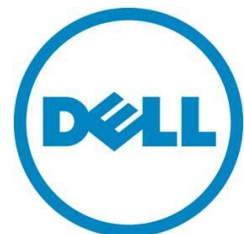


# DELL POWERVAULT NX3500 INTEGRATION WITHIN A MICROSOFT WINDOWS ENVIRONMENT

A Dell Technology White Paper  
Version 1.0



THIS TECHNOLOGY WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2011 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

*Dell*, the *DELL* logo, and the *DELL* badge, *PowerConnect*, and *PowerVault* are trademarks of Dell Inc. *Microsoft*, *Windows*, *Windows Server* and *Hyper-V* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Apr. 2011

---

## Table of Contents

Preface .....	4
Introduction .....	4
Dell PowerVault NX3500 - Unified Storage Solution with DSFS .....	4
System Management .....	5
Authentication .....	6
Kerberos Authentication .....	6
NTLM Authentication .....	7
Installing and Configuring the PowerVault NX3500 in the Microsoft Windows Environment .....	7
Network and Load Balancing Considerations .....	8
ALB vs. LACP .....	9
Data Management .....	10
CIFS Shares .....	11
Snapshots/Shadows Copies .....	13
Quotas .....	13
Data Migration Strategies .....	14
Backup.....	16
Summary .....	16

## Preface

The Dell PowerVault NX3500 NAS storage system delivers highly available, scalable enterprise class file services to Microsoft Windows and Linux clients utilizing the CIFS and NFS protocols. The PowerVault NX3500 integrates seamlessly with Dell PowerVault MD3200i storage system, allowing you to consolidate file and block data to a unified storage system. The PowerVault NX3500 utilizes Dell Scalable File System (DSFS) technology and features online scaling of capacity, snapshots, asynchronous replication, quota, and NDMP. This technical report describes integration aspects of the PowerVault NX3500 system in a Windows environment utilizing the CIFS protocol.

The following topics are presented in this document:

- Integrating the PowerVault NX3500 storage system in Active Directory environments and standalone authentication methods
- Managing the PowerVault NX3500 system using the system GUI and Microsoft administrative tools such as MMC
- PowerVault NX3500 support of common client-side features such as shadows copies
- Easy data management utilizing PowerVault NX3500 features such as NAS File System, snapshots and quota.

The reader is assumed to be knowledgeable about Microsoft Windows servers and workstations products and their features.

## Introduction

Digital content data files and application data are driving storage capacity and performance needs to new heights. The ever-growing need for block and file storage is challenging for IT departments because scaling traditional storage solutions (for instance, by adding file servers or disk arrays) can be costly and cumbersome, adding system management overhead and sometimes underutilized “islands” of data across the organization.

The Dell Scalable File System (DSFS) is a high availability scale-out file-system that supports horizontal scaling in both performance and capacity. DSFS utilizes a SAN-based architecture that leverages the Dell portfolio of block storage solutions. DSFS enables enterprises to scale their storage applications as their business grows.

### Dell PowerVault NX3500 - Unified Storage Solution with DSFS

The PowerVault NX3500 is the first in a series of products based upon Dell Scalable File System that delivers enterprise class file services to Microsoft Windows and Linux clients. It works with PowerVault MD32x0i and MD36x0i storage arrays to help provide affordable unified storage with iSCSI, CIFS and NFS access to block and file data.

You can use the PowerVault NX3500 to consolidate user data, as well as other file and block applications, into a single, easy-to-manage unified



