Quantum.

DXi-Series Configuration and Best Practices Guide
For NetBackup from Veritas™

Table of Contents

DXi-Series Configuration and Best Practices Guide for NetBackup from Veritas™

This guide seeks to help Quantum customers who own DXi-Series systems (DXi4000-Series, DXi6000-Series, DXi9000-Series and DXi V-Series), and who also use NetBackup from Veritas™ 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 Veritas NetBackup with Quantum DXi-Series systems. This guide includes advice and best practices for using Quantum DXi-Series systems with NetBackup.

How to Use This Guide

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

This document provides key recommendations and useful information for quickly setting up a DXi system with Veritas NetBackup. 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 Veritas NetBackup. Depending on the DXi model, the DXi can appear as a Storage Device using OST, as a Virtual Tape Library (VTL) storage device over Fibre Channel (FC), and as a Network Attached Storage (NAS) device over NFS and/or CIFS. These access methods are discussed in the following order:

- DXi OST (OpenStorage Technology)
- DXi VTL
- DXi NAS – NFS and/or CIFS

Shortcuts to Quick Start Activities

To go directly to any of the following sections, click on that section's name or the page number:

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 products

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

In the lists below, if multiple versions of a manual for your DXi are listed on the linked page, scroll down and select the version for your hardware/software combination. Please note that documents are not listed in alphabetical order, so two versions of the same manual will not necessarily be listed in consecutive lines.

DXi-Series Management Console, OpenStorage (OST) Setup, Virtual Tape Library Setup, Network Attached Storage, DXi Replication

Refer to the following documents for more information as applicable:

- DXi4700 User's Guide
- DXi4701 User's Guide
- DXi4800 User's Guide
- DXi6700 User's Guide
- DXi6900 / DXi6902 User's Guide (same doc covers both models)
- DXi9000 User's Guide
- DXi V-Series User's Guide

DXi Knowledge Base

The knowledge base can help you quickly search for Quantum product articles:

- Quantum Knowledge Base

Online Documentation for Your NetBackup product

- NetBackup Documentation
- NetBackup Master Compatibility Lists
- NetBackup Backup Planning and Performance Tuning Guide (not updated for NBU 7.7 and 8.0)

Best Practices for NetBackup Installation

Best practices include tips and recommendations to help you install or upgrade Veritas NetBackup more effectively. See the appropriate Administrator's Guide for your particular Operating System for additional information.

The following best practices are for preparing to install or upgrade NetBackup:

- Visit the Veritas Support Web site to check for updates to the documentation.
- Review the Readme document and Documentation Addendum for updates to the NetBackup Administrator's Guide.
- Review the "Features or requirements no longer supported by NetBackup" section of the readme.

- Use only standard ANSI characters for the computer name of the computer on which you want to install NetBackup. You may receive errors if you install NetBackup on a computer with a name that uses non-standard characters.

- Ensure that the most recent version of the Microsoft .NET framework is installed on the computer on which you want to install NetBackup on a Windows platform.

- Document your current configuration and settings before you upgrade NetBackup. You can verify your configuration after the upgrade is complete.

- Back up your server before you install or upgrade any software, including NetBackup. Copy NetBackup catalogs and data folders for additional security.

- Pause or stop all jobs before upgrading NetBackup. If you run NetBackup jobs during an upgrade, the jobs will fail.

- Delete any unnecessary job history and alert history before an upgrade, to help expedite the process.

- Disable any monitoring utilities that may restart services.

- Perform database maintenance on your NetBackup Database immediately before an upgrade.

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

- Use an uninterruptable power supply (UPS) for your NetBackup 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, or by push-installing from the local server.

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

- Run Microsoft Windows Update. NetBackup uses many Microsoft technologies that may have been updated since NetBackup's release.

- Monitor your disk space regularly to prevent space problems. NetBackup's space requirements vary depending on usage and installed options. For example, the requirements listed in the Administrator's Guide do not include space estimates for the Simplified Disaster Recovery files, catalogs, or job logs.

- Consult any of the following resources on the Help and Documentation menu if you have questions or difficulties:
  - o Use the NetBackup Documentation Web site for comprehensive information about NetBackup.
  - o Use the NetBackup Help for searchable, topic-based documentation.

Summary of Tuning Parameters for NetBackup

For backup administrators who are well versed on Veritas NetBackup and Quantum DXi systems, the following table offers a summary of suggested parameters/values. As with any modifications to a system that impact performance and/or tuning, your results may vary and are not guaranteed.

Compression	Do not enable NetBackup's Compression feature. To obtain effective Deduplication performance rates, you should **NOT** compress your backup data before sending it to a DXi appliance.

Encryption	Do not enable NetBackup's Encryption feature. For best Deduplication performance, use the hardware encryption provided by the DXi appliance (DXi hardware encryption not available in all regions).
Deduplication	Do not enable NetBackup's Deduplication feature. To obtain effective deduplication rates, you should **NOT** deduplicate your backup data before sending it to a DXi appliance.
Max Connections	300
LSU Images	250,000
VTL sign-on string	Use native DXi Inquiry. Emulated library sign-on strings can mislead support. Emulate as per the NetBackup HCL.
Drive sign-on string	Emulate as per the NetBackup HCL: DXi9000: HP LTO5 DXi6902: HP LTO5 DXi670x: HP LTO4 DXi4800: HP LTO5
SCSI Reserve	Enable with SPC-2 SCSI Reserve. Do not use SCSI Persistent Reserve.
Server Resources	Refer to the NetBackup Backup Planning and Performance Tuning Guide.
Server Name	Use only standard ANSI characters for the computer name of the computer on which you want to install NetBackup. You may receive errors if you install NetBackup on a computer with a name that uses non-standard characters. Windows users must access the NetBackup server by logging in through their Windows domain or the Local account, depending on where it is installed.
TCP/IP Network Buffer Size	NET_BUFFER_SZ = 262144 Refer to NetBackup KB Article TECH1724 for additional information.
Data Buffer Size and Number of Data Buffers	Most cases: SIZE_DATA_BUFFER = 262144 NUMBER_DATA_BUFFER = 16 10GB Single Stream Performance: SIZE_DATA_BUFFER = 1048576 NUMBER_DATA_BUFFER = 16 Refer to NetBackup KB Article TECH1724 for additional information.
Services	Disable the Removable Storage Manager (RSM) service. (No longer present in Windows Server 2003, 2008 and above versions.) Refer to the NetBackup Backup Planning and Performance Tuning Guide.
Network	On heavy utilized systems, consider increasing the TCP/IP timeout on the NetBackup Media Server. See the Additional Considerations for Highly Utilized Systems, Heavy Network Traffic, or Low-Latency Networks section on p.38 for more information. Users may also reference Microsoft performance tuning articles for the Windows Server version being used.

	Apply the following Microsoft hot fixes to improve performance on Windows if applicable
	http://support.microsoft.com/kb/979612
	http://support.microsoft.com/kb/982383

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

- Use the NetBackup Documentation Web site for comprehensive information about NetBackup.
- Use the NetBackup Help for searchable, topic-based documentation.
- Use the **Getting Started** wizards to help you work through the most common configuration steps.

Configuring Veritas NetBackup with the DXi-Series

Configuring NetBackup with DXi OST

OpenStorage API Support

The integration of Veritas's OpenStorage (OST) API initiative with Quantum's DXi4000 series, DXi6000 series, DXi8000 series, and DXi9000 series disk backup, deduplication, and replication solutions provide end users with a highly optimized solution for managing backup data across multiple locations and storage tiers. The DXi's OST support allows users to set up Storage Servers and Logical Storage Units (LSUs) on the DXi units, and to use NetBackup to duplicate data between DXi-based LSUs in different locations. This provides disk-to-disk DR protection, while leveraging the DXi's Deduplication technology to dramatically reduce network bandwidth requirements.

DXi systems can copy data from one system to another (can perform replication). NetBackup uses this capability to initiate an optimized duplication of backup images between these appliances. The duplication operation of NetBackup triggers the duplication function in the OST Disk Appliance, if both the source and destination volumes for the copy are OST LSUs.

OST optimized duplication reduces the workload on the NetBackup Media Server because the replication is performed by the DXi. Duplication is done in the background and is faster because it uses Quantum's data deduplication capabilities to reduce the copy bandwidth. Duplication is still initiated, managed, and controlled by the NetBackup Media Server, while the actual data movement process is off-loaded to gain the maximum benefits from the Quantum appliance's replication capabilities. OST optimized duplication can be used for duplication from or to a DXi, as disk backup targets.

Veritas's NetBackup OST (OpenStorage) allows NetBackup to seamlessly integrate with a DXi-Series disk backup system. Once installed and configured, NetBackup 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 NetBackup with OST

The following steps outline the configuration process at a high level. For detailed instructions, refer to the Veritas NetBackup Guides (To go directly to any of the following steps, click on that step's name).
   - » **Install the DXi OST License Key**
   - » **Configure the DXi for OST (p.7)**
   - » **Install the OST Plugin on the NetBackup Media Server**
   - » **Configure the NetBackup Media Server with OST**
   - » **Back Up to the DXi OST Storage Target Device**
   - » **Configure Optimized Synthetic Full Backups**

OST Network Configuration Considerations

For topics such as high-level network and zone recommendations, DXi network segmentation, and bonding, see the Best Practices Guide with DXi OST section.

Install the DXi OST License Key

Before you can configure the DXi with OST, you must install the OST License key. To determine if the OST License key is already installed, open the DXi GUI and click on "Utilities". Click the "License Key' tab and scroll through the list to see if the OST license is already installed. If the OST license is not already installed, you must obtain a License Certificate containing the authorization code. If OST capability was part of the features ordered for your DXi, you can follow these instructions to install the OST License key:

http://www.quantum.com/licensekeys

- You will be asked for the DXi serial number and authorization code. Once you have OST license key, install it using the DXi Remote Management Console under **Utilities > License Keys**.

- DXi4xxx, and DXi6902 - The OST license key is pre-installed on DXi4xxx and DXi6902 systems. You do not need to install the license key on the system. Use "DXi4000 series", "DXi6900 series" to be consistent with other parts of the doc.

