DXi-Series Configuration and Best Practices Guide

For Backup Exec from Veritas™

Quantum#: 6-67709-01 Rev J

BPG00019A-v06

Table of Contents

DXi-Series Configuration and Best Practices Guide for Backup Exec 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 Backup Exec 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 Backup Exec with Quantum DXi-Series systems. This guide includes advice and best practices for using Quantum DXi-Series systems with Backup Exec.

How to Use This Guide

This document assumes that the reader has basic expertise with Veritas Backup Exec 2012 or newer, as well as basic networking and SAN experience. It also assumes that the reader has a Quantum DXi installed in a working Backup Exec environment.

This document provides key recommendations and useful information for quickly setting up a DXi system with Veritas Backup Exec. 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 Backup Exec. 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 Network Attached Storage device (NAS) over NFS and/or CIFS. These access methods are discussed in the following order.

- DXi OST (Veritas 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 that section's name.

Documentation and References

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

Online Documentation for your Quantum product

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

DXi-Series Management Console, 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

Backup Exec Installation Documentation

- Veritas Backup Exec Documentation
- Veritas Backup Exec Administrator's Guide (PDF)
- Best practices for Backup Exec 16 installation
- Veritas Desktop and Laptop Option (SDLO) Version 7.0 Administrator's Guide:

Note: Veritas DLO is not currently supported by the Quantum DXi product line. Veritas offers no standard certification testing for DLO and offers no specific guidance on the resource requirements of DLO to target backup appliances. Quantum is working with Veritas to determine the current requirements for DLO, and with what parameters DLO can be tested and certified with a DXi target deduplication.

Summary of Tuning Parameters for Backup Exec

For backup administrators who are well versed on Veritas Backup Exec 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.

Parameter or Option	**Recommendations**
Compression	No
Encryption	No
Deduplication	No
OST Options	
Concurrent Streams	2
VTL Options	
VTL sign-on string	Use native DXi Inquiry. Emulated library sign-on strings are not supported.
Drive sign-on string	Emulate as per the Backup Exec HCL: • DXi4000-Series/DXi6700/DXi9000-Series: HP LTO4 For additional emulated tape drive types, see the appropriate Veritas Backup Hardware Compatibility List (HCL).
BUE Device Tab	• Block size: 1024KB on LTO4 • Buffer size: 1024KB • Buffers: 30 • High water mark: 15
Miscellaneous Options	
Server Resources	Set up no more than 1-2 drives per 3.x GHz CPU core. The server should have 2GB RAM, plus 1GB per drive. If performance per data stream seems low, disable CPU Hyperthreading on the master or media server, and verify whether this improves your speed per stream. You may need to keep Hyperthreading disabled for best throughput per stream.
Server Name	Use only standard ANSI characters for the computer name of the computer on which you want to install Backup Exec. You may receive errors if you install Backup Exec on a computer with a name that uses non-standard characters.
Backup Exec GRT (Granular Restore Technology)	OST is highly recommended over CIFS, especially for large or complex environments where performance may be as much as 5x better than CIFS.
Windows OS Options	
Services	• Disable the Removable Storage Manager (RSM) service. (No longer present in Win2003/2008) • Disable the Microsoft Volume Shadow Copy service. • Disable the Microsoft Advanced Open File System service. **Note:** Stop, then restart, the BE device services after making these changes on each Media Server.

Network	On heavy utilized systems, consider increasing the TCP/IP timeout on the Backup Exec media server. See the Microsoft Knowledge Base: http://support.microsoft.com/kb/q191143/ **TcpMaxDataRetransmissions** Adjusting the following TCP/IP setting by adding a subkey in the registry should reduce the number of timeouts by allowing more time for the connection to complete. This setting is not present in the registry by default. 1. Start the Registry Editor (**Regedt32.exe**) and go to the following subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 2. On the **Edit** menu, click **Add Value**, then add the following information: Value Name: TcpMaxDataRetransmissions Value Type: REG_DWORD Valid Range: 0 - 0xFFFFFFFF Default Value: 5 Decimal New Value: 10 Decimal 3. Click **OK**, then quit the Registry Editor. 4. Reboot after the registry change has been made. 5. Apply the following Microsoft hot fixes to improve performance: ○ 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:

- See the Veritas Backup Exec Administrator's Guide on the Backup Exec Documentation page for comprehensive information about Backup Exec.
- Use the Backup Exec Help for searchable, topic-based documentation.
- Use the **Getting Started** screen to help you work through the most common configuration steps.
- Use the **Backup Exec Assistant** for access to wizards, documentation, and technical support.

Configuring Veritas Backup Exec 16 with the DXi-Series

Configuring Backup Exec with DXi OST

OpenStorage API Support

The integration of Veritas's OpenStorage (OST) API initiative with Quantum's DXi4000-Series, DXi6700, DXi6900 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 Backup Exec to duplicate data between DXi-based LSUs in different locations. This provides disk-to-disk DR protection and leverages the DXi's deduplication technology to dramatically reduce network bandwidth requirements.

DXi systems can copy data from one system to another (can perform replication). Backup Exec uses this capability to initiate an optimized duplication of backup images between these appliances. The duplication operation of Backup Exec 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 Backup Exec 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 Backup Exec 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 a disk backup target.