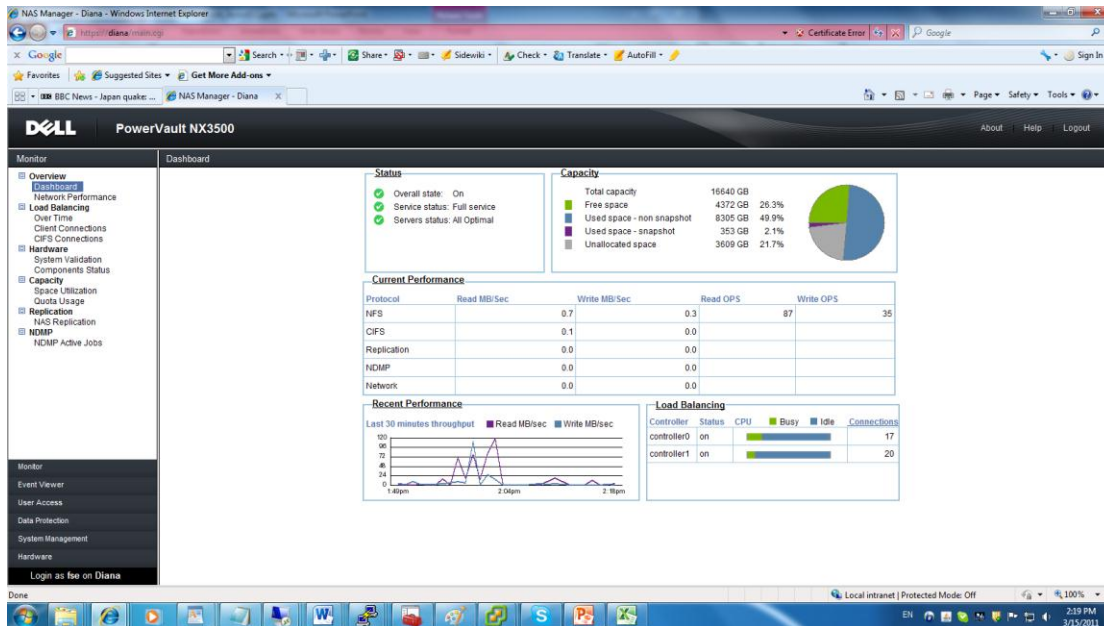
storage system with best-of-breed data management and scaling capabilities. The PowerVault NX3500's scale-up architecture delivers a flexible, load-balanced pool of high performance storage, making it easy to grow capacity up while avoiding the scalability constraints and challenges of managing separate block and file systems. With its dual active-active file controllers and backup power supply, the PowerVault NX3500 gives you data protection and excellent performance with no single point of failure. Find out more about the PowerVault NX3500 at Dell.com/NX3500.

### System Management

A Windows environment administrator can manage the PowerVaultNX3500 storage system using the system's web GUI or CLI interface or Microsoft Computer Management (MMC). Day-to-day operations can be done via either the MMC or the system GUI/CLI. Certain operations unique to the PowerVault NX3500 storage system must be done via the system GUI or CLI; for instance, the creation of the NAS File System and CIFS shares, snapshot configuration and initial configuration.

### Using PowerVault NX3500 GUI AND CLI

The PowerVault NX3500 graphical interface and the CLI each provide management for all supported NAS (file) tasks. The PowerVault NX3500 consists of two redundant active/active storage controllers, coupled during the installation process to become system nodes. The system GUI provides the administrator with a system dashboard, reporting tools, performance trends analysis, and management of system configuration and hardware.



PowerVault NX3500 NAS Manager Interface

## **Authentication**

The PowerVault NX3500 can operate in Windows Workgroup mode or Windows Domain mode. Workgroup authentication utilizes the system's internal directory of users/groups and does not rely on a domain controller. In domain mode the system is part of the Active Directory and domain controllers provide user/groups directory and authentication services. In domain authentication, the client negotiates the highest possible security level when establishing a connection with the PowerVault NX3500. There are two primary levels of security:

- Basic security, based on NTLM (NT LAN Manager challenge/response)
- Extended security, based on Kerberos implementation

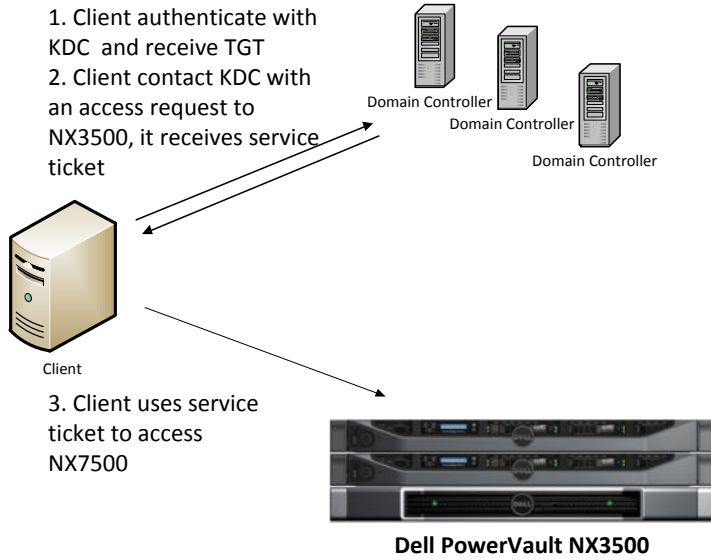
Windows computers that are not part of an Active Directory domain use only NTLM-based authentication. By default, Windows clients (XP/2000 and above) that are part of an Active Directory domain will try to use Kerberos authentication first and then NTLM authentication.

