide
- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4800 User's Guide
- DXi4700 User's Guide
- DXi4500 User's Guide
- DXi V-Series User's Guide

### Virtual Tape Library Setup

Refer to the following documents for VTL setup:

- DXi9000 User's Guide
- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4800 User's Guide
- DXi4700 User's Guide

### Network Attached Storage

Refer to the following documents for NAS Share setup:

- DXi9000 User's Guide
- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4800 User's Guide
- DXi4700 User's Guide
- DXi4500 User's Guide
- DXi V-Series User's Guide

### DXi Replication

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

- DXi9000 User's Guide
- DXi8500 User's Guide
- DXi6800 User's Guide
- DXi6700 User's Guide
- DXi4800 User's Guide
- DXi4700 User's Guide
- DXi4500 User's Guide
- DXi V-Series User's Guide

## *HP Installation Documentation*

The following Data Protector documentation is available at this location
http://support.openview.hp.com/support.jsp

- Compatibility Matrices
- Data Protector Installation and Licensing Guides
- HP Support and Drivers
- Enterprise Backup Solution with HP Data Protector Implementation guide

## Best Practices for Data Protector Installation

Best practices include tips and recommendations to help you install or upgrade HP Data Protector more effectively. The following best practices are for preparing to install or upgrade Data Protector:

- Visit the HP Support Web site to check for updates to the documentation. http://www8.hp.com/us/en/support-drivers.html
- Review the Readme document and Documentation Addendum for updates to the Data Protector Administrator's Guide.
- Use only standard ANSI characters for the computer name of the computer on which you want to install Data Protector. You may receive errors if you install Data Protector on a computer with a name that uses non-standard characters.
- Document your current configuration and settings before you upgrade Data Protector. You can verify your configuration after the upgrade is complete.
- Back up your server before you install or upgrade any software, including Data Protector. Pause or stop all jobs before upgrading Data Protector.
- Close all instances of the Data Protector Administration Console before the upgrade and stop the Omniback services.

The following best practices are for during the installation process and the upgrade process:

- Use an uninterrupted power supply (UPS) for your Data Protector server during the installation. A UPS helps ensure that you do not have a failed installation due to a power outage.
- Wait until after the installation to make configuration changes. Do not make configuration changes during the installation.
- Run the installation wizard from the local server, from a DVD image on the local server.

The following best practices are for after the installation process or the upgrade process:

- Run Microsoft Windows Update on Windows servers.
- Monitor your disk space regularly to prevent disk space problems. Data Protector's space requirements vary depending on usage and installed options.
- Consult any of the following resources on the Help and Documentation menu if you have questions or difficulties:
- Use the following link for comprehensive information about Data Protector:
    - http://support.openview.hp.com/support.jsp
    - Use the Data Protector Help for searchable, topic-based documentation.

## *Summary of Tuning Parameters for Data Protector*

**For backup administrators who are well versed on HP Data Protector and Quantum DXi systems, the following table offers a summary of suggested parameters/values**. 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** | Do not utilize Data Protector's Compression feature. See **Configuring HP Data Protector with the DXi-Series** on how to disable this function within Data Protector |
| **Encryption** | Do not utilize Data Protector's Encryption feature. See **Configuring HP Data Protector with the DXi-Series** on how to disable this function within Data Protector |
| **Deduplication** | Do not utilize Data Protector's Deduplication feature. See **Configuring HP Data Protector with the DXi-Series** on how to disable this function within Data Protector |
| VTL Options | Settings |
| **VTL sign-on string** | Use native DXi Inquiry when possible. Scalar i2000 emulation has also been tested successfully with Data Protector. |
| **Drive sign-on string** | Emulate as per the Data Protector HCL:<br>• DXi9000:<br>• DXi8500: HP LTO4/5 or IBM LTO4/5 recommended<br>• DXi6xxx: HP LTO4/5 or IBM LTO4/5 recommended |
| **Direct Library Access option** | Enable if multiple computers in a cell need to control the virtual tape library and devices, provided they are configured in Data Protector Cell Manager with multiple working paths to these devices. |
| **SCSI Reserve/Release option** | Enable |
| **Use Lock Name option** | Default |
| Miscellaneous Options | Recommendations |
| **Server Resources** | Set up no more than 1-2 drives per 3.xGHz CPU core. The server should have 2GB RAM, plus 1GB per drive. |
| **Server Name** | Use only standard ANSI characters for the computer name of the computer on which you want to install Data Protector. You may receive errors if you install Data Protector on a computer with a name that uses non-standard characters. |
| Global options | See the **HP Data Protector global Options Considerations** section later in this document for additional information |
| | |
| Windows OS Options | Recommendations |
| **Services** | • Disable the Removable Storage Manager (RSM) service on Windows. (No longer present in Win2003/2008.)<br>• Service Management Usage:<br>omnisv (-start \| -stop \| -status \| -start_mon \| - version \| -help) |
| **Network** | On heavy utilized Windows system consider increasing TCP/IP timeout on Data Protector media server. Reference Microsoft Knowledge Base http://support.microsoft.com/kb/q191143/ |

| | |
|---|---|
| | TcpMaxDataRetransmissions<br><br>Adjusting the following TCP/IP setting by adding a subkey in the registry should reduce the number of timeouts by allowing more time for the connection to complete. This setting is not present in the registry by default.<br><br>Start Registry Editor (Regedt32.exe) and go to the following subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters<br><br>On the Edit menu, click Add Value, and then add the following information:<br>Value Name: TcpMaxDataRetransmissions<br>Value Type: REG_DWORD - Number<br>Valid Range: 0 - 0xFFFFFFFF<br>Default Value: 5 Decimal<br>New Value: 10 Decimal<br><br>Click OK, and then quit Registry Editor.<br>Reboot after registry change has been made. |
| | Apply the following Microsoft hot fixes to improve performance:<br>• http://support.microsoft.com/kb/979612<br>• http://support.microsoft.com/kb/982383 |
| UNIX OS Options | Recommendations |
| **HPUX** | The schgr and stape (eschgr and estape) drivers have to be loaded in the HPUX kernel, before adding discovering and adding the devices in Data Protector. |
| | See the Link to NFS client settings later in this document for additional information |