- DXi V1000 - The OST license key is installed as part of the initial setup for the DXi V1000. For information about installing the OST license key on the DXi V1000, see the *Quantum DXi V1000 Quick Start Guide* at DXi V-Series Documents

- After locating the License Certificate, perform the following steps to obtain and install the license:

- Open a Web browser on a computer with Internet access and enter http://www.quantum.com/licensekeys in the browser address box.

- On the **License Key Management** page, enter the DXi system serial number in the **Serial Number** box, and click **Submit**.

- Enter the authorization code (printed on the License Certificate) and click **Get License Key**. The **Licensed Feature** page returns a license key. Print out or write down the license key or save it to a text file.

- Access the DXi remote management console, click on the **Utilities** menu, then click the **License Keys** tab.

- Enter the license key on the **License Keys** page and click **Add.**

Configure the DXi for OST

When configuring a DXi system for OST, keep the following in mind:

- Storage servers and Logical Storage Units (LSUs) must be configured on the DXi remote management console before you configure NetBackup.

- The DXi OST Wizard is another option to configure the DXi for OST. To learn more about using the Configuration Wizards, refer to the User's Guide for your DXi model.

- To authenticate the OST storage servers on a Media Server, you *must* create OST user credentials.

- Do not use an underscore (_) in the name of the storage server.

- Storage server names must be unique and must not be used again on other DXi systems.

- If Concurrent Optimized Duplication is enabled, when data is written to the storage server, it is simultaneously replicated to the target DXi. When optimized duplication or Automatic Image Replication subsequently occurs, the operation is more efficient, because a portion of the required data has already been replicated to the target storage server. To use Concurrent Optimized Duplication, configure the source DXi and target DXi for replication.

- You must add target IP mapping information if you are performing optimized duplication on a segmented network and replication is not configured between the source DXi and target DXi.

- The OST user credentials to use for authentication on the remote (target) DXi must match a local user on the target DXi.

- If Automatic Image Replication (AIR) is enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as of the backup images that are duplicated, is determined by the storage lifecycle policies (SLPs) configured in NetBackup.

- To use Automatic Image Replication, configure the source DXi and target DXi for replication and configure at least one remote user before enabling Automatic Image Replication. Also, you must associate a source data IP address with a replication IP address on a target DXi. This might be necessary if the target DXi is configured with different network interfaces (and therefore different IP addresses) for data and replication traffic.

- When configuring AIR, use storage server names that are unique among the DXi systems involved in an AIR configuration.

- OST AIR requires NetBackup 7.1 or higher.

Note: In DXi 2.x and later software, you should no longer include a domain name as part of the username. If you have upgraded from DXi 1.4.x software, create a simple username and password using the rules noted above, then provide the same credentials on the Media Server.

If you have upgraded from a version released prior to 2.0, you **MUST** add new OST credentials to the DXi to continue using OST. To do so:

1. Shut down the NetBackup services.
2. Create new OST user credentials, making sure to use the same username and password that were used to register the existing OST devices.
3. Restart the NetBackup services.

Note: Quantum recommends that you create a different storage server for each NetBackup domain (master server plus associated Media Servers). This segregates data, so that a NetBackup administrator cannot accidentally modify or remove backup images belonging to another domain.

As you carry out configurations, keep the following recommended parameter values in mind:

Parameter	Values	Recommended
Max Connections	3 – 65536	300
LSU Images		250,000
LSU Physical Capacity	Available / Specific	Available

Perform the following steps to configure the DXi for OST:

1. Log on to the DXi remote management console.
2. Navigate to the **Configuration > System> Manage Users** page.
3. Add the Username and Password.
4. Navigate to the **Configuration > OST > Storage Servers** page and add a Storage Server.
5. On the same the **Configuration > OST > Storage Servers** page, add a Logical Storage Unit (LSU).

Install the OST Plugin on the NetBackup Media Server

Before you can configure NetBackup with DXi OST, you must download and install the OST Plugin and install it on the Media Server configured with NetBackup. A link to the plugin download is provided in the

DXi's GUI under **Configuration >System>Client Plug-Ins**. Compatibility and Installation information are available at:

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

Make sure to download the correct OST Plugin for the Operating System installed on the NetBackup Media Server.

This procedure is the same for each NetBackup Media Server operating system platform. Follow the Installation instructions to install and configure the OST Plugin on the NetBackup Media Server(s).

Some items to consider:

- By default, the OST Plugin for Windows is installed in the **%VERITASHOME%\NetBackup\bin\ost-plugins** folder.
- Quantum default certificate files placed in the **%WINDIR\Quantum** folder.
  These files are needed if the TLS with AES256 encryption option for Accent is enabled on the DXi.
- On Windows platforms, if you expect to run a larger number of concurrent backups, consider modifying TCP settings as described in the OST Installation instructions.
- By default, OST Plugins for Linux/UNIX are installed in the **/usr/openv/lib/ost-plugins/** directory unless directed elsewhere by the user. See the OST Plugin Installation Instructions for specific information.
  - Move the configuration file, using **/bin/mkdir -p /usr/Quantum; /bin/mv QuantumPlugin.conf /usr/Quantum**.
- For the 64-bit Solaris SPARC plug-in, the 64-bit gcc3 run-time libraries must be installed before installing the OST plug-in.
- On Solaris platforms, if you expect to run a larger number of concurrent backups, consider modifying TCP settings as described in OST Installation instructions.
- When multiple Media Servers are using a single DXi system, you can distribute the load by dividing the hosts into groups.

Configure the NetBackup Media Server with OST

Please consult the Veritas NetBackup Installation Guide and Veritas NetBackup Administrator's Guide for information about NetBackup installation and basic configuration.
Note: Use the applicable guides for your NetBackup version.

OpenStorage (OST) devices are created using the **Configure Disk Storage Servers wizard** on the **Details** panel on the NetBackup Administration Console.

The Accelerator feature is now available on the NetBackup media server in the following configurations:

- NetBackup 7.5 and 7.6 (VMware Accelerator is only supported for NetBackup 7.6).
- OST Plug-in 3.0.0 or higher.
- DXi system running DXi 3.1 Software or higher.
- Mappings file version 1.122 from NetBackup, or higher
- **Use Accelerator** Policy attribute checked.

High and Low Water Mark Considerations

While configuring the storage server in NBU, users can change the default high and low water mark settings to avoid spanning operations with the LSUs. Backup and restore operations that span LSUs can cause failures and are not recommended. Depending on the size of the backup images and the LSUs (if fixed size), users may wish to set the high watermark threshold below the default, 98 percent. A volume is considered full when the high watermark is reached. NetBackup will begin image cleanup when the high watermark is reached and will delete any expired media on the volume.

The low water mark default is set at 80%. This is the point where NBU will stop image cleanup processing. NetBackup users can manage these thresholds to suit their environment.

Note: Quantum recommends setting maximum concurrent jobs to no more than 16 jobs on DXi6510 systems, or 64 jobs on all other DXi6000-Series models. Keep in mind that restore jobs and optimized duplication jobs will cause additional system load. When configuring disk pool settings for the storage server, users can choose to limit I/O streams.

Command Line Configuration for OST

Creating and Authenticating Quantum Storage Servers

Note: These steps assume that the storage server and LSU have already been created on the DXi.

Creating Storage Servers with **nbdevconfig**:

- ▪ Windows: Run **<Install Dir>\veritas\netbackup\bin\admincmd\nbdevconfig.exe**
- ▪ UNIX: Run **/usr/openv/netbackup/bin/admincmd/nbdevconfig**

   Important: When you create an OST device in NetBackup, the format of the "**Server name:**" required in the dialog **must** be in the form: **<OST Server_DXi FQDN>**. An IP address can be used in place of the DXi's Fully Qualified Domain Name.

   For example, in the step above, if a Storage Server called **OSTserver1** was created on a DXi named **QuantumDXi1.mycompany.com**, the server name *must* be specified as **OSTserver1_QuantumDXi1.mycompany.com**.

   The "**Logon account:**" username and password *must* be the same as the OST user credentials created on the DXi management console.

nbdevconfig Information

USAGE: (Create storage server):

```
nbdevconfig -creatests [-noverbose]
-storage_server < OST Server_DXi FQDN >
-stype Quantum
-media_server <media_server FQDN>
-st 9
```

Command line usage for **nbdevconfig** is available by issuing the command **nbdevconfig –help**.

Important: **nbdevconfig** may return success in cases where the Storage Server was not created. Use "**nbdevquery -liststs**" to verify that the Storage Server was correctly created.

Authenticating Storage Servers with tpconfig:

- Windows: **<Install Dir>\veritas\volmgr\bin\tpconfig.exe**
- UNIX: **/usr/openv/volmgr/bin/tpconfig**

USAGE:

```
tpconfig -add
-storage_server < OST Server_DXi FQDN >
-stype <Quantum>
-sts_user_id <user ID>
-password <password>
```

Command line usage for **tpconfig** available with **tpconfig –help**.

Creating disk pools

USAGE (Create disk pool):

```
nbdevconfig -createdp
-dp <disk_pool_name>
-stype Quantum
-storage_server < OST Server_DXi FQDN >
```

Refer to the *Veritas NetBackup Administrator's Guide* for more information and instructions on configuring storage.

Back Up to the DXi OST Storage Target Device

After you have configured your OST device(s), test the configuration by performing a backup job and monitoring the results.

See the *NetBackup System Administrator's Guide* for information on creating a backup policy to back up data to an OST disk pool.

Configure Optimized Synthetic Full Backups

One of the capabilities a vendor may expose is the disk appliance's potential to construct synthetic backup images. A media server uses messages to instruct the storage server which full and incremental backup images to use to create the synthetic backup. The storage server constructs (or synthesizes) the backup image directly on the disk storage. The backups that NetBackup creates in this way are known as optimized synthetic backups.

The OpenStorage optimized synthetic backup method provides the following benefits:
- Faster than a synthetic backup.

Regular synthetic backups are constructed on the media server. They are moved across the network from the storage server to the media server and synthesized into one image. The synthetic image is then moved back to the storage server.
- Requires no data movement across the network.
- Regular synthetic backups use network traffic.
- Uses fewer disk resources, depending on the vendor implementation.