Veritas Backup Exec OST (OpenStorage) allows Backup Exec to seamlessly integrate with a DXi-Series disk backup system. Once installed and configured, Backup Exec 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 Backup Exec OST for operation consists of the following major steps, which are covered below:

1. **Install the DXi OST License Key**
2. **Configure the DXi for OST**
3. **Install the OST Plug-in on the Backup Exec Media Server**
4. **Configure the Backup Exec Media Server with OST**
5. **Back Up to the DXi OST Storage Target Device**
6. **Configure Backup Exec Optimized Duplication**

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 below.

Configuring the DXi for OST

The following steps outline the configuration process at a high level. For detailed instructions, refer to the Veritas Backup Exec OST Guide.

Install the DXi OST License Key

Before you can configure the DXi with OST, you must install the OST license key. To install the OST license key, you must obtain a License Certificate containing an authorization code.

To find the license key:

- DXi6700 - The OST license is included with all DXi6700 systems. A License Certificate containing an authorization code is included in the accessory kit that shipped with the system. Visit http://www.quantum.com/licensekeys to obtain OST License Keys for your DXI. You will be asked for the DXI serial number and authorization code. Once you have OST license key, install it from the DXI Remote Management Console, under **Utilities > License Keys**.
- DXi4000-Series, DXi6900/6902, and DXi9000-Series - The OST license key is preinstalled on these systems. You do not need to install the license key on these systems.
- 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 http://downloads.quantum.com/dxiv1000/6-67611-01_DXi_V1000_QuickStartGuide_RevA.pdf.

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:

- You must configure storage servers and logical storage units on the DXi remote management console before you configure Backup Exec.
- You can also use the OST Wizard 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.

Note:

- For usernames, alphanumeric characters are allowed, as well as underscores (_) and hyphens (-).
- For passwords, alphanumeric characters are allowed, as well as the following special characters: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " , < . > / ?

Caution: In DXi 2.x 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 to DXi 2.0.x software 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 Backup Exec 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 Backup Exec services.

Note: Quantum recommends that you create a different storage server for each Backup Exec domain (master server plus associated media servers). This segregates data, so that a Backup Exec 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	Possible Values	Recommended
Max Connections	3 – 65536	300
LSU Images		250
LSU Capacity	Available / Specific	Available*

* See the Special Environment Considerations section below for cases that contradict this recommendation.

Install the OST Plug-in on the Backup Exec Media Server

Before you can configure Backup Exec with DXi OST, you must download and install the OST Plug-in and install it on the media server configured with Backup Exec. You can access the Quantum Client Plugins download page at:

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

On the Quantum Web page that displays:

1. Click the link for your operating system to see the available OST Plug-in download options.
2. Click the links to download the latest Quantum OST Plug-in and the *OST Plug-in Installation Instructions*. Make sure to download the correct OST Plug-in for the operating system installed on the Backup Exec media server.

This procedure is the same for each Backup Exec media server operating system platform. Follow the instructions to install the OST Plug-in on the Backup Exec media server.

Some items to consider:

- By default, the OST Plug-in for Windows is installed in the **C:\Program Files\Veritas\Backup Exec** folder.
- RAWS is an agent used to back up Windows clients (which Backup Exec calls *remote agents*). In Backup Exec 16, a remote agent (client) can perform client-side deduplication, which is called *Direct Access*. For this, the OST plug-in must be installed on the remote agent, and the plug-in **.dll** file must exist in the **\Backup Exec\RAWS** folder.

Configure the Backup Exec Media Server with OST

Please consult the *Veritas Backup Exec Administrator's Guide* for instructions on Backup Exec installation and basic configuration.

Note: Installation and licensing of the deduplication option in Backup Exec is required for OST support.

With Backup Exec, you can use the **Configure Storage Wizard** to configure all of your storage devices, including creating backup-to-disk folders and OpenStorage devices.

Note on Backup Exec User Accounts:

The Backup Exec System Logon Account (SLA) is created when you install Backup Exec. When the SLA is created, the user name and password match the credentials that were provided during installation for the Backup Exec Services credentials. The owner of the SLA is the user that installed Backup Exec, which is a common account, by default. Common accounts are shared accounts that all users can access.

The Backup Exec System Logon Account may have access to most or all of your data, since it contains the Backup Exec Services credentials. Quantum suggests that you keep the following in mind:

- If you want to make Backup Exec more secure, you can change the SLA to be a restricted account.
- You can also delete it after making another logon account the default. However, if you delete the SLA, the jobs in which it is used may fail.
- If the SLA is deleted, you can re-create it using the Logon Account Management dialog box.

The SLA is used for the following tasks and jobs:

- Jobs that were migrated from a previous version of Backup Exec
- Duplicate backup data jobs
- Command Line Applet (**bemcli.exe**)

OpenStorage (OST) devices are created using the **Configure Storage** task under the **Storage** tab.

Important Notes:

- When you create an OST device in Backup Exec, the format of the "**Server name:**" required in the dialog box must be ***<OST Server_DXi FQDN>***.
- For example, in the step above, if you created a Storage Server called "OSTserver1" on a DXi named "QuantumDXi1.mycompany.com", the server name must be specified as **OSTserver1_QuantumDXi1.mycompany.com**

  See Entering an OpenStorage (OST) device server name incorrectly or using improper credentials results in "A deduplication storage folder was not found" error message for further information.