Consult any of the following resources on the Help menu if you have questions or difficulties:

- Use http://support.openview.hp.com/support.jspl or comprehensive information about Data Protector.
- Use the Data Protector Help option in the Data Protector administration GUI for searchable, topic-based documentation.
- HP Data Protector GUI provides contexts for all major management functions, including Interactive Backup Wizards for configuring Backup jobs.

# Configuring HP Data Protector with the DXi-Series

## *Configuring Data Protector 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.

The DXi VTL is viewed though Fibre Channel interfaces and appears as a virtual library with virtual drives and cartridges. During backups, the application creates a backup image on the virtual tape cartridges.

### VTL Device Path Considerations

One of the key ways 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 is 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. This enables Data Protector device discovery to align these two addresses, reducing the potential for improper configuration.

If the Device Configuration Manager does not serialize the devices listed, do not commit the changes, and be sure to check the VTL online state. The DXi VTL partition must be online for this to function properly.

The Quantum recommended device identification for each DXi system is the native mode (in other words, use the DXi inquiry response string as the identification for each model, respectively). This allows product identification for the service teams at both HP and Quantum.

When using the native device mode, Windows environments will display the device in the Device Manager as an *unknown media changer*. This is normal and not an error, and does not create a problem for Data Protector. If the customer environment has requirements for a specific changer device for compatibility, the Quantum DXi products support emulation of many popular devices to meet those requirements.

Always ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and HBA.

To verify that the drivers have been loaded for the tape drive, return to Device Manager in

Windows and open the properties of the Tape Drive. Verify that the Driver is at the latest level.

### Supported Hardware Compatibility List

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

For the device to work properly within Data Protector, the inquiry string that the device provides must match exactly with what is documented on the HCL. HP certifies Libraries and Tape drives separately. See http://support.openview.hp.com/support.jsp

The following steps outline the configuration process at a high-level. For detailed instructions, refer to the HP Data Protector Guides.

- **Configuring the DXi for VTL**
- **Configure Data Protector with Library and Tape Drives**
- **Test Backup to DXi VTL storage target device**
- **Advanced Tape Drive Options (under Tape Drive Settings)**

## Configuring the DXi for VTL

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

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 standard backup applications. 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.

**Note:** Use DXi Native (e.g. DXi6800) or Scalar i6000 emulation for the library and HP or IBM LTO emulation for the tape drives

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 Protector system is properly configured for the correct number of tape drives emulated in the DXi system partition. Failure to do so may cause Data Protector 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 Protector with Library and Tape Drives

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

- Install the Data Protector Cell Manager system to configure and control devices and clients within the cell. By default, cell manager installations include media and disk agents, along with a user interface. UNIX Install Path:

  <HP DP Source>/Bxxxx-xxxxx/LOCAL_INSTALL/omnisetup.sh

Example: <install path>/omnisetup.sh –CM, installs a cell manager with default agents and a user interface.

- UNIX Binary Path: /opt/omni/bin/xomni - Launches the Data Protector user interface.
- Connect DXi VTL via FC SAN to the Data Protector server.

**Note:** HP Data Protector supports Quantum's Virtual Tape Libraries (VTL) as well as CIFS and NFS File Library devices. If necessary, install the latest SCSITab to ensure support for attached Tape devices, physical or emulated, within the VTL.

Link to HP Support downloads: http://www.hp.com/support/downloads/

- HP-UX drivers and discovery. Verify that the latest drivers are installed.
- HP-UX pass-thru drivers for Autochangers:
  The schgr and stape (eschgr and estape) drivers have to be loaded in the kernel before discovering and adding the devices in Data Protector.
- To review the special file, execute the following command:
  # **ioscan –fn**
- Review the sp (special file) that the library and tapes were created.

  Example:
  **Autoch** 30 0/4/1/1.1.3.255.0.0.0 schgr NO_HW DEVICE QUANTUM DXi6800 /dev/rac/c7t0d0

  **tape**50 0/4/1/1.1.3.255.0.0.1 stape NO_HW DEVICE HP Ultrium 5-SCSI/dev/rmt/c7t0d1BEST /dev/rmt/c7t0d1BESTb /dev/rmt/c7t0d1BESTn /dev/rmt/c7t0d1BESTnb

  **tape** 52 0/4/1/1.1.3.255.0.0.2 stape NO_HW DEVICE HP Ultrium 5-SCSI/dev/rmt/52m /dev/rmt/52mn /dev/rmt/c7t0d2BEST /dev/rmt/c7t0d2BESTn

If these were not created, run the following command to install the special files in the devices directory (/dev):
# **insf –emc and mt commands**

Use the following mc and mt commands to manipulate the library and tape drives directly:

Examples:

Review a slot in the library
**# mc -p /dev/rac/c26t0d1 -r S**

Review the drives in the library
**# mc -p /dev/rac/c26t0d1 -r D**

Review the cab or mailbox in the library
**# mc -p /dev/rac/c26t0d1 -r I**

Move a tape from Slot 1 to Drive 5
**# mc -p /dev/rac/c26t0d1 –s S1 –d D5**

Eject the tape from drive 5
**# mt –f /dev/rmt/5m offline**

Move a tape from Drive 5 to slot 20
**# mc -p /dev/rac/c26t0d1 –s D5 –d S20**

**Additional Support Resources**

Devbra utility lists the Changer and Tape drives and their paths.
Ex. <Install Path>\Omniback\bin\Devbra.exe –dev

**Note:** Data Protector includes a GUI for both Windows and UNIX platforms. Command line and Java GUI support is also provided for Windows and UNIX. Clients connect through port 5556 to access the Java GUI.

- Map the DXi VTL to the host on the appropriate FC connection for target devices using the DXi configuration GUI
- Verify the SAN-attached VTL is visible and properly configured within the Data Protector operating system.

**Note:** It may be necessary on some UNIX platforms to remove stale device entries in the OS prior to discovering devices and configuring them in HP Data Protector. Data Protector provides an Auto-configure option for configuring SCSI libraries and tape drives. Alternatively, devices may be added manually through the user interface.

**Auto configuration process:**

- Navigate to the Devices & Media window in the Data Protector GUI (Data Protector refers to the pull down menu options as “contexts”)
- Right-click on Devices in the left pane.
- Select “Autoconfigure Devices” to open the Wizard.
- Select the client system that is connected to the VTL from the list and click Finish

**Manual configuration process**

- Enter details:
  Device name: Example: Scalar i6000
  Description: optional
  Client: Select the client to which the device is connected

Device Type: SCSI Library
Interface Type: SCSI

- Click Next
- Select the appropriate SCSI address from the pull down options. Click Add.
- After selecting next, select the appropriate media type, e.g. LTO
- Click Finish

Add tape drives in a similar manner and associate them with the newly created library from the previous step.

- Configure Additional Library Options
  - Under Properties:
    General: Multipath Device support
    Control: Barcode Reader support
    SCSI Reserve/Release support
    Repository: Limit the slots, presented by the library, if desired

## Test Backup to DXi VTL storage target device

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

**Configuring and running a test backup**

1. Select Backup from the Data Protector pull down menu
2. Select the Task tab at the bottom of the left pane
3. Choose a sample dataset to back up from the file system tree
4. Select the Storage Target
5. Choose additional options if needed. Do **not** choose source-side deduplication.
6. Specify a schedule or skip to next step
7. Start the interactive backup – backup type: Full

Job status is displayed automatically.

**Restoring from a backup**

By default, backup objects are restored to the same location they were backed up from.

1. Select Restore from the Data Protector pull down menu
2. Select the file system object you wish to restore in the left pane
3. In the right pane select the files you wish to restore
4. Select tabs for options including: Destination, Devices, Media, Copies, and Restore Summary.
5. Select Restore
6. Review selection and select Finish

Job status is displayed automatically.

## Advanced Tape Drive Options (under Tape Drive Settings)

Direct Library Access option

The Use Direct Library access option allows for multiple computers in a cell to control the virtual tape library and devices, provided they are configured in Data Protector Cell Manager with multiple working paths to these devices. e.g.: A cell manager and a client are both configured with SAN connections to a VTL. If the cell manager loses its FC connection, there is still a path to it from the client using Direct Library Access.

### SCSI Reserve/Release option

Selecting this option prevents access to SCSI devices (Library and Tape drives) while they are being utilized by another process.

### Use Lock Name option

Selecting the device lock name option will ensures that Data Protector will not try to use the same device with a different name at the same time. The user can create lock names for the devices or go with default names assigned.

## *Best Practices Guide with DXi VTL*

### Robot/Media Changer Device Serialization Considerations

One of the key requirements for ensuring 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, which are 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 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. This enables Data Protector device discovery to align these two addresses, reducing the potential for improper configuration.

If the Device Configuration Manager does not serialize the devices listed, do not commit the changes, and be sure to check the VTL online state. The DXi VTL partition must be online for this to function properly.

It is recommended that device identification used for each DXi system be the native mode for that system. (In other words, use the DXi4700, DXi4800, DXi6700, DXi6802, DXi8500 or DXi9000 inquiry response string as the identification for each model, respectively.) This allows product identification for the service teams at both HP and Quantum.

When using the native device mode, Windows environments will display the device in the Device Manager as an *unknown media changer*. This is normal and is not an error or a problem for Data Protector. If the customer environment has requirements for a specific changer device for compatibility, the Quantum DXi products support emulation of many popular devices (such as the Quantum Scalar i6000) to meet those requirements.

### Device Driver and Firmware level

Ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and for the HBA.

### 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 Protector 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 Protector media servers. 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 Protector media server separate from the production server, to eliminate downtime from maintenance. This requires the media servers to have a fast network connection to the source data.

### 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) |
| DXi4800 | | | |
| 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) |
| DXi9000 | | | |

* 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 Protector 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.

Quantum's general guidance is to specify a smaller virtual tape cartridge capacity, such as 50GB to 100GB, for the reasons mentioned above. For Data Protector recommendations on media management, refer to http://www.hp.com/cgi-bin/hpsupport/index.pl

## 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.

## Recommended Handling of Expired Media

When a tape is expired or recycled by Data Protector, there is no direct communication of the event to the DXi. The result is that a tape may be displayed as empty or SCRATCH in the Data Protector graphical interface, but will show the same tape on the DXi GUI as containing data. This indicates the data on the expired tape is still using space on the DXi.