The storage vendor determines the storage implementation. If the disk appliance uses data deduplication, duplicate data is not created and stored.

In NetBackup, the OptimizedImage attribute enables optimized synthetic backup. It applies to both storage servers and disk pools.

To ensure that the storage server and disk pools are correctly configured for both optimized synthetic full backups and the NetBackup Accelerator feature, run the following commands on the Media Server:

```
nbdevconfig –changests

-stype Quantum

-storage_server <ss_name>

-setattribute OptimizedImage

nbdevconfig -changedp

-stype Quantum

-dp <dp_name>

-setattribute OptimizedImage
```

To verify the configuration, run the following commands, and ensure that they return the flag **OptimizedImage**:

```
nbdevquery   -liststs  –U
nbdevquery   -listdp   –U
```

Configure NetBackup Optimized Duplication

Data can be copied from one DXi system to another DXi system (to perform replication). NetBackup uses this capability to initiate an optimized duplication of backup images between these appliances. The duplication operation of NetBackup triggers the duplication function in the OST disk appliance if both the source and destination volumes for the copy are OST LSUs.

OST optimized duplication reduces the workload on the NetBackup Media Server, because the duplication is performed by the DXi.

- Duplication is done in the background and is faster because it uses Quantum's data deduplication capabilities to reduce the copy bandwidth.
- Duplication is still initiated, managed, and controlled by the NetBackup Media Server, while the actual data movement process is off-loaded to gain the maximum benefits from the Quantum appliance's replication capabilities.
- OST optimized duplication can be used for duplication to or from a DXi as a disk backup target.

The DXi can replicate (duplicate) OST data to another DXi using the following methods:

- **Optimized Duplication** - With optimized duplication, backup images on a storage server can be replicated to another storage server on a DXi that resides in the same NetBackup domain. The duplication occurs when Optimized Duplication is initiated by NetBackup.
- **Concurrent Optimized Duplication** - For both optimized duplication and Automatic Image Replication, you can optionally enable Concurrent Optimized Duplication. If enabled, as data is written to the storage server, it is simultaneously replicated to the target DXi. When each

subsequent optimized duplication or Automatic Image Replication occurs, the operation is more efficient, because a portion of the required data has already been replicated to the target storage server.

- **Automatic Image Replication (AIR)** - If you are using Veritas NetBackup 7.1 or higher, you can configure an LSU for Automatic Image Replication*. If enabled, data on an LSU is automatically replicated to a remote LSU that resides on a DXi in a different NetBackup domain. The timing of the duplication, as well as of the backup images that are duplicated, is determined by the storage lifecycle policies (SLPs) configured in NetBackup. When a replication event occurs, the DXi notifies NetBackup through the OpenStorage API.

*NetBackup AIR requires OST Plugin 2.6 or higher, and DXi code level 2.2.1 or higher.

It is important to remember that with Automatic Image Replication, the local and remote LSUs reside in different NetBackup domains. This differs from optimized duplication, which occurs between two LSUs residing within the same NetBackup domain.

Note: For information about configuring NetBackup for optimized duplication or Automatic Image Replication (also referred to as *duplicating images to a remote master server domain*), see the Veritas NetBackup Administrator's Guide.

DXi systems use the replication channel to perform optimized duplication. This significantly increases performance. In addition, more than two optimized duplication streams per source DXi are supported.

Note: When using **Replication Channel** for OST, up to two replication targets can be configured on the DXi.

Caution: Using **Replication Channel** for OST requires that the network interfaces used for replication on the source and target DXi be on the same subnet.

Configuring the DXi for AIR Support

To create the storage units in the different domains, add a remote user, and create OST user credentials for use with OST AIR. The remote user credentials on the source DXi must match the local user credentials on the target (remote) DXi.

To add a remote user, under OST configuration on the source DXi:

1. Click **Add** on **Configuration > OST > Manage Remote Users**.

   The **Add Remote AIR Credential** window displays.

2. Enter information about the remote user:

   User name   Enter the name of the remote user.
   New Password Enter the password for the remote user. Confirm the new password.
   Description   (Optional) Enter a brief description of the remote user.

3. Click **Apply**.

4. Create or edit the LSU to be replicated.

   Remote Storage Server Name - The name of the remote storage server (on the target DXi) to replicate data to. The source DXi and target DXi must reside in different NetBackup domains.

5. Configure the target DXi.

   Remote LSU Name - The name of the LSU in the remote storage server that will receive the replicated data.

   Remote User - The OST user credentials to use for authentication on the remote (target) DXi.

   Note: The selected remote user **must** match an authenticated user on the **Configuration > System > Manage Users** page on the target DXi.

Note: Encryption is enabled by default. However, for best performance, if your data network is already secured, you should clear the **Use Encryption** check box. Using 256-bit encryption (default) provides a stronger level of security but may have an impact on system performance in some situations.

Configuring AIR in NBU

In the first (originating) NetBackup domain:

Configure one SLP that contains at least one Backup operation and one Replication operation that is configured to replicate to a target NetBackup domain (Auto Image Replication SLP).

In the second (target) NetBackup domain:

Configure one SLP that contains an Import operation to import the replication (Import SLP). The Import SLP can be configured to create additional copies in that domain, or to cascade the copies to another domain.

Note: Both SLPs must have identical names.

Using DXi Accent for OST

Designed for bandwidth-constrained environments, DXi Accent for OST dramatically increases backup performance by using a hybrid-mode workflow to move part of the deduplication process to the backup server, so that only new blocks in each backup are sent to the appliance.

The minimum system requirements for using DXi Accent are a CPU greater than 2.2 GHz processor with at least 2 cores (4 cores recommended), and 2 GB RAM or greater.

For complete details on configuration of NetBackup with DXi Accent, refer to the *OST Configuration Guide Instructions, available from the* Service and Support > Client Plugins *page.*

Configuring Encryption with NBU

Do not enable Encryption within the NetBackup job policy when backing up data to a DXi target, as it will have a negative effect on Deduplication. With DXi Accent, the user can configure Inline Deduplication and use 128- or 256-bit Encryption when sending OST data from the Media Server to the DXi. OST duplications between the source and target LSU's will be encrypted through this process.

Usage:

- **DXi Configuration Menu > OST > Accent >Enable Inline Dedupe with Accent**
- Option: Use Encryption, 128-bit or 256-bit

With *DXi 3.1 FW or higher*, the encryption settings are now located as follows:

- **DXi Configuration Menu -> System > Security > Data Encryption**

- Option: Use Encryption, AES 128-bit, AES 256-bit, or TLS AES256-bit

Configuring OST PATH TO TAPE

NetBackup users can configure storage lifecycle policies to run backups that automatically duplicate data to a secondary target. With the DXi configured as an NDMP host in NBU, physical tape libraries and drives that are attached to it are available for discovery and configuration, and to be targets for direct copy to tape. Users can also run duplications manually through NBU's catalog function. With direct copy to tape, the duplication job is handled by the DXi, leaving the Media Server free to manage other tasks.

Note!
1. Install the Backup Application Specific Path to Tape and OST licenses on the DXi. See your *DXi User's Guide*.
2. OST plugin should be installed on NBU server.

Steps to configure OST Direct to tape:

On the DXi system side:

Configure OST:
1. From the DXi remote management console, select **Configuration > OST** and click **Add.** Specify Storage Server Name, LSU Name and Capacity in the correspondent fields**.**
2. Select **Configuration > System > Manage Users**, click **Add** button to display the **Add User Credential** dialog box. In the **User Name**, **New Password**, and **Confirm New Password** fields, enter the OST user.

Configure NDMP credentials and PTT:

3. From the DXi remote management console, select **Configuration > PTT and click Scan** button to discover all attached PTLs. After the DXi completes its scan, make sure that the changer and all of its drives are enabled. If you need to enable a changer or drive, select the component and click **Enable**.
4. Select **Configuration > System > Manage Users**, click **Add** button to display the **Add User Credential** dialog box. In the **User Name**, **New Password**, and **Confirm New Password** fields, enter the NDMP user.

In Netbackup Administration Console:

 Configure OST:

5. On the main page click **Configure Disk Storage Servers** to display **Storage Configuration Wizard**, select **OpenStorage** and click **Next.**
6. Specify Media Server, Storage server type as Quantum, Storage server name as "ostName_dxiIP address", user name and password that created in Step1 and click **Next**.
7. Select volumes to add to the disk pool, specify disk pool name. Then agree to create storage unit specifying its name and finish the configuration.

Setup a backup policy and start a backup:

8. On the left menu bar go to **Netbackup Management > Policies** and after right click select **New Policy.** Use configuration wizard to setup policy step by step. After the policy is created, double click on it and specify OST storage unit created in Step7 in **Policy storage,** click **OK.**

9. Right click on the policy and select **Manual Backup** to start a backup. Wait until it completed.

Configure NDMP and PTL

10. On the left menu bar go to **Media and Device Management > Credentials > NDMP Hosts**, click **New NDMP Host** button and specify DXi hostname.

11. Select "Use the following credentials for this NDMP host" option and specify NDMP user credentials created in Step4.

12. On the main page click "**Configure Storage Devices**" to display "**Device Configuration Wizard**". Under DXi hostname click **Change** button, select **NDMP host** radio button and click **Next**. Then NBU will scan for devices and all tape devices will be displayed on the page. Finish the configuration.

13. On the left menu bar go to **Media and Device Management > Devices > Robots,** right-click on necessary robot and select **Inventory Robot .** Make sure that **Update volume configuration** is selected and click **Start** button**.** The job will find the media for the duplication job.

Perform a direct copy to tape

14. On the left menu bar go to **Netbackup Management > Catalog,** under **Action** select Duplicate, specify Date range and click **Search Now** button for list all backup jobs**.**

15. Right-click on the desired backup in the search results window and select **Duplicate**.

16. Under **Storage Unit** select the physical library, under **Volume Pool** select NetBackup, press **OK**. To check the job status open **Activity Monitor**.

Configure NetBackup Optimized Duplication

Steps to setup Optimized Duplication:

Configure a Replication between source and target DXi-es.

1. From the Target DXi remote management console, select **Configuration > Replication** and under **Source DXis** tab add ip-address of the source DXi.