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

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

About Sharing a Deduplication Device between Multiple Backup Exec Servers:

If you use the Backup Exec Central Admin Server option, you can select which Backup Exec servers can share a deduplication disk storage device or an OpenStorage device. When you add a deduplication disk

storage device or an OpenStorage device, the Backup Exec 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 Backup Exec servers that you want to have access the device, except for the Backup Exec server that was used to create it.

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.

Configure Backup Exec Optimized Duplication

Data can be copied from one DXi system to another DXi system (to perform replication). Backup Exec uses this capability to initiate an optimized duplication of backup images between these appliances. The duplication operation of Backup Exec 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 Backup Exec 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 Backup Exec 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 a disk backup target.

  Note: No more than two concurrent optimized duplication streams per source DXi to a target DXi are supported. Additional concurrent streams are not optimized.

- Using **Replication Channel** for OST allows the DXi to 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, only a single replication target 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 DXis be on the same subnet.

Special Environment Considerations

Certain environments might require special handling. These environments could be where there is a high number of OST images per LSU, a high job concurrency per LSU, or a high-latency network environment (i.e., WAN).

Background

Each Backup Exec backup job needs to list OST images before an OST image can be mounted and written. The frequency at which Backup Exec requires the list of OST images, in combination with the number of OST images created over time, might start to negatively impact the overall performance.

For the purpose of illustration, please note the following. Keep in mind that these numbers may vary, depending on the DXi series used, the hardware resources of the Backup Exec server, and the network environment.

- With no other OST jobs running, it takes approximately 20 to 30 seconds to enumerate about 10,000 OST images from a Backup Exec server with a DXi connected to the same LAN.
- If 10 backup jobs are running concurrently, the first one will start writing to its image in less than 30 seconds, while the last job will start writing to its image within 3 to 5 minutes (20 seconds x 10 jobs, to 30 seconds x10 jobs).
- If we double the number of images or concurrent jobs that exist, the elapsed time in a "queued" state will also double.

Through Quantum Accent technology, deduplication at the source is also possible (known as *client-side deduplication* in Backup Exec). The OST image enumeration in this case will be performed from the remote client. If remote clients have to cross high-latency networks to communicate with the DXi, additional delays will occur.

The increase in time span produced by these effects can range from a few minutes to several hours, especially under heavy loads with a high number of images on the LSUs. This can have a significant impact on backup windows.

Recommendations

- Keep the number of LSUs in line with the number of jobs and their frequency. Having many jobs (10 or more) running more than once a day against a single LSU can significant noticeable problems within 2 to 3 months of usage. To ensure that backup jobs are executed within the backup windows, create more LSUs and reduce the job frequency, or the number of jobs targeted to LSUs.

- Keep data retention in line with the number of jobs and their frequency. Having higher data retention will cause Backup Exec to create more OST images, rather than re-using the existing ones.

- Where possible, use a mixture of DXi deduplication jobs and Quantum Accent client-side backup deduplication jobs. Environments where all or most backup jobs are client-side deduplication jobs will incur further delays if remote clients have to cross high-latency networks.

Deduplication Considerations

Deduplication works by dividing data into segments and then storing the segments on disk, along with a database to track the segments. When a backup application 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:

- Where the file system data is from Windows and Linux
- Where the same file is backed up multiple times
- Where the percentage of data that changes is small

Backup Streams Considerations

A different storage server should be created and used for each Backup Exec domain (master server plus associated media servers). This segregates data, so that a Backup Exec administrator cannot accidentally modify or remove backup images belonging to another domain.

Optimized Duplication Considerations

- To increase performance, configure the DXi to use the Replication Channel when performing optimized duplication.
- No more than two concurrent optimized duplication streams per source DXi to a target DXi are supported. Additional concurrent streams are not optimized.

Additional Best Practice Considerations

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

Configuring Backup Exec 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 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 Path Considerations

One of the key ways to ensure that SAN-connected physical and virtual tape libraries are detected properly by backup servers is *serialization*. Serialization provides a unique identifier for each device in a physical or virtual tape library, to automate device association from multiple backup servers. These identifiers, returned by the VTL devices, are separate from the *element 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 Backup Exec device discovery to align these two addresses, reducing the potential for improper configuration.

Quantum suggests that you keep the following suggestions in mind:

- If the Device Configuration Manager does not serialize the devices listed, do not commit the changes, and be sure to check the VTL online state. The DXi VTL partition must be online for this to function properly.
- The Quantum recommended device identification for each DXi system is the native mode. (In other words, use the DXi4700, DXi6700, 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 not an error, and does not create a problem for Backup Exec. 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.
- Always ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and HBA. For best performance, Veritas drivers should be loaded for the tape drive. Veritas does not test performance or compatibility with Original Equipment Manufacturer (OEM) drivers, unless otherwise noted on the Hardware Compatibility List.

Supported Hardware Compatibility List

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

For the device to work properly within Backup Exec, the inquiry string that the device provides must match exactly with what is documented on the Hardware Compatibility List (HCL) for your Backup Exec version.