## **Kerberos Authentication**

In an Active Directory environment, the Kerberos Key Distribution Center (KDC) service provides authentication service (AS) and ticket granting service (TGS). The Kerberos service runs on Windows domain controllers. A Windows client that wants to establish a session with another system such as the PowerVault NX3500 system, contacts the KDC directly to obtain session credentials, which are presented to the client in the form of a Kerberos ticket.

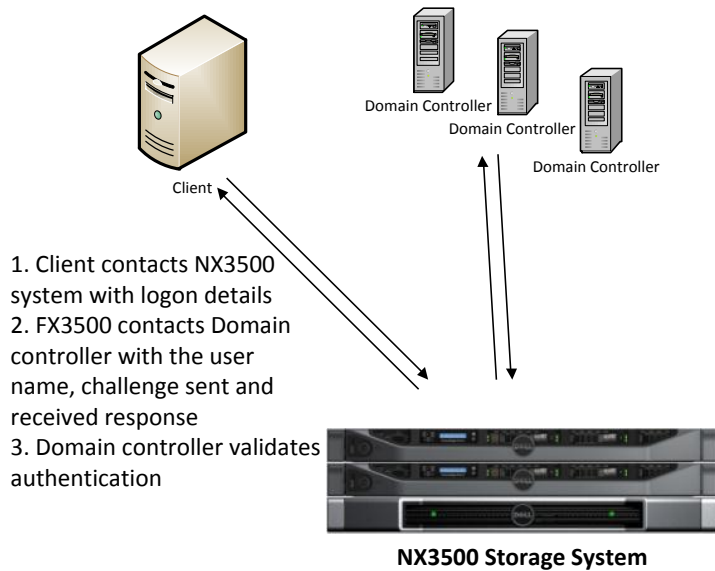
The process has three main phases:

1. The client authenticates with the KDC and receives a Ticket to Get Tickets (TGT) to be used in future request from KDC.
2. The client issues a request to access the PowerVault NX3500 to the KDC (using its TGT), and receives a service ticket.
3. The client establishes a session with the PowerVault NX3500 using the service ticket; the PowerVault NX3500 can decrypt the information using its long term key.



### NTLM Authentication

Using NTLM, the PowerVault NX3500 storage system contacts the Domain controller to verify user-supplied credentials. The Domain controller will encrypt the user password with a challenge and compare the result with a response sent from the client. If these are identical the authentication is successful.



### Installing and Configuring the PowerVault NX3500 in the Microsoft Windows Environment

Requirements and configuration actions in the Active Directory environment

Commonly in a Windows environment, the storage system is configured as a domain member using Active Directory for authentication of users and data permissions management.

When installing the PowerVault NX3500 in an Active Directory environment the following requirements must be met:

### **Name Resolution**

The NAS Service queries Domain Name Service (DNS) servers to locate domain controllers. The common scenario is for the DNS service provided by Windows servers to be integrated in Active Directory. The administrator should configure at least one DNS server (preferably more) in order for the system to be able to locate the domain controllers and other services in the domain.

Clients access the NAS service via one or more NAS service IP addresses. It is recommended to create a host (“A” address) DNS record for the NAS virtual IP.

### **NTP Configuration**

NTP (Network Time Protocol) servers are used to synchronize network server and clients’ time. Windows clients synchronize their clock with the domain controller’s clock. As Kerberos authentication protocol requires that time setting on the PowerVault NX3500 and domain controller should be nearly the same, the administrator should verify the time setting of the NAS service. A best practice is to configure the PowerVault NX3500 using one or more time servers to synchronize its clock.

### **Joining a Domain**

The PowerVault NX3500 can become part of Active Directory domain and provide file services to the domain users and applications. The domain will provide NAS authentication services and directory access to enable various file permission schemes using the Active Directory’s users and group’s database.

In order to join the system to a domain you should have access to a domain account that has rights to add a computer to the domain.