2. From the Source DXi remote management console, select **Configuration > Replication** and under **Target DXis** and add the target DXi specifying **Target Hostname or IP, Encryption** and **Source IP**.

Configure Optimized Duplication on the both DXi-es

3. On the Target DXi, select **Configuration > OST** and click **Add.** Specify Storage Server Name, LSU Name and Capacity in the correspondent fields**.**

4. Select **Configuration > System > Manage Users**, click **Add** button to display the **Add User Credential** dialog box. In the **User Name**, **New Password**, and **Confirm New Password** fields, enter the OST target user.

5. On the Source DXi, select **Configuration > OST** and click **Add.** Specify Storage Server Name, LSU Name and Capacity in the correspondent fields. Also check **Enable Concurrent Optimized Duplication** option and select target IP address.
6. Repeat Step4 for OST source user.

Configure OST in NetBackup Administration console

7. On the main page click **Configure Disk Storage Servers** to display **Storage Configuration Wizard**, select **OpenStorage** and click **Next.**
8. Specify Media Server, Storage server type as Quantum, Storage server name as "ostName_dxiIP address", user name and password that created in Step4 and click **Next**.
9. Select volumes to add to the disk pool, specify disk pool name. Then agree to create storage unit specifying its name and finish the configuration.
10. Repeat Steps7-9 for source OST.

Setup a backup policy and start a backup:

11. On the left menu bar go to **Netbackup Management > Policies** and after right click select **New Policy.** Use configuration wizard to setup policy step by step. After the policy is created, double click on it and specify source OST storage unit in **Policy storage,** click **OK.**
12. Right click on the policy and select **Manual Backup** to start a backup. Wait until it completed.

Perform Optimized Duplication

13. On the left menu bar go to **Netbackup Management > Catalog,** under **Action** select Duplicate, specify Date range and click **Search Now** button for list all backup jobs**.**
14. Right-click on the desired backup in the search results window and select **Duplicate**.
15. Under **Storage Unit** select the target OST and press **OK**. To check the duplication job status open **Activity Monitor**.

OST Plugin Configurable Options for Troubleshooting

- Red Hat Linux x86 64-bit, SuSE Linux x86 64-bit, Solaris SPARC 64-bit/Solaris x86 64-bit:

  The Quantum OST Plugin maintains logs for troubleshooting purposes in:

  /var/log/ostlog/client

- Windows 2003/2008 32-bit/Windows 2003/2008/2012 64-bit:

  OST logs reside in the Windows folder **%WINDIR%libstspiQuantum*.log**

The logging level, opdup timeout, and LOG LIMIT values can be configured in the **libstspiQuantum.ini** file for Windows, or in **/usr/Quantum/QuantumPlugin.conf** for UNIX platforms.

Default Values:

```
LOG_LEVEL=ERROR  #Change this value to DEBUG when troubleshooting.
LOG_LIMIT=104857600  #Value is shown in bytes - 104MBs by default.
LOG_TIMEOUT=60000
LOG_FILE_LIMIT=10
```

Logging Levels:

```
NONE    Disables logging for the logger.
TRACE   Enables tracing to error messages.
DEBUG   Enables debug to error messages.
INFO    Enables information to error messages.
WARN    Enables warning and error messages.
ERROR   Enables only error messages (Default).
```

To change the logging level:

1. Apply logging level changes to the log file, log app, and log dbg sections of the OST Plugin Configuration file.

See the Quantum DXi User's Guide for your DXi system, or backup application user's guide, for more information on OST Plugin logging.

Best Practices Guide with DXi OST

OST with NetBackup Granular Recovery

Quantum DXi Appliances running OST are certified for Granular Recovery Technology support with. NetBackup 7.5 and above. This technology allows for individual data storage recovery, including for Microsoft Exchange data.

Useful references:
About Exchange backups and Granular Recovery Technology (GRT)
Active Directory granular backups and recovery
Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)

Deduplication Considerations

Quantum's deduplication technology divides a data stream into variable-length data segments using a data-dependent methodology that can find the same block boundaries in different locations and contexts. This block-creation process allows the boundaries to "float" within the data stream, so that changes in one part of the data set have little or no impact on the boundaries in other locations of the data set.

Through this method, duplicate data segments can be found at different locations inside a file, inside different files, inside files created by different applications, and inside files created at different times. When NetBackup encounters a segment of data that is already stored in the deduplication storage folder, the data is not stored again. So if you back up the same unchanged file repeatedly, it is stored only one time in the deduplication storage folder.

Deduplication works best in the following scenarios:
- For Windows and Linux file system data

- ▪ Where the same file is backed up multiple times
- ▪ Where the percentage of data that changes is small

About Sharing a Deduplication Device between Multiple NetBackup Servers:

If you use the NetBackup SSO Option, you can select which NetBackup servers can share a deduplication disk storage device or OpenStorage device. When you add a deduplication disk storage device or an OpenStorage device, the NetBackup server that you used to add the device is automatically selected for sharing.

Note: To share a deduplication disk storage device, you must add it as an OpenStorage device on all NetBackup servers that you want to have access the device, except for the NetBackup server that was used to create it.

Backup Streams Considerations

You should create and use a different storage server for each NetBackup domain (master server plus associated Media Servers). This segregates data, so that a NetBackup administrator cannot accidentally modify or remove backup images belonging to another domain.

Multistreaming Considerations

OST works with an NBU capability called *multistreaming*. This causes NBU to generate several backup streams in parallel to back up different subdirectories at the same time. This can cause a single backup stream from a single server to become 10 or more streams. But this also means that sometimes a stream contains nothing but a single file, which can produce very short backup files. Quantum recommends exercising caution when using this option.

Quantum recommends that you **DO NOT** set multistreaming to a value greater than the number of spindles on the client. For further information on this topic, refer to this Veritas Tech Note:

https://www.veritas.com/support/en_US/article.TECH10085

Each backup job will create between 2 and 4 connections to the OST storage (DXi). When OST is NOT in use, using multistreaming can push the performance level as high as the client allows.

The following tables indicate the recommended maximum values for setting the TOTAL number of streams per DXi model. While the various DXi models have been designed and tested for values much higher than what are listed here, lab testing suggests that these values will provide maximum performance in a generalized environment. Keep in mind that each data protection ecosystem is unique, and that its configuration will determine the final settings.

DXi 3.4.x/4.x Maximum Individual Stream Count Guidance						
Model	NFS/CIFS-SMB	OST/	OST (DXi Accent)	VTL	OST Accelerator	Multi-Protocol*
DXi4700/1	50	50	50	32	7	50
DXi4700/2	50	50	50	32	7	50
DXi4800	50	50	50	32	7	50
DXi4800 (with memory up-grade kit and ISC enabled)*	200	200	300	150	28	200
DXi690x 128GB	128	128	128	160	25	128
DXi690x 256GB	256	256	256	256	55	256
DXi6900-S 256GB	512	256	768	512	110	512
DXi9000 192GB	256	256	384	256	55	256
DXi9000 384GB	512	512	768	512	110	512
DXi9000 768 GB (VDMS)	512	512	768	512	110	512
DXi9000 768 GB (ISC enabled)	1000	1000	2000	1000	280	1000

*Multi-Protocol Weighting: Each protocol contributes a different work load on the stream count. When determining the total number of streams, use the following weight factor: VTL 1.25, SMB 1, NFS/Veeam 5, OST/RMAN DXi Accent 1, OST Accelerator 7, OST/RMAN 1.

DXi 2.x Maximum Individual Stream Count Guidance						
Model	NFS	CIFS	OST	VTL	DXi Accent	Total
DXi6700	100	100	100	80	100	256
DXi6701/2	100	100	100	80	100	256

Optimized Duplication Considerations

When performing optimized duplication, DXi systems can use either the replication channel or the OST channel. Using the replication channel significantly enhances Optimized Duplication performance.

Accelerator Considerations

Use the following best practices to determine if using the Accelerator feature is right for your client backups.

- The first backup of any client will be a traditional full backup. See the *NetBackup System Administrator's Guide* for information on creating a full backup.
- Backups after the first initial full backup will use the Accelerator feature. The client data change rate (referred to as "change rate" below) is defined as the percentage of ingest data bytes that have been merged with synthetic data bytes on the DXi.
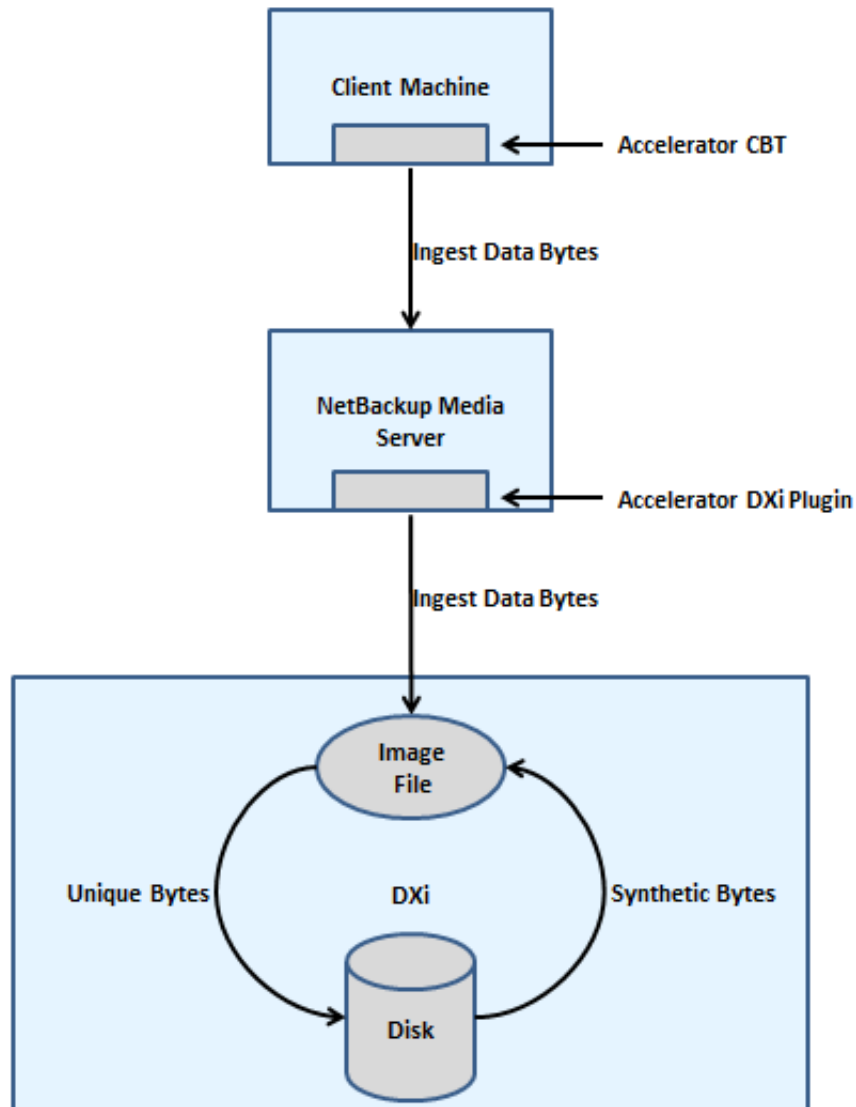
- The change rate between backups should be 5% or less, though you may see performance savings above traditional full backups with higher change rates. For more information on recommended change rates, see the *NetBackup System Administrator's Guide*.