Configuring the DXi for VTL

Veritas Backup Exec seamlessly integrates with a DXi-Series disk backup system using the VTL interface. Once installed and configured, Backup Exec 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 Backup Exec for VTL operation consists of the following major steps:

1. **Configure the DXi for VTL.**
2. **Configure the Backup Exec Library and Tape Drives.**
3. **Perform a Test Backup to the DXi VTL Storage Target Device.**
4. **Configure Backup Exec 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 existing backup software. Virtualizing disk storage as tape allows integration of VTLs with existing backup software, and with existing backup and recovery processes and policies. The benefits of such virtualization include storage consolidation and faster data restores.

In the Remote Management Console, under the **Configuration** tab, the **VTL** page allows you to configure a DXi to present its storage capacity as VTL (virtual tape library) partitions that are compatible with standard backup applications. You can add virtual tape drives and storage slots to VTL partitions, and you can create and work with virtual tape cartridges. You can also map partitions to hosts.

Partitioning lets you divide the DXi virtual tape drives and storage elements into separate partitions, usable by separate host computers. The **Partitions** page contains a list of assigned tape drives and lists 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 Backup Exec system is properly configured for the correct number of tape drives emulated in the DXi system partition. Failure to do so may cause Backup Exec to malfunction or cease to operate.

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

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

Caution: It is possible to oversubscribe space on the DXi system. The total capacity for all media could be more than the capacity of the system. Be careful to ensure that this does not happen.

Configure the Backup Exec Library and Tape Drives

To configure the Backup Exec library and tape drives, follow these steps:

1. Use the **Device Driver Installation Wizard** to install Veritas device drivers. You can run this wizard from the **Backup Exec Device Configuration Wizard** or from **tapeinst.exe**.

   Tapeinst.exe is located in the Backup Exec for Windows Servers installation directory. Updates for this program are available in the Device Driver Installer package. For complete information about downloading and running the Device Driver Installer package, go to http://www.veritas.com/docs/000013933
2. After you have installed device drivers and run the **Device Configuration Wizard**, initialize your library.
3. Inventory and label your virtual tapes.
4. 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 Backup Exec for Windows Servers Administrators Guide.*
5. If you will be using Backup Exec for DXi VTL NDMP Path to Tape, you must install the **Backup Exec NDMP** option locally on the media server as a separate add-on component of Backup Exec. Refer to “Installing Additional Backup Exec Options” in the Backup Exec Installation Guide.

Perform a 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 Backup Exec for DXi VTL Path to Tape

After the normal backup process has completed, Backup Exec 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.

Please note that:

- Because this is a normal duplication job, Backup Exec catalogs the physical tape copy in its database.
- Both the VTL and the physical tape library are visible to Backup Exec. Therefore, restores can be performed directly from either copy (virtual or physical).
- To duplicate the virtual tape image, Backup Exec selects an NDMP device path to the VTL and creates an NDMP control session for this device. It then 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. Backup Exec 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 DXi4000-Series, DXi6700, DXi6900, and DXi9000-Series systems. The NDMP option is installed as a separate component in Backup Exec to support this feature. You must dedicate a partition within the DXi for use with Backup Exec. The partition cannot be shared with another backup application.

Note: NDMP user names are case sensitive.

The following device paths must be visible to Backup Exec:

- 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.
- NDMP device paths to the attached physical tape devices, to read or restore data directly from a physical tape.

Please note that e DXi virtual medium changer must be viewed through TCP/IP and will appear as an NDMP host.

Backup Exec 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.
- Backup Exec 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: Refer to the Hardware Compatibility Guide for a complete list of supported libraries.

If you use the Backup Exec Central Admin Server Option (CASO) or the SAN Shared Storage Option (SSO), you can select which media servers can share the devices that are attached to an NDMP server. When you add an NDMP server, the media server that you used to add the server is automatically selected for sharing.

Robot/Media Changer Device Serialization Considerations

One of the key requirements 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, 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 Backup Exec device discovery to align these two addresses, reducing the potential for improper configuration.

Quantum suggests that you keep the following suggestions in mind:

- If the Device Configuration Manager does not serialize the devices listed, do not commit the changes, and be sure to check the VTL online state. The DXi VTL partition must be online for this to function properly.
- The Quantum recommended device identification for each DXi system is the native mode. (In other words, use the DXi4700, DXi6700, 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, and does not create a problem for Backup Exec. 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.
- Always ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and HBA. For best performance, Veritas drivers should be loaded for the tape drive. Veritas does not test performance or compatibility with Original Equipment Manufacturer (OEM) drivers, unless otherwise noted on the Hardware Compatibility List.

Device Driver and Firmware Level

Ensure that the latest drivers and firmware have been installed for the tape drive, robotic library, and HBA. For best performance, Veritas drivers should be loaded for the tape drive. Veritas does not test performance or compatibility with Original Equipment Manufacturer (OEM) drivers, unless noted on the Veritas Hardware Compatibility List. For Backup Exec 11 and higher, Veritas recommends running Live Update to apply updates to Backup Exec Media Servers:

To make sure that the installed drivers and firmware are up to date:

1. Run Live Update to apply the latest Service Pack (SP).
2. Run Live Update a second time to get the latest Hot Fix (HF) and Device Drivers (DDI) updates since the SP.
3. After the updates are applied to the Backup Exec Media Server, you must redeploy the Remote Agents, so that they receive the updates that Backup Exec recommends.