To reclaim this space, we recommend using Data Protector's graphical interface to re-label the expired media. This new label is a data block written to the virtual tape cartridge at the beginning of tape, effectively blanking the tape. The DXi VTL will act similarly to a physical tape and the data after the label becomes no longer accessible. The space reclamation can be initiated at a scheduled time or started manually from the DXi GUI. Additional information about the reclamation process can be found in the DXi-Series User Manual.

## Copy to physical Tape

Migrating data to physical tape allows for long term archiving of sensitive data. After copying data, the user can free up the media resources and reclaim space on the DXi.

The close integration of DXi and Data Protector also allows you to change media types and sizes when data is moved from virtual to physical media, while maintaining a single point of management. For example, data from several small virtual cartridges might be consolidated onto a single, larger physical piece of media.

## VTL Fibre Channel Performance Tuning

To tune performance for Data Protector Environments, refer to HP documentation at http://bizsupport2.austin.hp.com/

### Recycling Expired Media within Data Protector

Under Devices and Media -> Pools -> Default Media Pool, select the media you wish to recycle. Data Protector will then allow for it to be overwritten in future backup operations. The user can also format the media, to free up space on the DXi, immediately.

### Data Protector Block size and transfer size

As with physical tape, larger tape block sizes and host transfer sizes are of benefit. This is because they reduce the amount of overhead of headers added by the backup application and also by the transport interface. The recommended minimum is 256 KB block size, and up to 1 MB is suggested.

### Media Management in HP Data Protector

The following media operations are supported on the virtual tape drives:

- Barcode Scan
  - Inventory media by barcode
- Format Medium
  - Data Protector writes its own header on each tape so it can be recognized later. This can be done manually, as described in this section, or automatically.
- Scan Medium
  - Scan contents of media, one at a time or multiple in parallel.
- Copy Medium
  - Copy the contents of one tape to another.
- Eject & Enter Media from Mailslot
  - Not supported in VTL.
- Import/Export
  - When a tape is moved from a Storage Slot to an I/E mailslot, depending on the Auto Export setting, the media:
  - Will be removed from the virtual I/E slot if Auto Export is enabled. (Default) The user has the option to recycle or import the tape via the DXi GUI
  - Will remain in the virtual I/E slot if Auto Export is disabled.
- Verify Medium
  - This process checks that the data format is valid on a tape. It will update the Internal Database, following the Verify, which can take a long time, depending on how much data is on the tape.
- Cleaning
  - *Cleaning functions are not supported in a Virtual Tape Library (VTL).*

### Additional Best Practice Considerations

Several operational considerations are common to two access methods (VTL and NAS). See Common Operational Considerations section at the end of this document for more information on Deduplication, Encryption, Compression, Backup Streams and Replication.

## *Configuring Data Protector with DXi NAS*

A NAS (Network Attached Storage) unit is essentially a self-contained computer connected to an Ethernet network, with the sole purpose of supplying data storage services to other devices on the network. Several DXi models can present themselves as a NAS appliance for backup purposes. Before you can use a DXi system as a NAS appliance, you must first configure a NAS share on the DXi.

A DXi system can serve as a NAS backup system where the following protocols are supported:

- **CIFS Protocol -**The CIFS (Common Internet File System) protocol defines a standard for remote file access using many computers at a time. This protocol allows users with different platforms to share files without installing additional software. This protocol is used with Windows networks.
- **NFS Protocol** - The NFS (Network File System) protocol was originally designed by Sun Microsystems and allows all network users to access shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP. Users can manipulate shared files as if they were stored locally on the user's own hard disk. With NFS, computers connected to a network operate as clients while accessing remote files, and as servers when providing remote users access to local shared files. This protocol is used with UNIX/Linux networks. The Quantum Network-Attached Storage (NAS) appliance is intended to act as a target for backup applications. This includes Network-Attached Storage or shares. Data Protector can use a NAS share as a Backup-to-Disk Target.

### NAS Device Path Considerations

**Network segmentation** is the process of splitting a single network into several sub-networks or segments. The advantages of a segmented network are improved performance and security. Performance is improved because there are fewer hosts on the segmented network, which in turn minimizes local traffic. Security is improved because the data traffic is contained on this segment and is not visible to the outside network.

**Note**: If you are using network segmentation and Automated Deployment Services (ADS), you must use the data segment IP information for ADS management, NOT the management segment. ADS uses the Server Message Block (SMB) data protocol to manage the NAS shares on your system, which requires that the management traffic use the data segment.

DXi systems allow you to configure your network for separate segment types. The three primary segments are defined by the type of network traffic that can be used on that segment. The three types of network traffic are:

- **Replication traffic** - This segment is used exclusively for replication data movement.
- **Management traffic** - This segment is used exclusively for DXi Series remote management (Web page access).
- **Data traffic** - This segment is used exclusively for NAS data movement.

Each network segment has its own network interface (IP address, network mask, and default gateway). In this way, the segment is separated from other network segment traffic.

**Note:** If you are using the Round Robin (Mode 0) option, and you have either a Dell or CISCO switch, the ports that connect to the DXi must be bonded.

HP Data Protector seamlessly integrates with a DXi-Series disk backup system using the NAS (CIFS or NFS) interface. Once installed and configured, Data Protector can manage backups through the DXi and take advantage of the system's capabilities, such as data deduplication and replication.