- You can view change rates in the **OST Accelerator – Savings** report in DXi Advanced Reporting. For more information, see the **3. Install** section in the Print Documentation section of the DXi6900 Documentation Center.

- For backups with consistently high change rates, Optimized Synthetic Backups can be used instead of the Accelerator feature. See Configure Optimized Synthetic Full Backups.

- When using Accelerator to create incremental backups, configure the NetBackup media server to create differential incremental backups. See the NetBackup System Administrator's Guide for more information.

- Accelerator use on a DXi system should be configured for fewer concurrent accelerated backup streams from media servers. Use the OST Accelerator column in the table above to determine the best fit for your usage.

- High density clients containing many files of smaller size will see slower backup performance than less dense clients.

- If the following errors occur during a backup when using NetBackup 7.6, it is recommended that you upgrade to NetBackup 7.6.0.4:

  Error bpbrm(pid=xxxxx) could not send server status message

  Info bpbkar32(pid=yyyyy) done. status: 13: file read failed

Additional Best Practice Considerations

Several operational considerations are common to all three access methods (OST, VTL and NAS). See the Common Operational Considerations for NetBackup section for more information on Deduplication, Encryption, Compression, Backup Streams, and Replication.

Configuring NetBackup 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 can appear differently, depending on the interface through which it is viewed. If the DXi is viewed though Fibre Channel interfaces, it appears as a virtual library with virtual drives and cartridges. When viewed through a TCP/IP interface, it appears as an NDMP (Network Data Management Protocol) host. During backups, the application creates a backup image on the virtual tape cartridges. The application can then use the NDMP host interface to duplicate the image on virtual tape cartridges to physical tape cartridges.

VTL Device Installation and Configuration 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 addresses* that define 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 NetBackup device discovery to align these two addresses, reducing the potential for improper configuration.

Caution: If the Device Configuration Manager does not serialize the devices listed, **DO NOT** commit any 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 DXi400-Series, DXi6700, DXi6900, or DXi9000-Series inquiry response string as the identification for each model, respectively). This allows product identification for the service teams at both Veritas and Quantum. 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 NetBackup, the inquiry string that the device provides must match exactly with what is documented on the HCL (see the "Hardware Compatibility List (HCL)", which is linked to on the Veritas Web page NetBackup Master Compatibility List).

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 NetBackup. 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.

Use the Veritas tape drive drivers for backup hosts running the Windows 32-bit operating systems. For backup hosts running the 64-bit versions of the Windows operating system, the OEM tape device drivers are recommended. A wizard for installing NetBackup tape drivers on Windows 32-bit systems can be obtained by following the directions at https://www.veritas.com/content/support/en_US/downloads.

Quantum recommends against using the Windows update function to get the latest tape drive drivers, since it is possible that Windows Update can find unexpected driver matches for a tape drive. These unexpected matches often are not the same as those supplied by the tape drive manufacturer and may introduce unexpected incompatibilities. This can result in an undesirable change to the device in the Windows Device Manager.

Note: Quantum highly recommends installing NetBackup's latest Device Mappings Package for your appropriate Operating System(s) to support properly identifying devices in NetBackup.

Configuring the DXi and NetBackup for VTL operations

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

Installing and configuring the DXi and NetBackup for VTL operation consists of the following major steps:

- » **Configure the DXi for VTL**
- » **Configure the NetBackup Library and Tape Drives**
- » **Test Backup to the DXi VTL Storage Target Device**
- » **Configure NetBackup for DXi VTL Path to Tape**

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 NetBackup. 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 DXi GUI 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.

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 NetBackup system is properly configured for the correct number of tape drives emulated in the DXi system partition. Failure to do so may cause NetBackup to malfunction or cease to operate.

The "drives" presented by a DXi aren't assigned their own WWPNs, but rather appear as LUNs on the DXi Fibre Channel port. While many operating systems recognize this, Solaris is not one of those. Solaris uses a combination of **st** and **sg** files to control how many LUNs a single WWPN can present to the OS. This requires special handling, since the default number of LUNs is 16. So, if a user configures a 20-drive VTL on Solaris, it will see the changer and 15 drives. The **sg.conf** file must be rebuilt in order to allow the OS to "see" those additional LUNs. This Veritas Tech Note contains additional information on this subject: https://www.veritas.com/support/en_US/article.TECH31047.

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 total of capacity for all media could be more than the physical capacity of the system. For more information on this, see the Oversubscription of Space on the DXi section.

The DXi-Series VTL is qualified by Veritas and is included in the latest mapping files. Make sure you have the latest mapping files for your NetBackup application before starting the Device Wizard.

DXi Tape Drive Emulations and Recommend Drivers

SDLT 600 & DLT-S4: Use the Veritas driver or OEM driver.

HP LTO drives: Use the Veritas driver or OEM driver.

IBM LTO drives: IBM Driver 6.1.5.4 with DPO function for 64-bit systems.

Note: Quantum does not support mixing drive types in a single partition.

Configure the NetBackup Library and Tape Drives

After a VTL has been defined in the Quantum DXi-Series system and the host HBA has been configured, you can begin integration with the NetBackup application.

To configure the newly created library and tape drives within NetBackup, follow these steps:

1. Open the NetBackup Administration Console and run the **Configure Device Wizard**.

2. If you have SSO installed, select all servers with access to the VTL.

   Note: As of NetBackup 7.5, the AIX 6.1 and 7.1 operating systems are no longer supported as a robotic library controller. Veritas recommends using an operating system other than AIX as a robotic library controller.

   See Quantum TSB 00002693 for more information.

3. Inventory and label your virtual tapes.

Ensure that you have created the appropriate Backup Policy, so that you can start backing up your data. Further instructions can be obtained from the *Veritas NetBackup for Windows Servers Administrators Guide* or the *Veritas NetBackup for UNIX Servers Administrators Guide.*

If you will be using NetBackup for DXi VTL NDMP Path to Tape, you must install the **NetBackup NDMP** option locally on the Media Server as a separate add-on component of NetBackup. Refer to "Installing Additional NetBackup Options" in the *NetBackup Installation Guide*.

Test Backup to the DXi VTL Storage Target Device

After you have completed the configuration, test the configuration by performing a backup job and monitoring its results.

Configure NetBackup for DXi VTL Path to Tape

After the normal backup process has completed, NetBackup can perform a copy operation using NDMP to transfer data directly from the virtual tape library (VTL) to the physical tape library. The data movement is over a Fibre Channel connection. The backup Media Server controls this copy process, but it does not read or write the data, which frees it to do other tasks. Because this is a normal duplication job, NetBackup catalogs the physical tape copy in its database.

Both the VTL and the physical tape library are visible to NetBackup; therefore, restores can be performed directly from either copy (virtual or physical). To duplicate the virtual tape image, NetBackup selects an NDMP device path to the VTL and creates an NDMP control session for this device. It selects a tape volume from the physical tape library and selects an NDMP device path from this library. It then creates a second NDMP control session for this device. NDMP messages are then sent via the control sessions to move data and to monitor the data transfer. NetBackup writes headers as needed, and handles tape spanning, tape errors, and similar items.

On DXi systems, a separate license is required to support Backup Application Specific Path to Tape (also known as NDMP Path to Tape). The Backup Application Specific license is pre-installed on all DXi4800, DXi6700, DXi6902, and DXi9000-Series systems. The NDMP option is installed as a separate component in NetBackup to support this feature. You must dedicate a partition within the DXi for use with NetBackup. The partition cannot be shared with another backup application.

Note: NDMP user names are case sensitive.

The following device paths must be visible to NetBackup:

- Fibre Channel device paths (emulating tape) to the VTL storage for backup data from the primary storage device.
- NDMP device paths (emulating tape) to the VTL storage. This Ethernet device path access is required both for reading from a VTL to duplicate to a physical tape library, and for reading from a physical library to duplicate to a VTL.
- The DXi virtual medium changer must be viewed through TCP/IP. It will appear as an NDMP host.
- NDMP device paths to the attached physical tape devices, to read or restore data directly from a physical tape.

NetBackup controls the virtual tape library backups and NDMP duplication from virtual tape library to the physical tape library.

Before you back up NDMP resources, review the following information:

- The NDMP option does not exclude folders from the backup job if the parent folder is backed up. Instead, all items in the parent folder are backed up, even if you marked items for exclusion from the backup.

- NetBackup cannot gather sufficient file and directory information on an NDMP backup to accurately populate the **Job Summary** and **Set Detail** Information sections of the job history. Therefore, the numbers of files, directories, files skipped, corrupt files, and files in use always display as **0**.

- If your environment includes NAS devices from more than one provider, you must create separate backup jobs for each provider. If you include NAS devices from multiple providers in the same backup job, the job will fail.

- A physical tape library that is connected to the same network as the DXi can be recognized and configured for the Path to Tape (PTT) feature.