If a device is presenting itself properly to the operating system, it should provide the operating system an inquiry string. For the device to work properly within Backup Exec, the inquiry string the device provides must match exactly with what is documented on the Hardware Compatibility List (HCL).

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. However, this does not prohibit a single tape drive from using all available bandwidth. The media server typically determines individual tape drive performance.

To balance bandwidth use, consider the following:

- It is not a good idea to configure the maximum number of virtual tape drives and perform I/O through all of them concurrently. Better performance can be achieved by using a subset of those virtual tape drives at the same time.

  Quantum expects the customer configuration to distribute those virtual tape drives among multiple media servers, to simplify initial installation by providing dedicated resources to each media server.

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

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

The following table lists the recommended maximum number of concurrently active virtual tape drives for various maximum aggregate bandwidths.

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.

Tape Cartridge Capacity Considerations

Keep the following tape cartridge considerations in mind:

- Space on a given tape cartridge cannot be reused until after all backup data on that cartridge has expired.
- The greater the capacity of a cartridge, the longer it will typically take for all data on that cartridge to expire.
- Expired data continues to take up space on the virtual tape cartridge, as well as in the DXi, until that cartridge is overwritten, relabeled, or erased. This means that lower cartridge capacities are more desirable, so that tapes will be returned to the Backup Exec 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 permitted by the tape drive emulation; the minimum is 5GB.

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

If Application Specific Path to Tape is used, the ultimate cartridge destination size is the suggested size.

Quantum's general guidance is to specify a smaller virtual tape cartridge capacity, such as 50GB to 100GB, for the reasons mentioned above.

Tape Drive LUN Mapping

Quantum recommends the following tape drive LUN mapping strategies:

- Map the device starting with LUN 0 on each port, and **DO NOT** skip any LUNs.
- As a best practice, zone the VTL devices and the Backup Exec media servers 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.

Quantum DXi-Series VTL devices support reserve and release to accommodate sharing drives. This option allows devices to be shared between Backup Exec media servers. The advantage of this is that you will have a pool of drives available to each media server. Other SAN architectures assign drives to each media server and eliminate the shared function.

For both conditions, it is a good practice to keep the Backup Exec media server separate from the production server, to eliminate downtime from maintenance. This requires the media servers to have a fast network connection to the source data.

Application Specific Path to Tape

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

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

Using the Application Specific Path to Tape option has important advantages for end users. 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 Backup Exec to coordinate the data duplication, there is a single point of management. The Backup Exec catalog tracks the virtual and physical tapes as separate instances and allows you to assign different expiration policies to the different tape types. For example, you might decide to expire 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 Backup Exec 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, see the Application Specific PTT Guide for your model.

VTL Fibre Channel Performance Tuning

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

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

> “… a conflict in Windows Server 2003 causes a Test Unit Ready (TUR) request issue on SCSI-attached and fiber-attached devices. When this issue occurs, an overflow of TUR requests causes the storage unit not to respond or to respond slowly to SCSI commands. In a SAN environment, any Windows Server 2003-based computer that is zoned to detect the Tape Backup Unit hardware can send TUR requests.” The cause and workaround are documented in the Microsoft knowledge base article number 842411. Microsoft support link: (http://support.microsoft.com/kb/842411/en-us).

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

Handling of Expired Media within Backup Exec Considerations

When a tape is expired by Backup Exec, the event is not directly communicated to the DXi-series device. The result is that a tape may be displayed as empty or SCRATCH to the Backup Exec graphical Interface, but the same tape will display in the DXi-series GUI as containing data. This indicates that the data on the expired tape is still using space on the DXi-Series library.

Use the Backup Exec media management option to overwrite recyclable media before you overwrite scratch media. This media management option is called *Overwrite recyclable media contained in the targeted media set before overwriting scratch media.* You can find this option under **Configuration and Settings > Backup Exec Settings > Storage**.

Create media sets with append and overwrite protection periods that accommodate your needs. When the COMBINED append and overwrite-protection periods expire, the media are recyclable, and Backup Exec has access to overwritable media. Make sure to follow **ALL 3 STEPS** listed below, to limit a given media set to using the amount of DXi space allocated in a DXi-sizing exercise.

Change media retention settings to use recyclable media before scratch: In the BE Administration Console (the main BE GUI), select **Configuration and Settings > Backup Exec Settings > Storage**.

1. Media overwrite options = Overwrite scratch media before overwriting recyclable media contained in the targeted media set CHANGE TO = Overwrite recyclable media contained in the targeted media set before overwriting scratch media.
2. Change the media set append period to 2 weeks, or to as short a time as is workable, based on your DXi sizing exercise.
3. Change the media set Overwrite-Protection period to 10 weeks, or to as short a time as is workable, based on your DXi sizing exercise.

You should periodically overwrite or re-label expired media. This keeps the media family at a manageable size, so that Backup Exec can rebuild the catalog if necessary. You can use a media rotation strategy so that media is periodically overwritten or select the **Overwrite media** option when you run a full backup.