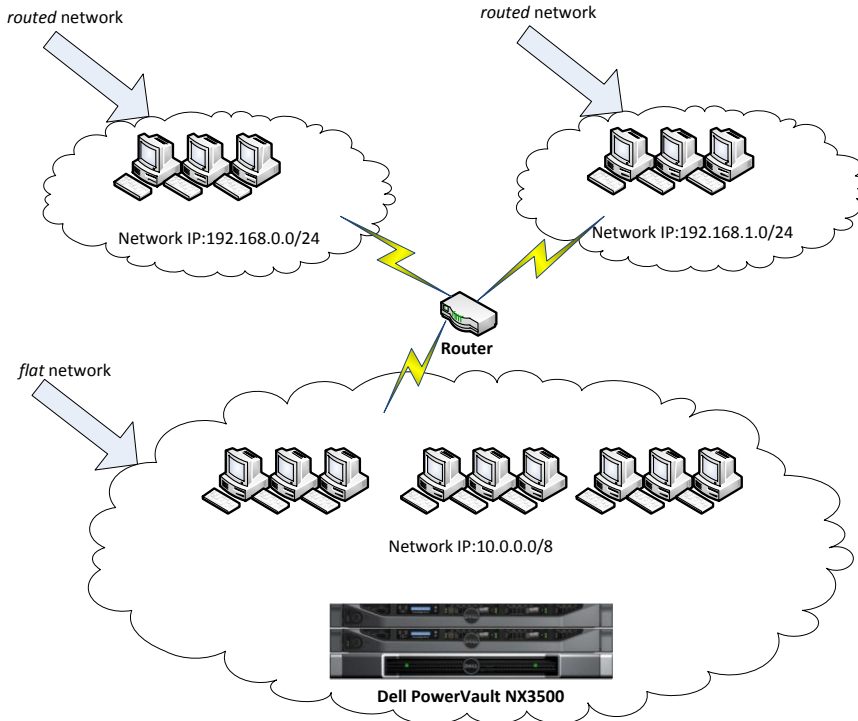
### **Network and Load Balancing Considerations**

The PowerVault NX3500 system utilizes a network load balancing mechanism between the PowerVault NX3500 nodes. Traffic is balanced between nodes in the network layer. In case of a node failure, network traffic is automatically redirected to an active NAS node in the system.

Network servers and workstations may access the system in a variety of network topologies. From a performance perspective, it is important to define the subnets that the network servers and workstations belong to (there may be more than one) relative to the PowerVault NX3500 client network subnet.



When a client accesses the PowerVault NX3500 system from within the same network subnet as the system, it is considered a *flat network*; in this case it is sufficient to define one NAS service IP address. When there are clients that access the PowerVault NX3500 from additional subnets, network traffic will be routed to and from the system via a router or Layer 3 switches; this is considered *routed network*. In routed network configuration it is recommended that administrators define multiple virtual IP addresses in a single subnet and create multiple A records (that point to the virtual IP addresses) for the PowerVault NX3500 under the same DNS name.



Network topology diagram

### ALB vs. LACP

As network traffic is balanced between the NAS nodes, traffic is also balanced between any node client network NICs to maximize efficiency. Supported client network NICs teaming modes are ALB and LACP (also known as dynamic 802.3ad). ALB mode relies on layer 2 traffic manipulation dynamically to balance network traffic between the NICs. LACP protocol requires network switch port configuration yet allows the use of fewer NAS Service IPs in a routed network scenario.

The main considerations are:

Node NICs load balancing method	Network Switch Configuration	Recommended # of NAS Service IPs*
---------------------------------	------------------------------	-----------------------------------

ALB	Not required	Number of nodes X number of client network NICs per node
LACP	Required	Number of nodes

\*The *minimum* number of NAS Service IPs recommended to configure in a routed network layout.

### Data Management

The PowerVault NX3500 enables simple, flexible and efficient data management. This section will discuss space planning, space provisioning, data protection and data access.

#### NAS volumes

The PowerVault NX3500 gives you the flexibility to divide its single file system into multiple NAS volumes, so that you can distribute data and access to meet various needs. A NAS volume is seen by the client as a separate file system. It can grow or shrink instantly according to needs, thus permitting flexible management. Each NAS volume presents CIFS shares to the network.

NAS volumes are also an administrative boundary. You can apply data management and protection policies per individual NAS volume and allocate data based on the policy required for that data type.