Note: See the "Hardware Compatibility List (HCL)" links in the NetBackup Master Compatibility List Web page for a complete list of supported libraries.

If you use the NetBackup SAN Shared Storage Option (SSO), you can select which Media Servers can share the devices that are attached to an NDMP host. When you add an NDMP host, the Media Server that you used to add the server is automatically selected for sharing.

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 addresses* that define 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 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 NetBackup 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 any 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, DXi6800, DXi6900, or DXi9000 inquiry response string as the identification for each model, respectively.) This allows product identification for the service teams at both Veritas 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 NetBackup. 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 HBA.

Obtain and apply the latest maintenance release.

Before starting the Device Wizard, make sure you have the latest mapping files for your NetBackup application. For UNIX/Linux systems and Windows systems, refer to https://www.veritas.com/content/support/en_US/downloads.

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 NetBackup, the inquiry string the device provides must match exactly with what is documented on the Hardware Compatibility Guide

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.

It is recommended that backups be staggered so that only a subset of drives is in use at any 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 makes it possible 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. On the contrary, it could 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
DXi470x	64	32	1,650 MB/s (5.9 TB/Hr)
DXi4800	150	32	12,800MB/s (46.0 TB/Hr)
DXi4800 (with memory upgrade kit and ISC enabled)	150	150	
DXi6700	80	80	972 MB/s (3.5 TB/Hr)
DXi6701 / DXi6702	256	80	1,580 MB/s (5.7 TB/Hr)
DXi690x 256GB	512	256 **	6,277 MB/s (22.6 TB/Hr)
DXi690x-S 256GB	512	512 **	9,722 MB/s (35.0 TB/Hr)
DXi9000 (192 GB)	512	256	25,600MB/s (92.0 TB/Hr)
DXi9000 (384 GB)	512	512***	
DXi9000 (768 GB) (VDMS)	1000	512	
DXi9000 (768 GB and ISC enabled)	1000	1000	

* Virtual Tape Drives; max # defined in the system
** Quantum suggests that you contact NetBackup about possible limitations or other considerations related to the maximum number
   of concurrently active VTDs
*** 150 VTDs are pre-installed on the system, effective with DXi Software version 4.1. A 512 VTD license is factory-installed.

Virtual Tape Drive Management

The NBU utility **tpconfig** cannot remove Tape Drives with indexes greater than 256. To remove these Tape Drives, use the utility **vmglob** instead.

vmglob -delete -drive -drvtype <drive_type> -serial <serialnum> -name <drive_name>

Storage Lifecycle Policies

Quantum recommends that you **DO NOT** use Storage Unit Groups in conjunction with Storage Lifecycle Policies. Both features are completely permissible in their own rights when used properly and in the appropriate applications. However, using both features at the same time can result in problematic situations.

Storage Unit Fragment Size

Based on customer feedback and performance tuning testing, you can balance backup and restore operations by reducing the fragment size for the storage unit in NetBackup.

(See Veritas Articles 11412 for background information and how to change the "Maximum Fragment Size" setting.)

- At the cost of some performance, use smaller Fragment sizes in mission critical or unpredictable ecosystems where power and network connectivity may cause occasional jobs to fail in the middle. Creating smaller Fragments ensures that partial backups can succeed, and that subsequent retries will only need to move the balance of a previously failed backup job. Smaller fragment size settings result in more filemarks on tape, which consume space and cause the tape to fill up faster.

- Use smaller Fragment sizes when backup jobs are large. This will help performance when jobs might span a Tape or Storage Unit and will help restore operations.

- Use a larger Fragment size where performance is key, and where starting a failed backup job from the beginning will not impact overall backup scheduling.

- If restores are failing or performing poorly, reduce the Fragment size as one diagnostic tool.

Network Buffering for Windows Servers Overview

Windows NetBackup network buffering only has three components: **NET_BUFFER_SZ**, the **Buffer_Size** Registry value and the Communications buffer. For Windows NBU Media servers, **Buffer_Size** is used, and the default value varies by NBU version. **NET_BUFFER_SZ** does not exist by default; it is configured by the user and will supersede **Buffer_Size**, if it does exist. The Communication buffer is for clients. It is set in the NBU GUI.

NOTE: For optimal performance, the NetBackup client **Buffer_Size** KB value should match the Media Server **NET_BUFFER_SZ** byte value.

There are several Veritas Tech Notes on this subject. Quantum highly recommends referring to all of them before deciding to make changes to the NetBackup environment. This is a very complex subject, and many unintended consequences and unexpected results may occur if all of the following information is not considered fully. The Tech Notes include but are not limited to:

- Where are the values for SIZE_DATA_BUFFERS, NUMBER_DATA_BUFFERS and NET_BUFFER_SZ located on Windows NetBackup Servers?

- NET_BUFFER_SZ, SIZE_DATA_BUFFERS and NUMBER_DATA_BUFFERS on UNIX - how they work and how to configure them

IMPORTANT: After making any changes, it is vitally important to verify that the following tests can be completed successfully:

1. Run a backup.
2. Restore data from the new backup created in step 1.
3. Restore data from a backup created prior to the changes to **SIZE_DATA_BUFFERS** and **NUMBER_DATA_BUFFERS**.
4. Check the number and size of the data buffers used by the NetBackup Media Server, by looking in the **bptm** log file.
5. Make sure that there is sufficient shared memory. Increasing the size and number of data buffers will use up more shared memory, which is a limited system resource. The total amount of shared memory used is:

(buffer_size * num_buffers) * drives * MPX

Tape Cartridge Capacity Considerations

Space on a given tape cartridge cannot be reused until after all backup data on that cartridge has expired, **AND** DXi space reclamation has run. 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 virtual tape cartridges, 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 to the NetBackup 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 operations 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, as permitted by the tape drive emulation. The minimum is 5GB.
- Capacity utilization is tracked in UNCOMPRESSED GB, and data is stored in compressed form.

The user may choose any destination cartridge size for Application Specific Path to Tape, because the application will automatically span cartridges if necessary.

Tape Drive LUN Mapping

Quantum recommends the following best practices:

- Map the device starting with LUN 0 on each port, and **do not** skip any LUNs.
- Zone the VTL devices and the NetBackup Media Servers together, to prevent other servers from taking control of the VTL resources.
- Use the HBA driver to bind the devices to a specific address. This helps keep devices in the same order after a reboot.
- Set the **WWNN = WWPN** for DXi systems. This allows for binding on the HBA to use either WWNN or WWPN.

Path to Tape Zoning Considerations

When configuring NetBackup for Path to Tape zoning with a DXi, Fibre Channel, consider the following:

- Use only single initiator to single targets zoning
- Do not share drives between FC ports — dual path is not supported.

Backup Application Specific Path to Tape

When creating physical tapes from virtual tapes in a DXi, you have two options:

- Clone tapes through the NetBackup Media Server.
- Use the DXi Backup Application Specific Path to Tape option.

Using the Backup Application Specific Path to Tape option has important advantages for the end user. Among these are:

- This process creates physical media from the data stored on virtual tapes, using a dedicated Fibre Channel connection and a directly connected tape library.

- The data is moved by the DXi and does not use the resources of the Media Server, freeing the Media Server's resources for other operations.

- Because the operation uses NetBackup to coordinate the data duplication, there is a single point of management.

- The NetBackup catalog tracks the virtual and physical tapes as separate instances and allows you to assign them different expiration policies. For example, you might decide to expire the disk-based virtual tape copies after 60 days but retain the copy of the data on physical tape for 24 months.

- The close integration of DXi and NetBackup 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.

For details about the Backup Application Specific Path to Tape option, see the information for your specific DXi model in the *Quantum DXi-Series: Backup Application Specific Path to Tape Configuration Guide* listed in the VTL documents section of this document.

VTL Fibre Channel Performance Tuning

To enhance performance for NetBackup 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 KB article mentioned above.

Configuring NetBackup with DXi NAS

A Network Attached Storage (NAS) 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.

Note: The DXi is **NOT** a Network Attached Storage device to be used to store customer data. The DXi only emulates a NAS device for the sole purpose of being a Backup-to-Disk target for backup applications such as NetBackup. **DO NOT** use the DXi NAS share as "Drag-and-Drop" file storage.

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

CIFS/SMB Protocol -The CIFS/SMB (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.

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 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: Regardless of which type of bonding is used on the DXi (Round Robin or LACP), the ports on the Ethernet switch that the DXi are connected to must be in a matching group type as the bond on the DXi.

Veritas NetBackup seamlessly integrates with a DXi-Series disk backup system using the NAS (CIFS or NFS) interface. Once installed and configured, NetBackup 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 NetBackup for NAS operation consists of the following major steps, which are discussed below:

- » **Configure the DXi for NAS**
- » **Configure the NetBackup NAS Storage Device**

Configure the DXi for NAS

The DXi system allows you to configure it to present its storage capacity as NAS shares that are compatible with NetBackup. You can create NAS shares for use with Windows or UNIX/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. The NAS license is preinstalled on DXi4800 and 9000 Series systems.

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 a NetBackup Media Server. CIFS (Windows) and NFS (UNIX/Linux) are available on the **NAS > Summary** tab. After NAS Shares have been configured on the DXi, NetBackup can be configured to use these shares as storage resources.

Configure the NetBackup NAS Storage Device

On CIFS platforms, from the NetBackup Master Server, you can **Create New Storage Unit** resources for the NetBackup environment. Although the DXi is presenting its storage capacity as a NAS share, and NetBackup will be creating a network-based storage resource, you still must choose Storage Unit Type **Disk,** then Disk Type **BasicDisk** when configuring NAS storage.

In the **"Absolute pathname to directory"** field, you must specify a path that includes the FQDN "Fully Qualified Domain Name" (or IP address) to the DXi share directory you wish to use as a storage unit. Entering the **<\\DXi FQDN\NAS share name>** in this field will enable the NetBackup Media Server to access specific DXi shares. It is possible to use short names for the share directory, if DNS is configured properly.

Note: NetBackup recommends AGAINST configuring multiple BasicDisk storage units to share the same path, since this may lead to unexpected behavior with respect to capacity watermarks on NBU.