Remove excess media from a media set and return it to the Scratch pool. If the media set grows and needs more virtual cartridges, it will get them from the scratch pool again, but in the meantime, you should keep Backup Exec in the cycle of re-using its intended media set most efficiently.

Do not use the default overwrite protection period of **infinite** for all media:

- Backup data may quickly consume tape and disk capacity.
- Media does not become recyclable automatically. You must specify when to overwrite each media.

Here is a description of Backup Exec media types, options, and behaviors:

Scratch media: This refers to media that can be overwritten by any backup operation and is in the Scratch Media set. Scratch media will be displayed in blue under the Scratch Media set. It can be new media, blank media, erased media, or media moved from another media set.

When Scratch media is used for a backup operation, Backup Exec automatically moves the media to the User Media set that was targeted during the backup operation. The media color will then change from blue to black, and the media will inherit the overwrite protection period and append periods for that User Media set.

User Media sets: User Media sets contain all the allocated media that are assigned to media sets.

Allocated media: This refers to media that is part of a User Media set before its overwrite protection period expires. The media may also be available for append operations if the append period for the media has not expired. The media will be displayed in black under the User Media set.

Once the overwrite protection period expires, the Allocated media becomes Recyclable media, is displayed in blue, and will remain in the User Media set.

Recyclable media: Allocated media that is part of a User Media set before its overwrite protection period expires. The media is available for overwrite operations or append operations (append operations are only possible if the append period still allows the media to be appended to). The media will be displayed in blue under the User Media set.

Overwrite protection period: The amount of time (specified in hours, days, weeks, or years) to keep a piece of media from being overwritten. Change the overwrite protection period from the default of **Infinite - Don't Allow Overwrite**, to the shortest acceptable period.

Quantum recommends a period that matches the number of weeks specified during your DXi sizing-exercise, MINUS the number of days or weeks specified in the Append Period. For example, if the overwrite protection period is set to 10 weeks and the Append Period is set to 2 weeks, the media will be protected from being overwritten for 12 weeks. After these 12 weeks are over, the media becomes Recyclable and can be overwritten. The overwrite protection period is measured from the time when the last overwrite or append operation ended.

Append Period: The amount of time (specified in hours, days, weeks, or years) that data may be added (appended) to a media. Change the append period from the default of **Infinite - Allow Append**, to the shortest acceptable period; Quantum recommends 2 weeks. This means that the media can be appended to for the next two weeks. After these two weeks are over, the media cannot be appended to. The append period is measured from the time the media was first allocated to the media set or overwritten.

Additional Best Practice Considerations

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

Configuring Backup Exec with DXi NAS

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

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

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

NAS Device Path Considerations

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

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

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

- **Replication traffic** - This segment is used exclusively for replication data movement.
- **Management traffic** - This segment is used exclusively for DXi remote management (Web page access).
- **Data traffic** - This segment is used exclusively for NAS data movement. Each network segment has its own network interface (IP address, network mask, and default gateway). In this way, the segment is separated from other network segment traffic.

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

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

1. Configure the DXi for NAS
2. Configure the Backup Exec NAS Storage Device

Configure the DXi for NAS

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

In the DXi Remote Management Console (the GUI) the **Configuration** page allows you to configure many of the features of the DXi, including storage presentation. The NAS license is preinstalled on the DXi4800 Series and DXi9000 Series.

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

Configure the Backup Exec NAS Storage Device

From the CASO (Central Administration Server Option), you can use the **Configure Storage** function to configure resources for the Backup Exec environment. Although the DXi is presenting its storage capacity as a NAS share, and Backup Exec will be creating a network-based storage resource, you must choose **Disk-Based Storage,** then **Disk Storage** when configuring NAS storage.

When the **"Where do you want to create the disk storage device?"** dialog box appears, you can connect to the DXi NAS share. Enter **<\\DXi FQDN\NAS share name>** as the **Network share:** this will join the Backup Exec media server to the DXi.

Number of Shares Considerations

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

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

Network Share Access Control Considerations

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

Network Considerations

Some network considerations include:

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

Backup Exec Storage Settings and Tuning Considerations

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

- Set the maximum size for backup-to-disk files to an appropriate size. If you create small but numerous files, performance may be slow, since the computer must still process each file. However, if you create large files, file system limitations can cause memory allocation problems or network issues. These issues can be a problem if you store files across a network.
- Specify fewer backup sets in a backup-to-disk file, to allow Backup Exec to reclaim disk space faster. Fewer backup sets may allow the overwrite protection period to expire sooner.
- Enable the **Allocate the maximum size for backup-to-disk files** option, to reduce disk fragmentation. To ensure that backup data fills each backup-to-disk file to capacity, increase the

append period of the media set that you associate with the backup-to-disk files. The backup data's overwrite protection period may also increase because the overwrite protection period starts at the end of the last append job.

- Backup performance may be affected when you enable the **Allocate the maximum size for backup-to-disk files** option. To find what works best for your environment, enable this option for a job. Then, compare the performance with a job that does not allocate the maximum size for backup-to-disk files. Experiment with the options for buffered reads and buffered writes. Enabling these options may increase backup performance.

For performance considerations, if you are using the backup-to-disk feature, make sure that existing images are first erased before overwriting them.