Installing and configuring the DXi and Data Protector for NAS operation consists of the following major steps, which are discussed below:

- **Configure the DXi for NAS**
- **Configure the Data Protector NAS Storage Device**
- **Test Backup to DXi NAS storage target device**

## Configure the DXi for NAS

The DXi system allows you to configure it to present its storage capacity as NAS (Network Attached Storage) shares that are compatible with Data Protector. You can create NAS shares for use with Windows or Linux networks. You can also join the DXi to a Windows domain or workgroup, and manage users.

In the DXi Remote Management Console (the GUI) the **Configuration** page allows you to configure many of the features of the DXi, including storage presentation. A NAS license must be installed on the DXi prior to configuring NAS shares.

Configuring the DXi for NAS lets you choose which network protocol will be used as the transport method for backing up data from client machines to the Data Protector media server. CIFS (Windows) and NFS (UNIX/Linux) are available on the **NAS > Summary** tab. After NAS Shares have been configured on the DXi, Data Protector can be configured to use these shares as storage resources.

## Configure the Data Protector NAS Storage Device

1. Configuring a file library device:
   Create a share on the DXi Target, CIFS for Windows or NFS for UNIX.
2. Mount the share to the backup server if it is NFS.
3. For CIFS/Windows support configure workgroup or Domain within the DXi GUI. Also add additional users as required.
4. Under the Data Protector GUI select Devices & Media.
5. Right-click Devices and select Add Device to open the device definition pane.
6. Enter details:
   Device name: Example: File Library Device 01
   Description: optional
   Client: Select the client to which the device is connected
   Device type: Select File Library
7. Click Next
8. Specify the directory for the file library device you created in step 1 and click Add
   Example:
   Windows = \\hpdpserver\cifsshare or
   Unix = /nfsshare

   Where cifsshare is a DXi CIFS share and /nfsshare is an active mount point for a DXi NFS share.
9. Click Next. In the Results Area, select the media type: File.
10. Click Finish

**Note:** Scan and Format operations will not function until after the first backup is run which creates

media (referred to as slots) on the target share.

### Test Backup to DXi NAS storage target device

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

1. Select Backup from the Data Protector pull down menu
2. Select the Task tab at the bottom of the left pane
3. Choose a sample dataset to back up from the file system tree
4. Select the Storage Target
5. Choose additional options if needed. Do **not** choose source-side deduplication.
6. Specify a schedule or skip to next step
7. Start the interactive backup – backup type: Full

Job status is displayed automatically.

**Restoring from a backup**

By default, backup objects are restored to the same location they were backed up from.

1. Select Restore from the Data Protector pull down menu
2. Select the file system object you wish to restore in the left pane.
3. In the right pane select the files you wish to restore
4. Select tabs for options including; Destination, Devices, Media, Copies, and Restore Summary.
5. Select Restore
6. Review selection and select Finish

Job status is displayed automatically.

## *Best Practices Guide with DXi NAS*

### Number of Shares Considerations

Quantum DXi systems support both CIFS (Windows-based) and NFS shares. Each system can support multiple NAS shares, with a maximum of 128 shares. It is recommended that users create only the required number of shares for each media server. DXi systems can support concurrent NFS and CIFS shares, and can support Fibre Channel VTLs concurrently with those NFS and CIFS shares.

When using NAS shares on DXi systems, it is recommended to create at least one share for each media server to use. Media servers should not share the NAS shares during normal backup operations. Root access to an NFS share is not allowed, and the access rights will be changed to **nfsnobody** as a security precaution. This does not impact the access to the share from the backup application.

### Network Share Access Control Considerations

In Windows Active Directory environments, the share acts as the target for Data Protector. The share is not intended as primary storage or drag-and-drop storage. A best practice is to create a new account and workgroup, as opposed to joining the domain, to limit access and prevent accidental file deletion by another user. It is recommended that you DO NOT reconfigure or delete NAS shares while data is being written. There is no mechanism to detect the I/O and provide a warning to the user.

### Network Considerations

Some network considerations include:

- Use a dedicated network for backup data, or use QoS features that guarantee network bandwidth. Another option would be to use virtual networks (VLANs) to segregate backup from production network traffic.
- Configure network interface cards (NICs) in the server and clients, and set routers to full duplex.
- Use only CAT 5e or CAT 6 cables for 1Gb/s networks and SFP+ Optical or TwinAx for 10 GbE networks.
- If you are using a DNS server, verify that the DNS server configuration settings are correct by using **nslookup** on the host name, as well as the IP address.
- It is also a good idea to add the HOST NAME and IP Address to the host file.
- Use multiple DXi ports when connecting to the network. The more DXi Ports used, the better the performance capability will be across the ports.
- For redundancy, connect at least two DXi ports to an Ethernet switch.
- Set each switch port used by the DXi to **auto-negotiate/auto-sensing**. The DXi network interface cards are preset to auto/auto and cannot be changed.
-

### Data Protector Storage Settings and Tuning Considerations

When using a DXi as NAS for a Backup-to-Disk target with Data Protector, consider the following when you create a backup-to-disk folder:

- Set the maximum size for backup-to-disk files to an appropriate size. If you create small but numerous files, performance may be slow, since the computer must still process each file. However, if you create large files, file system limitations can cause memory allocation problems or network issues. These issues can be a problem if you store files across a network.