On UNIX/Linux platforms, you must first mount the NFS share on the host OS of the Media Server you plan to use to back up your data. *Use NFS version 3 mount options per your OS' network file system mounting instructions.*

From the NetBackup Master Server, you can **Create New Storage Unit** resources for the NetBackup environment. Although the DXi is presenting its storage capacity as a NAS share, and NetBackup will be creating a network-based storage resource, you still must choose Storage Unit Type **Disk,** then Disk Type **BasicDisk** when configuring NAS storage.

In the **"Absolute pathname to directory"** field, you must specify the local path to a previously mounted share from your DXi (see the UNIX/Linux platform instructions above). In this example, entering the **</mnt/dxi_share>** allows the NetBackup Media Server to access to the DXi's NFS share called **dxi_share** (previously mounted at **/mnt/dxi_share**) for use with your backups. Best Practices Guide with DXi NAS

Best Practices Guide with DXi NAS

Number of Shares Considerations

Quantum DXi systems support both CIFS/SMB (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 NetBackup. 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.

In NFS environments, 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 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.
- Cabling:
  - Use only CAT5e or CAT6 cables (1Gb/s rated cables).
  - Use only OM3 or OM4 (Aqua) Fibre Optic cables (10Gb/s rated FC).
- If you are using a DNS server, verify that the DNS server configuration settings are correct and don't conflict, by using **nslookup** on the host name, as well as the IP address.
- It is also a good idea to add the HOSTNAME 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.
- Install and configure multiple network ports on the NetBackup Media Servers. Dedicate multiple ports for the transfer of data to the DXi.
- Install and configure multiple network ports on the Media Servers. Dedicate multiple ports for the transfer of data from NetBackup Client to the Media Server.

- Set up multiple networks and segregate traffic such that the NetBackup Client to Media Servers traffic does not interfere with the Media Servers to DXi traffic.
- For redundancy, connect at least two DXi ports to an Ethernet switch.
- Leverage NetBackup's ability to use multiple Media Servers. This can help ensure the success of data backups, even if one Media Server goes down or loses connectivity with the DXi.
- Leverage the DXi's ability to set up multiple networks. The DXi network configuration allows for integration into nearly any networked environment.
- 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.

NetBackup Storage Settings and Tuning Considerations

When using a DXi as NAS for Disk Based Storage, consider the following when you create a new Storage Unit:

- Set the options for **NUM_DATA_BUFFERS_DISK** and **SIZE_DATA_BUFFERS_DISK** for optimal performance. Enabling these options may increase backup performance.

  To find what works best for your environment, compare the performance of jobs by changing these "DATA_BUFFER" settings.

  - NUM_DATA_BUFFERS_DISK 16
  - SIZE_DATA_BUFFERS_DISK
    - For Windows 2003 SP2 and above, use 262144.
    - For Windows 2003 SP1 and below, use 65536.
    - For UNIX/Linux, use 1048576.

Additional Best Practice Considerations

Several operational considerations are common to all three access methods (OST, VTL and NAS). See the Common Operational Considerations for NetBackup section for more information on Deduplication, Encryption, Compression, Backup Streams, and Replication.

Common Operational Considerations for NetBackup

Data Deduplication 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 ratio 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 with no 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 virtual machines, large databases, and unstructured data such as Microsoft Office documents (PowerPoint presentations, Word documents, and Excel spreadsheets), SQL, Oracle and Exchange databases, and source code.

Not So Good Candidates for Data Deduplication

Data deduplication does *not* work well with encrypted data, in-line compressed data, SQL with LiteSpeed (in-line compression), Oracle with multi-channel RMAN (in-line multiplex), Exchange 2010, and compressed or uncompressed music files or movies/videos.

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

Replication Considerations

For first-time replication setups, when the DXi share is first created, it is highly recommended to manually initiate a Replication while that share is empty. This facilitates the first replication following the first backup to that share/partition.

Keep in mind that:

- The replication is only available to NAS shares with deduplication enabled.
- The DXi supports 256-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.

Oversubscription of Space on the DXi

Deduplication will reduce the amount of space used on the physical system. However, Quantum recommends that you monitor for Low Space conditions on the DXi and free up virtual media and disk targets 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.

A different storage server should be created and used for each NetBackup domain (master server plus associated Media Servers). This segregates data so a NetBackup administrator cannot accidentally modify or remove backup images belonging to another domain.

When multiple hosts are using a single DXi system, you can distribute the load by dividing the hosts into groups. For more information, see the "Performance Tuning" section in the *OST Plugin Installation Instructions*.

DXi Multiprotocol Guidance - NFS/VTL Scenario

The NFS **Synchronous** setting requires all data written to be committed to physical storage; meaning that 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. You can change this setting through the CLI.

Asynchronous mode allows the system to acknowledge receipt of 'stable write' or 'commit' commands without having the data (and related metadata) fully written to disk. This mode allows backups to be completed faster (from the NetBackup point of view), but it creates 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, bursty and response-time-sensitive protocol.

In a mixed VTL and NFS environment, the DXi 2.1 you should change the configuration for NAS shares settings from the default mode of **synchronous** to run in **asynchronous** mode. You can do this in the Command Line Interface:

syscli --nfscommit async {--share <sharename>} | --all

All other multi-protocol combinations work well together, and the above recommendations apply to all operating systems and applications. Generally, reduced VTL traffic may lessen the frequency of NFS timeouts.

Performance Tuning Recommendations for NetBackup

Evaluating Backup and Restore Performance

A server's capacity to stream data over one or more ports varies, depending on the system model, bus architecture, storage, and memory. Heavily utilized systems will not provide optimal transfer rates, because CPU resources are in contention.

NetBackup lets you use the Administration Console to review completed jobs, including details on backup/restore sizes, job duration, and overall throughput, per job. You can also use the DXi GUI to view average ingest and restore rates during I/O. And Quantum DAR reports can give you additional details on throughput and capacity utilization. Quantum highly recommends using all these resources to evaluate your system's backup and restore performance.

Load Distribution and Capacity Planning

NetBackup allows servers and clients to share DXi resources. You can use this to maximize performance by running concurrent backup or restore operations. For example, you can configure multiple drives in a VTL and split the server's work load among them. Similarly, with NAS shares, you can configure multiple targets as storage units to service individual jobs submitted by the servers and their clients.

Perform test backups to determine how long it takes to complete the jobs. Adding additional media servers or storage targets can help you maximize the I/O on a DXi system.

Additional Considerations for Highly Utilized Systems, Heavy Network Traffic, or Low-Latency Networks

Here are some adjustments you can make:

- Adjust the client connection and read timeouts. For example, you can adjust the Client Connect Timeout from 300 seconds to 32767, and the Client Read Timeout from 300 seconds to 32767.

- Adjust the OST Optimized Duplication Timeout. You can adjust the OPDUPE timeout from 86400 seconds (24 hours) to 129600 seconds (36 hours).

- Adjust the TCP **Keepalive** settings, using the OST plugin.

  The OST plugin configuration file lets you configure TCP Keepalive parameters for the OST network traffic, so that the overall Operating System TCP Keepalive parameters don't need to be changed. For more information, see the Client Plugins page.

  Here are some OS-specific setting changes you can make.

    o Adjust TCP Keepalive on Linux Servers – sysctl

      (See the TCP-Keepalive-HOWTO).

      ```
      Example:
      sysctl -w net.ipv4.tcp_keepalive_time=900.
      Edit  /etc/sysctl.conf and add the following line:
      net.ipv4.tcp_keepalive_time=900
      ```

    o Adjust TCP Keepalive on Microsoft Servers

      See Veritas Article 100028680

- Thread optimization with limiting MAX_QUERY_TASKS is addressed in 7.6.0.2.

  See Vertias Article 000019342

- Semaphore Usage (UNIX Masters)

  With many processes running on the master, it is important to review system semaphore usage and potentially raise the semaphore limits to ensure that there are no semaphore constraints.

  The following are recommended semaphor values:

  300   307200   32   1024

  More information on configuring these values can be found in this article:
  Recommended NetBackup *NIX semaphore tuning values (Linux/Solaris/HP-UX/AIX

Block Size Limitations on Tape

Some Fibre Channel host adapters limit the maximum block size that is written to tape. This means that you must take additional steps to configure the HBA for a larger block size.

Qlogic provides a utility with their driver distribution.

Example:

Default Transfer Size: 512 KB

 >qlfcx64.exe -tsize /fc /set 2048

 >qlfcx64.exe -tsize /fc

 Transfer Size: 2048 <-shows the maximum block size now set to 2048 KB.

After a reboot, the block size limitation is increased.

Emulex adapter block size changes are implemented with the **ONCommand** utility:

1. Select the HBA port.
2. On the Driver parameter tab, change E**xtTransferSize** to the desired size.
   Options are Extended transfer size: 0 = 512Kbytes: 1 = 1Mbyte: 2 = 2Mbytes: 3 = 4Mbytes

Helpful Resources

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

Retired Best Practice Guides from Quantum:

- *Best Practice Guide – NetBackup from Veritas with DXi-Series*
- *Quantum DXi8500, DXi7500 and DXi6700: Veritas NetBackup Application Specific Configuration Guide*

Quantum Web Site

http://www.quantum.com

StorageCare Guardian Web Site

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

Quantum Service Web Site

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

For support information and telephone numbers, see the Web site listed above.

Appendix A

Using NetBackup OST with Quantum Q-Cloud Storage

Quantum offers secure OST backup and archive to the cloud by integrating Veritas OST with DXi systems. This lets users back up directly to the cloud and/or build an archive in the cloud using a Storage Lifecycle Policy (SLP). The advantage to the user is that the backup application is completely aware of all copies in the cloud and can access them at will.

Users have three backup options:

- Back up directly to a DXi in the cloud, using OST. Data security can be ensured by using a Virtual Private Network (VPN) link between the user and the cloud storage.

- Back up directly to a DXi in the cloud, using DXi Accent (a no-cost feature of DXi) to only send compressed, new, unique data. This reduces the network volume and can reduce the backup window on high latency links. It has the additional benefit of being able to use native DXi encryption.

- Back up to a local DXi, providing a faster backup and restore. Then use Veritas Optimized Duplication (Opt Dup) to send a copy to a DXi in the cloud. Each copy can have its own retention policy. No-cost options are available to encrypt the data while in transit, or the user may elect to use a VPN.