Additional Best Practice Considerations

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

Common Operational Considerations for Backup Exec

Deduplication Data Considerations

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

It is not necessary to use multiplexing with DXi systems. 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 without any time penalty for repositioning. Additionally, multiplexing adds additional header information to the data and reduces the deduplication ratio.

Good Candidates for Data Deduplication

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

Not So Good Candidates for Data Deduplication

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

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

Replication Considerations

For first-time replication setups, it is important to manually replicate the name space once the target system is configured and is online. This facilitates the first replication following the first backup to that share/partition. The replication is only available to NAS shares with deduplication enabled.

The DXi supports 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. For more information, please refer to *Quantum DXi-Series Best Practices for Data Replication*.

Space Reclamation

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

Quantum recommends that you schedule daily reconciliation and reclamation, to manage the available space. The scheduled time should be configured to start the data reclamation process after daily backups are complete. The default schedule is weekly, and the default time for the data reclamation is set to

12:00 AM on Sunday. These parameters are user configurable; you should configure them for your backup window.

Backup Streams Considerations

Keep the following considerations in mind:

- A different storage server should be created and used for each Backup Exec domain (master server plus associated media servers). This segregates data, so a Backup Exec 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 Plug-in Installation Instructions*.

DXi Multiprotocol Guidance - NFS/VTL Scenario

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

Asynchronous mode allows the system to acknowledge receipt of 'stable write' or 'commit' commands without having the data (and related metadata) fully written to disk. This mode allows backups to be completed faster (from the Backup Exec point of view), excepting 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. This could result in slower overall performance.

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

Additional notes:

- All other multi-protocol combinations work well together.
- The recommendations in this section apply to all operating systems and applications.
- Reduced VTL traffic may lessen the frequency of NFS timeouts.

Configuring DXi Backup Specific Path to Tape with CIFS and RAWS

Changes to port assignments may be required to replicate images in Backup Exec from DXi CIFS targets to physical tape via NDMP.

For more information on changing port assignments, see the Veritas article How to change the default port used by the Backup Exec Remote Agent for Windows Servers (RAWS). Another option is to contact Quantum Technical Support to change the DXi's NDMP port to one not used by Backup Exec and the Remote Agent.

Additional Considerations for Heavy Network Traffic or Low-Latency Networks

Adjust TCP Keepalive using the OST plugin

The OST plugin configuration file allows you 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 *OST Plugin Configuration* in your system's Documentation Center or the Client Plugins page for more information.

Adjust TCP Keepalive on Microsoft Servers

The TCP Keepalive parameters can also be changed for the Operating System instead of doing so with the OST plugin. See the Veritas TCP Keepalive Best Practices **and** KeepAliveTime on Microsoft TechNet.

Helpful Resources

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

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

StorageCare Guardian Web Site
http://www.quantum.com/ServiceandSupport/Services/GuardianInformation/index.aspx

Quantum Service Web Site
http://www.quantum.com/ServiceandSupport/Index.aspx

Appendix A

Using Backup Exec OST with Quantum Q-Cloud Storage

Quantum is able to offer secure OST backup and archive to the cloud by integrating Veritas OST with DXi. This allows users to back up directly to the cloud and/or build an archive in the cloud, using Data Lifecycle Management (DLM). 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 are presented with a number of backup options:

- Back up directly to a DXi in the cloud using OST. Data security can be addressed 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, as well as restore. You can then use Veritas Optimized Duplication (Opt Dup) to send a copy to the 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.