## NFS/CIFS Recommended Mount Options

### *Sun Solaris NFS Client Settings*

Change socket buffer size:

*Solaris# ndd –set /dev/tcp tcp_xmit_hiwat 4194304*
*Solaris# ndd –set /dev/tcp tcp_recv_hiwat 4194304*
*Solaris# ndd –set /dev/tcp tcp_max_buf 4194304*
*Solaris# ndd –set /dev/tcp tcp_cwnd_max 2097152*

**NOTE**: 1M and 4M are both fine. Also, as per Solaris documentation, some of these can be added in */etc/system* file for persistence.

*set tcp:tcp_xmit_hiwat = 4194304*
*set tcp:tcp_recv_hiwat = 4194304*

**NOTE**: Set the socket buffers before doing mounts from clients. If they are already mounted, clients need to unmount and remount for the settings to take place. The unmount and remount may be done after the client is fully configured.

Verify the settings by issuing the command *ndd –get /dev/tcp tcp_recv_hiwat*

OPTIONAL. If your client has multiple NICs bonding can be beneficial.

Create Link aggregation group with LACP:

*Solaris# dladm create-aggr –d bge0 –d bge1 1*
*Solaris# ifconfig aggr1 unplumb*
*Solaris# dladm modify-aggr –P L4 –l active 1*
*Solaris# ifconfig aggr1 plumb <ip> netmask <netmask> up*

Verify the settings by issuing the commands:

*dladm show-aggr*
*dladm show-aggr –L*

Add the following lines to */etc/system* to support > 32K rsize/wsize:

*set nfs:nfs3_bsize=1048576*
*set nfs:nfs3_max_transfer_size=1048576*
*set nfs:nfs3_max_threads=32*

**NOTE**: this next step requires a reboot prior to mounting.

Mount with rsize/wsize set to 1M:

*mount –o vers=3,tcp,rsize=1048576,wsize=1048576 …*

**NOTE**: If the settings above are executed correctly, the default rsize, wsize should be 1M without a need for specifying in the mount command.

Verify the actual rsize and wsize:

*nfsstat –m*

### *Linux NFS Client Settings*

Change socket buffer settings to 4M default. Append these lines to */etc/sysctl.conf:*

*net.ipv4.tcp_rmem = 4194304 4194304 4194304*
*net.ipv4.tcp_wmem = 4194304 4194304 4194304*
*net.ipv4.tcp_mem = 10485760 10485760 10485760*
*net.core.netdev_max_backlog = 30000*

Run the command *sysctl –p* for the newly added configuration to take effect. Verify the configuration by running *sysctl net.ipv4.tcp_rmem*, it should show *4194304 4194304 4194304.*

**Note**: Set the socket buffers before doing mounts from clients. If they are already mounted, clients need to unmount and remount for the settings to take place. The unmount and remount may be done after the client is fully configured.

OPTIONAL: If your client has multiple NICs bonding can be beneficial.

Create Link aggregation group with LACP and add bonded round robin policy by adding this line in */etc/modprobe.conf*:

*options bonding mode=6 miimon=500*

**Note**: During this testing, in lieu of LACP, Layer3+4 xmit_hash policy was also successfully used to reduce TCP retransmissions. In the */etc/modprobe.conf*, add the line:

*options bonding mode=2 xmit_hash_policy=layer3+4 miimon=500*

**Note**: this step needs a reboot.

Mount with rsize/wsize set to 1M.

*mount –o vers=3,tcp,rsize=1048576,wsize=1048576 …*

**Note**: The older versions of Linux (pre-2.6.16) only support maximum of 32K rsize/wsizes that are not optimal. 2.6.18 and recent versions showed better performance. Verify the mount options by running the command *cat /proc/mounts*

#### *IBM AIX NFS Client Settings*

Change socket buffer settings to 4M default. Append these lines to */etc/sysctl.conf*

*/usr/sbin/no -o tcp_sendspace=4194304*
*/usr/sbin/no -o tcp_recvspace=4194304*

To make them permanent, add the following lines into the */etc/rc.net* file:

*/usr/sbin/no -o tcp_sendspace=4194304*
*/usr/sbin/no -o tcp_recvspace=4194304*

OPTIONAL: If your client has multiple NICs bonding can be beneficial. Configure the Etherchannel by using the *smit etherchannel* command. Mount with rsize/wsize set to 1M.

*mount –o vers=3,tcp,rsize=1048576,wsize=1048576*

**Note:** AIX clients may not scale past 50 streams on some servers.

#### *HP HP-UX NFS Client Settings*

Change socket buffer settings to 4M default.

*# ndd -set /dev/tcp tcp_recv_hiwater_def 4194304*
*# ndd -set /dev/tcp tcp_xmit_hiwater_def 4194304*

To make the changes permanent add the following lines to the /etc/rc.config.d/nddconf file and issue the command “ndd –c” to activate the changes:

*TRANSPORT_NAME[0]=tcp*
*NDD_NAME[0]=tcp_recv_hiwater_def*
*NDD_VALUE[0]=4194304*
*TRANSPORT_NAME[1]=tcp*
*NDD_NAME[1]=tcp_xmit_hiwater_def*
*NDD_VALUE[1]=4194304*

To verify the settings have changed following the ndd -c command:

*bash-4.2# ndd -get /dev/tcp*
*name to get/set ? tcp_recv_hiwater_def*
*value ?*
*length ?*
*4194304*
*name to get/set ? tcp_xmit_hiwater_def*
*value ?*
*length ?*
*4194304*

OPTIONAL: If your client has multiple NICs bonding can be beneficial. See HP-UX System Administration documentation.