Architecture

Figure 1 shows the requirements for supporting OST links for Q-Cloud storage.

The **Route A** path shows the requirements for backing up directly to the cloud, using either OST or DXi Accent.

- OST backups require all listed firewall ports, except 80 and 1062. An OST backup will not be deduplicated or compressed, so all data will be sent byte-for-byte as it is backed up. OST backups will run slower on a cloud link with, latency higher than 10 msec. The higher the propagation latency, the longer the backup will take. If the user wants to back up directly to the cloud and the link has high latency, DXi Accent backup is preferred.

- DXi Accent is a no-cost feature included with every DXi system. DXi Accent will deduplicate the backup data on the backup server and send only compressed unique data to the cloud. This can: 1) reduce the network load; and 2) reduce the backup window if network loading and/or propagation times have been extending the backup window. DXi Accent is not all-or-none but can be configured for individual backup servers. DXi Accent requires DXi OST plugin v2.6 or newer.
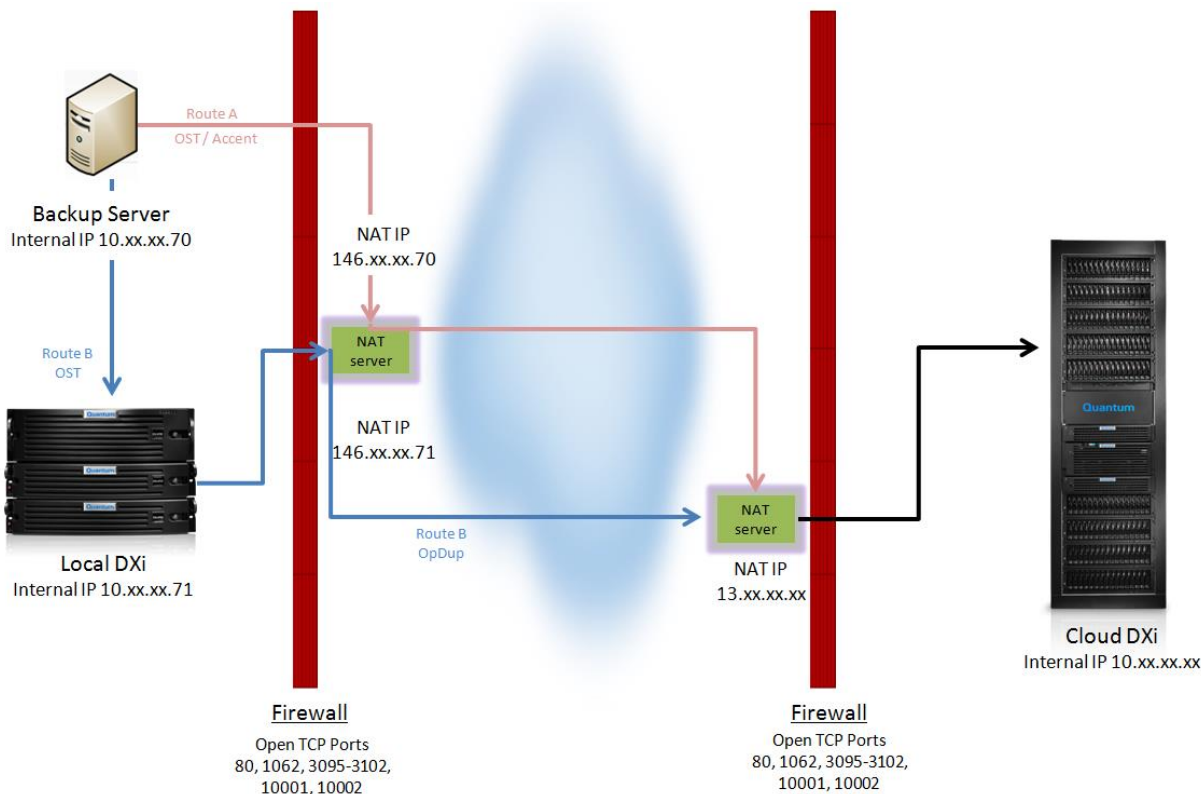
Figure 1 - Diagram showing backup options when using OST to store data in the Q-Cloud.

Route B shows an OST backup directed to a local DXi, which then leverages the backup application's Storage Lifecycle Policy (SLP) to automatically send a copy of that backup to the cloud, using Optimized Duplication (Opt Dup).

- The backup application is aware of both copies, and different retention policies can be leveraged for each copy. For example, using the backup application's retention policies, it is possible to retain the local copy for a much shorter period than the cloud copy, essentially treating the cloud as an archive.

- Backing up to the local DXi has the advantage of providing the highest throughput, resulting in the shortest backup window.

- Opt Dup uses DXi replication to transfer a copy of the backup to the cloud DXi. Only unique data is transferred, reducing network bandwidth requirements. The DXi can be configured to encrypt the network transfer using AES-256, reducing the requirement for VPN service.

- Opt Dup requires that all ports shown in the diagram be open in both firewalls.

Connectivity and Configuration Details

Figure 1 shows the logical path that data must traverse.

The requirements for **Route A** (DXi Accent backups directly to the cloud) are:

1. Obtain a NAT address for your backup server (a NAT address is required for the Master server and each Media server that will be backing up and restoring data to and from Q-cloud).

2. Confirm that the ports in the local firewall are open.
    o For OST: Ports 3095-3102, 10001, 10002
    o For DXi Accent: port 80, 1062, 3095-3102, 10001, 10002

3. Obtain the following from Quantum Q-Cloud:
    o The NAT address for the cloud DXi from your cloud service provider. Be sure and add this NAT address as an allowed IP to your firewall rule.
    o The OST storage server and LSU names that you will be writing to.

4. Provide Quantum Q-Cloud your NAT IP address, so they can add it to their firewall rule.

5. Add the NAT address of each DXi (Source and Target) Using the GUI, select **Configuration > Replication> Send "Source IP Address" box**.

6. Configure your backup server(s) to use OST to back up to the cloud LSU.

The requirements for **Route B** (OST backup to local DXi with Opt Dup to the cloud) are:

1. Obtain a NAT address for each backup server. All backup servers must be able to see the remote DXi in order to manage the entire Opt Dup lifecycle. A NAT address is required for the Master server, and for each Media server that will be backing up and restoring data to and from Q-cloud.
2. Obtain a NAT address for your local DXi.
3. Confirm that the ports in the local firewall are open and consider the possibility that a "keepalive probe" may be required to keep ports open.
    o You need all these ports: TCP ports 80, 1062, 3095-3102, 10001, 10002.
4. Obtain the following from Quantum Q-Cloud:
    o The NAT address for the cloud DXi. Be sure to add this NAT address as an allowed IP to your firewall rule.
    o The OST storage server and LSU names that you will be writing to.
5. Provide Quantum Q-Cloud both of your NAT IP addresses, so they can add them to their firewall rule.
6. Configure an OST storage server and LSU on your local DXi.
7. Add the NAT address of each DXi (Source and Target). Using the GUI, select **Configuration > Replication-> Send "Source IP Address" box.**
8. Configure all backup servers to use OST to back up to the local LSU.
9. Create the backup policy and the Storage Lifecycle Policy (SLP) for copying the backup to the cloud.
10. If you choose to duplicate the OST Storage Server from the cloud DXi back to the local DXi, you or Quantum Q-Cloud will need to issue an **opduptranslate** command to the remote/cloud DXi via its CLI. There is also a GUI option for **opduptranslate** configuration (**Configure > OST > Target IP Mapping**).

    Notes:
    o [In a single-tenant DXi hosting configuration, you will most likely be able to do the above configuration yourself. In a multi-tenant DXi hosting configuration, the Q-Cloud will have to do the above configuration for you.]
    o Consider that the backup server knows the cloud DXi by its NAT IP address and knows the local DXi by its local IP address. The cloud DXi does not know the local DXi's local IP address. It only knows the local DXi by its NAT IP address. So, you need to tell the remote DXi that when the backup server contacts it with a reference to the local DXi, using the local IP address, the cloud DXi should translate that to the NAT address.
    o Command format:
    ```
    bash-3.2$ syscli --add opduptranslate --replicationip <NAT IP> --
    dataip <local IP>
    ```

Other related **syscli** commands are listed below. Note that:

- o "Replication IP" is the same as "NAT IP" and "data ip" is the same as "local ip".

- o If you make a mistake when entering the **opduptranslate** command, you will have to delete the erroneous entry and make a new entry. This happens because **opduptranslate** commands do not "overwrite" or replace previous commands for that local IP.

- o Verify that you have the correct entry by reviewing the output of the "list" command.

  ```
  bash-3.2$ syscli --help opduptranslate

  syscli --add opduptranslate --replicationip <replication_ip> --
  dataip <data_ip>
  ```
  Lets you map the OST target IP address to a replication IP address.

  ```
  syscli --del opduptranslate --dataip <data_ip>
  ```
  Allows you to delete the mapping of the OST target IP address for a replication IP address.

  ```
  syscli --get opduptranslate --dataip <data_ip>
  ```
  Gets the replication IP address for a translated OST target IP address.

  ```
  syscli --edit opduptranslate --replicationip <replication_ip> --
  dataip <data_ip>
  ```
  Allows you to edit the existing map of an OST target IP address to a replication IP address.

  ```
  syscli --list opduptranslate
  ```
  Lists all mappings of OST target IP addresses to replication IP addresses.

11. You may need to run TCP "Keep Alive Probes" to prevent firewall ports from closing before the operations have completed. If the ports close prematurely, it will cause a connection error, resulting in the appearance that media is missing. A workaround for this situation is to restart NetBackup services.

The following articles provide helpful tips in setting Windows TCP Keepalive timer values on the NetBackup Server:

KeepAlive Time - Microsoft TechNet

The OST plugin configuration file also provides a means to configure TCP Keepalive parameters for the OST network traffic so that the overall Operating System TCP Keepalive parameters don't need to be changed. See the Quantum DXi-Series: NetBackup and Backup Exec OST Configuration Guide or the Plugin Configuration file for more information.