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

Architecture

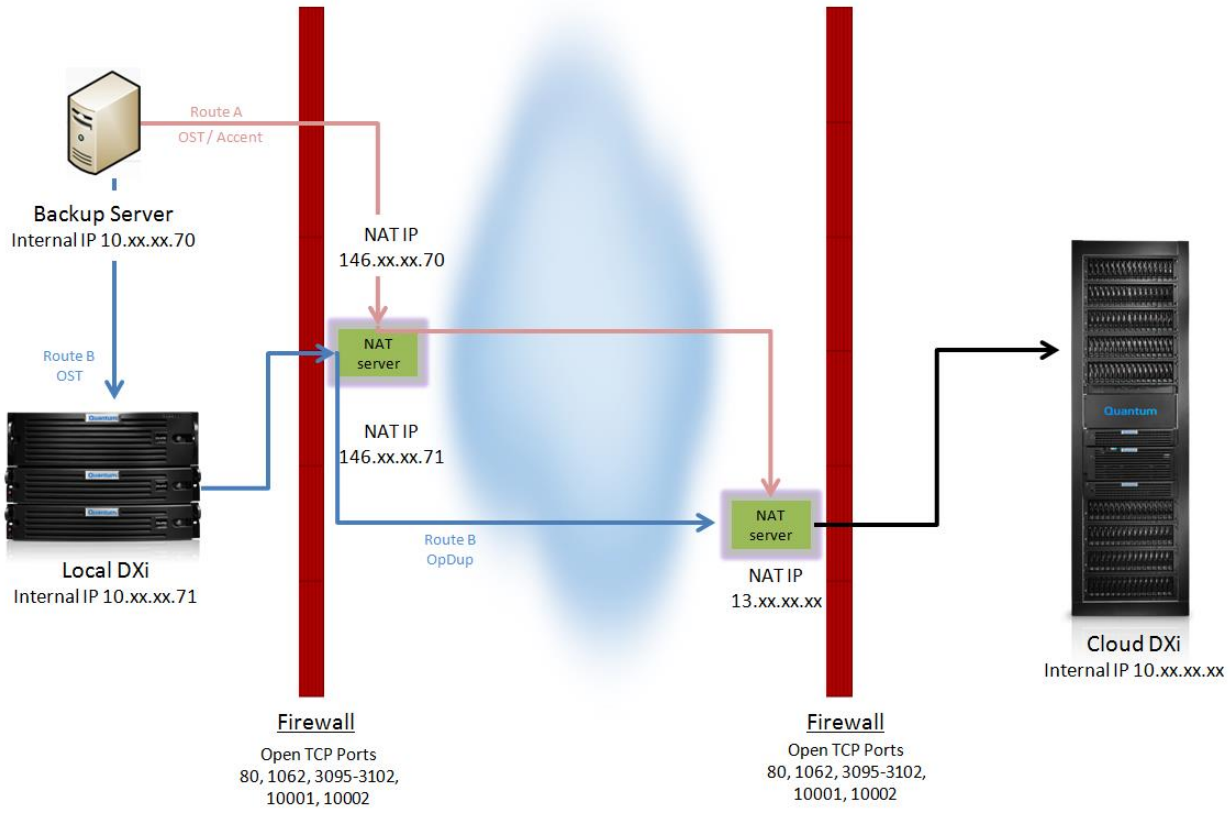

Figure 1 Diagram showing backup options when using OST to store data in the Q-Cloud

In this figure, the **Route A** path shows the requirements for backing up directly to the cloud, using either OST or 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 has a high latency, Accent backup is preferred.
- DXi Accent is a no-cost feature included with every DXi. Accent will deduplicate the backup data on the backup server and send only compressed unique data to the cloud. This can: 1) reduce network load; and 2) reduce the backup window if network loading and/or propagation times are 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.

Route B shows an OST backup that has been directed to a local DXi, and that then leverages the backup application Data Lifecycle Management to automatically send a copy of the 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 above shows the logical path that data must traverse.

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

1. Obtain a NAT address for your backup server (a NAT address is required for the Central Admin Server [CAS] and each managed BE server [MBES] that will be backing up and restoring data to and from Q-cloud).
2. Confirm that the ports in the local firewall are open:
    - For OST: Ports 3095-3102, 10001, 10002
    - For Accent: Ports 80, 1062, 3095-3102, 10001, 10002
3. Obtain the following from Quantum Q-Cloud:
    - The NAT address for the cloud DXi from your cloud service provider. Be sure to add this NAT address as an allowed IP to your firewall rule.
    - The OST storage server and LSU names that you will be writing to.
4. Provide Quantum Q-Cloud your NAT IP address, so it can be added to the Q-Cloud firewall rules.
5. Add the NAT address of each DXi (Source and Target) Using the GUI: **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 of your backup server(s). The backup server(s) must be able to see the remote DXi to manage the entire Opt Dup lifecycle. A NAT address is required for the Central Admin Server (CAS) and all managed BE servers (MBES) 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.
    - You need all of these: TCP ports 80, 1062, 3095-3102, 10001, 10002
4. Obtain the following from Quantum Q-Cloud:
    - The NAT address for the cloud DXi. Be sure and add this NAT address as an allowed IP to your firewall rule.
    - 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 be added to the firewall rules.
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: **Configuration > Replication > Send "Source IP Address" box**.
8. Configure your backup server(s) to use OST to back up to the local LSU.
9. Create the backup policy and the Data Lifecycle Management 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 configuring o*pduptranslate* [select **Configure > OST > Target IP Mapping**].)

    Please note:

    - In a single-tenant DXi hosting configuration, you will most likely be able to do this yourself. In a multi-tenant DXi hosting configuration, the Q-Cloud will have to do this for you.
    - Keep in mind 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 the remote DXi needs to be told 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.

    Command format:

    ```
    bash-3.2$ syscli --add opduptranslate --replicationip <NAT IP> --dataip <local IP>
    ```

    Notes:

    - Other related *syscli* commands are listed below. "Replication IP" is the same as "NAT IP" and "data ip" is the same as "local ip".
    - 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.
    - Verify that you have the correct entry by reviewing the output of the *syscli "list"* option.

    You may find the following information useful.

    bash-3.2$ syscli --help opduptranslate

syscli --add opduptranslate --replicationip <replication_ip> --dataip <data_ip>
Allows to map OST target ip address to a replication ip address.

syscli --del opduptranslate --dataip <data_ip>
Allows to you to delete the mapping of 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 to edit the existing map of OST target ip address to a replication ip address.

syscli --list opduptranslate
Lists all mappings of OST target ip address to a replication ip address

11. TCP “Keep Alive Probes” may be required to prevent firewall ports from closing before operations have completed. If ports close prematurely, this will cause a connection error, resulting in the appearance that media is missing. A workaround for this situation is to restart Backup Exec services.

See the Additional Considerations for Heavy Network Traffic or Low-Latency Networks section above for more information on TCP Keepalive.