In order to support greater than the default maximum of 32K rsize/wsize do the following:

*# kctune nfs3_bsize=1048576*
*# kctune nfs3_max_transfer_size=1048576*
*# kctune nfs3_max_transfer_size_cots=1048576*

Confirm they were added to the Tunable entries section of the file /stand/system:

*# cat /stand/system*

This change will take effect either after a reboot or after the NFS file systems are unmounted and remounted.
Mount with rsize/wsize set to 1M.

*mount –o vers=3,tcp,rsize=1048576,wsize=1048576 …*

Verify the actual rsize and wsize.

*nfsstat –m*

## Microsoft Windows CIFS Client Settings

Microsoft provides comprehensive guidelines for configuration and tuning for networks and storage.

Link to documents for specific Windows versions http://support.microsoft.com/

## Quantum vmPRO

Using Quantum's vmPRO solution, customers can back up virtual machines on an ESX VMware as a share to VTL or NAS targets on the DXi. Here are two examples of VM clients on vmPRO mounted shares:

**Windows** - \\10.1.1.40\export\10.1.1.148\W2003_A_Thin, where 10.1.1.40 is the vmPRO Appliance share AND 10.1.1.148 is the IP address for the ESX server.

**UNIX** - mount 10.40.167.40:/export/10.40.167.148/RHEL_6.1 /hpomniA, where /hpomniA is the local mount point for the virtual machine, RHEL_6.1.

## *Common Operational Considerations*

### Deduplication Data Considerations

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.

### 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.

### Backup Streams Considerations

Data Protector uses Load balancing to distribute the backup job objects over multiple devices. When defining a job, the user specifies the devices that are being for the backup. The backup objects are then divided among the target devices.

The default minimum is 1 and the default maximum is 5.

### DXi Multiprotocol Guidance - NFS/VTL Scenario

The NFS Synchronous setting requires all data written to be committed to physical storage; meaning protocol 'stable writes' and 'commits' require all data to be written to disk for before the command is complete. This ensures that when a backup completes all the data resides on disk. The default setting is Synchronous. This setting can be altered through the CLI.

Asynchronous mode allows the system to acknowledge receipt of 'stable write' or 'commit' command without having the data (and related metadata) fully written to disk. This mode allows backups to be completed faster (from the Data Protector point of view) accepting the possibility of having an incomplete backup if the system fails (e.g., power is lost) before all the data gets flushed to disk.

Simultaneous inline deduplication of VTL ***and*** NFS traffic represents the mixing of a heavy, intensive I/O payload with an out-of-order, burst and response time sensitive protocol.

In a mixed VTL and NFS environment, the DXi 2.1 configuration for NAS shares settings should be changed from the default mode of 'synchronous' to run in '*asynchronous'* mode. This setting can be changed via the Command Line Interface: **syscli --nfscommit async {--share <sharename>} | --all**

Additional notes:

- All other multi-protocol combinations work well together
- Recommendation applies to all operating systems and applications
- Reduced VTL traffic may lessen the frequency of NFS timeouts

### HP Data Protector global Options Considerations

Global options affect the entire Data Protector cell and cover various aspects of Data Protector, such as timeouts and limits. All global options are described in the global options file, which you can edit to customize Data Protector. The global options file is located on the Cell Manager:

- Windows Server 2008: Data_Protector_program_data\Config\Server\Options\global
- Other Windows systems: Data_Protector_home\Config\Server\Options\global
- UNIX systems: /etc/opt/omni/server/options/global

To set global options, edit the global file. Uncomment the line of the desired option by removing the '#' mark, and set the desired value.

**NOTE**: Most users should be able to operate Data Protector without changing the global options.

The following list includes the most often used global variables. See the global options file for a complete description.

- **MaxMAperSM**: Changes the default limit of concurrent devices per backup session. Maximum device concurrency is 32.
- **DCDirAllocation**: Determines the algorithm used for selecting the dcbf directory for a new detail catalog binary file: fill in sequence (default), balance size, or balance number. It is recommended to change the allocation policy from fill in sequence (default) to balance size.
- **DailyMaintenanceTime**: Determines the time after which the daily maintenance tasks can begin. Default: 12:00 (Noon). For a list of daily maintenance tasks, see the online Help index:
- **DailyCheckTime**: Determines the time after which the daily check can begin. Default: 12:30 P.M. You can also disable the daily check. For a list of daily check tasks, see the online Help index:
- **MediaView:** Changes the fields and their order in the Media Management context.
- **MaxBSessions:** Changes the default limit of five concurrent backups.
- **InitOnLoosePolicy:** Enables Data Protector to automatically initialize blank or unknown media if the loose media policy is used.

## Data Protector Device Concurrency, Segment Size, and Block Size Considerations

Any given infrastructure must be used efficiently in order to maximize performance. Data Protector offers some flexibility in order to adapt to the environment as noted in HP OpenView Storage Data Protector Administrator's Guide

**Streaming:** To maximize a device's performance, it has to be kept streaming. A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped; the device waits for more data, reverses the tape a little and resumes writing to the tape, and so on. In other words, if the data rate written to the tape is less than or equal to the data rate which can be delivered to the device by the computer system, the device is streaming. Device streaming is also dependent on other factors such as network load and the block size of the data written to the backup device in one operation. For additional information on device concurrency, segment size and block size, see the Media Management chapter in the HP OpenView Storage Data Protector Concepts Guide.

**Changing Concurrency:** Data Protector provides a default number of Disk Agents that are started for each device. Increasing the number of Disk Agents sending data to a Media Agent at the same time improves device streaming. In the Advanced Options dialog box of a specific device, set the Concurrency to the maximum number of Disk Agents allowed to feed data to each Media Agent. The concurrency set in the backup specification will take precedence over the concurrency set in the device definition.

**Changing Segment Size:** Segment size is related to the size of data areas which Data Protector uses in writing data to the media. It is user-configurable for each device. Note that a smaller segment size consumes media space because each segment has a file mark which takes up space on a medium. A larger number of file marks results in faster restores, because the Media Agent can quickly locate the segment containing the data to be restored. Quantum recommends using a larger segment size to avoid over-running the catalog when lots of small files are being backed up and also to increase the backup speeds. You can change the segment size in the Advanced Options dialog box of a specific device. For detailed steps, refer to the online Help index keyword "segment size".

**Changing the Number of Buffers**: Data Protector Media Agents and Disk Agents use memory buffers during data transfer. Memory is divided into a number of buffer areas. Values from 1 - 32 may be specified.

Each buffer area consists of 8 Disk Agent buffers, which are of the same size as the block size configured for the device. The default device block size is 64 KB. You can change the number of buffers by changing the Advanced Option properties of the selected drive. For detailed steps, refer to the online Help index keyword “number of Disk Agent buffers”. Block Size: When a device receives data, it processes it using a device-type-specific (DDS, DLT) block size. NOTE: Each backup device (drive) has a block size. A restore adjusts to block Size.

**Before Changing Block Size in Data Protector:** Data Protector uses a default device block size for each device type. The block size applies to all devices created by Data Protector and to Media Agents running on the different platforms. The device block size is written on a media header so that Data Protector knows the size to be used. If the device block size differs from the medium’s block size, an error occurs. You can change the device block size in the Data Protector GUI. However, before changing the block size you need to check the supported block size of the host adapter. Quantum recommends a minimum of 256 KB block size, and up to 1 MB.

**Changing the Block Size in Data Protector:** You can set the block size in the Advanced Options dialog box of a specific device. For detailed steps, refer to the online Help index keyword “block size”.

### Disable backup application verify pass

As noted in HP Best practices for VTL, NAS and Replication implementations, most backup applications will default to performing a verify operation after a backup job. Whilst this offers a very good way to ensure that data is backed up successfully it will also heavily impact the performance of the whole backup job. Performing a verify operation will more than double the overall backup time due to the fact that restore performance (required for verify) is slower for inline deduplication-enabled devices. Disabling verify for selected backup jobs can be done relatively safely as D2D Backup Systems perform CRC (Cyclic Redundancy Check) checking for every backed-up chunk to ensure that no errors are introduced by the D2D system. Verifying some backup jobs on a regular basis is recommended. For example, verifying the weekly full backups where additional time is available might be an option.

Troubleshooting

*<Return to Quick Start Activities>*

Debugging can be enabled through the Data Protector GUI under: File -> Preferences. The default range level is 0 to 99. Users are advised to consult with HP for further instructions on debugging.

### Report level option

Options include: **Warning**, **Minor**, **Major**, and **Critical**. Messages are reported at the set level and higher, so a Minor setting reports those events and all above it.

### Reviewing Sessions

1. Select Internal Database from the Data Protector pull down menu.
2. Expand the Sessions folder in the left pane.
3. Select the session you wish to review.

### Generating Reports

1. Select Reports from the Data Protector pull down menu.
2. Right-click on Reports, in the left pane. Select Add Report.
3. Select from available reports, including Reports on a single session.
4. Event logs are also available under this menu.

### Managing Data Protector Services

Run Data Protector file:

/opt/omni/sbin/omnisv –stop (-start, -status)
Or
<Install Path>\OmniBack\bin\omnisv.exe

**Example:**
Verify that the Data Protector services are running.
/opt/omni/sbin/omnisv –status
Output:

```
   ProcName  Status  [PID]
==============================
   rds     : Active  [10751]
   crs     : Active  [10755]
   mmd     : Active  [10753]
   kms     : Active  [10754]
   omnitrig: Active
   uiproxy : Active  [10757]
   Sending of traps disabled.
==============================
```

Status: All Data Protector relevant processes/services up and running

http://www.hp.com/support/

http://bizsupport.austin.hp.com/bizsupport/TechSupport/Home.jsp

## Additional Best Practice Considerations for HP Data Protector

Several operational considerations are common to the two access methods (VTL and NAS). See Common Operational Considerations section at the end of this document for more information on Deduplication, Encryption, Compression, Backup Streams and Replication.

HP Data Protector Internal Database (IDB) Purge best practices Guide contains information on purging obsolete data from the HP Data Protector IDB can be found on the HP support site: http://bizsupport.austin.hp.com/

# Helpful Resources

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

***Quantum Web Site***
http://www.quantum.com

***StorageCare Guardian Web Site***
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***
http://www.quantum.com/ServiceandSupport/Index.aspx

***Call Center Americas:***
To contact Quantum's world-class support representatives, please refer to the information below:

- Telephone (toll free): 800-284-5101
- Telephone (local, not toll-free): 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.
- Users with all other contracts can contact Quantum during normal business days from 5 AM to 5 PM US Pacific Time.

***View Quantum's Service-Level Objective:***
http://www.quantum.com/ServiceandSupport/ServiceLevelAgreement/Index.aspx