The following policies are applied per NAS volume:

- Snapshots policies -for example, when you have two types of data files that require different snapshot policies you may choose to create two NAS volumes and apply the relevant snapshot policy to each NAS volume.
- Quota policy - quota usage is calculated per NAS volume space consumption.
- Security style - Security style is relevant in a heterogeneous environment when CIFS and NFS clients must access the same NAS volume. Security style setting governs which protocol is used to manage file permissions on the NAS volume. In a homogenous environment (e.g., Windows only accessing the NAS file system), the default Mixed security style is recommended.

The PowerVault NX3500 system enables the administrator to instantly create NAS volumes as needed and apply the relevant policies. An example scenario would be an where the administrator needs to provision storage space to users' Home Directories or to an Application Data and Scratch area for an applications. Each of the requirements has different needs in terms of total space, snapshots policies and quota.

The following table illustrates NAS volume usage scenarios according the various data files classification:

NAS volume	Size	Snapshots Policy	Quota Policy	Security Style
------------	------	------------------	--------------	----------------

Home-Directories	2 TB	Scheduled - Daily	Enforced	NTFS
Application Data	1TB	Scheduled - hourly	None	NTFS
Temp Application Data	500GB	None	None	NTFS

### CIFS Shares

A Microsoft Windows administrator can create and manage a share by using the PowerVault NX3500 GUI/CLI. Shares are created per NAS volume.

When creating a share via the PowerVault NX3500 GUI/CLI, administrator can choose to allow guest access to the CIFS share. Configuring and managing share level permissions and Access Control Lists (ACLs) is done via the Microsoft Shared folders MMC snap in.

Once shares are configured, Windows users can access the NAS volumes using the CIFS protocol.

Note that although the PowerVault NX3500 system can have multiple NAS volumes with multiple shares on each volume, from a client perspective accessing all shares on all NAS volumes is done in the same manner.

Example:

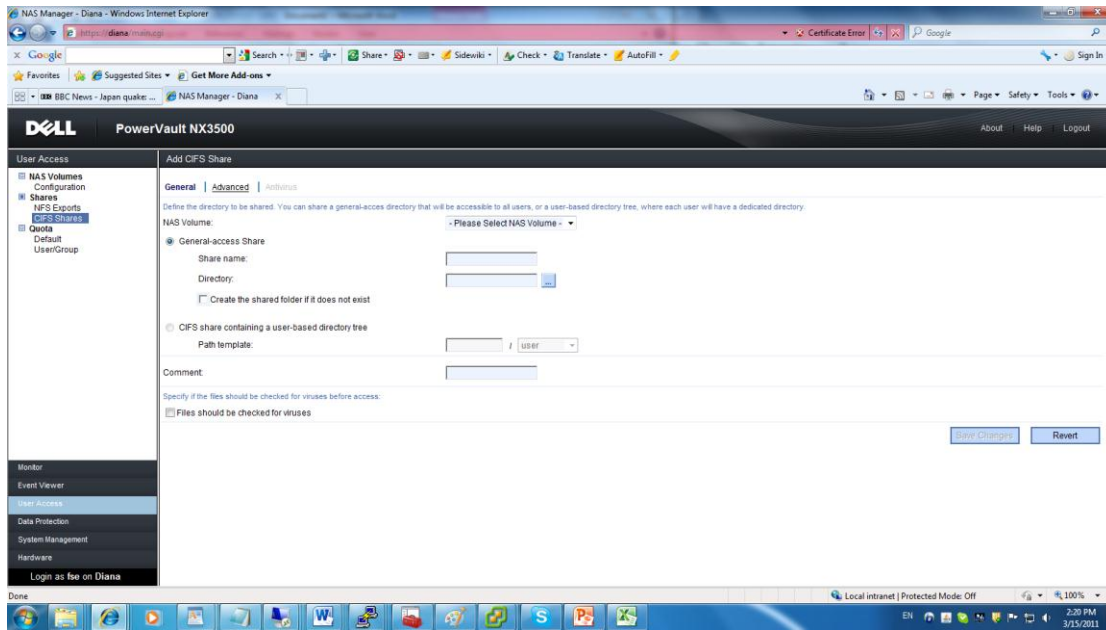
Accessing “data” share on “Application Data” NAS volume would be:

\\NX3500\data

Accessing “home” share on “Home-Directories” NAS volume would be:

\\NX3500\home

# DELL WHITE PAPER: POWERVAULT NX3500 INTEGRATION WITHIN A MICROSOFT WINDOWS ENVIRONMENT



NX3500 GUI CIFS share creation screen

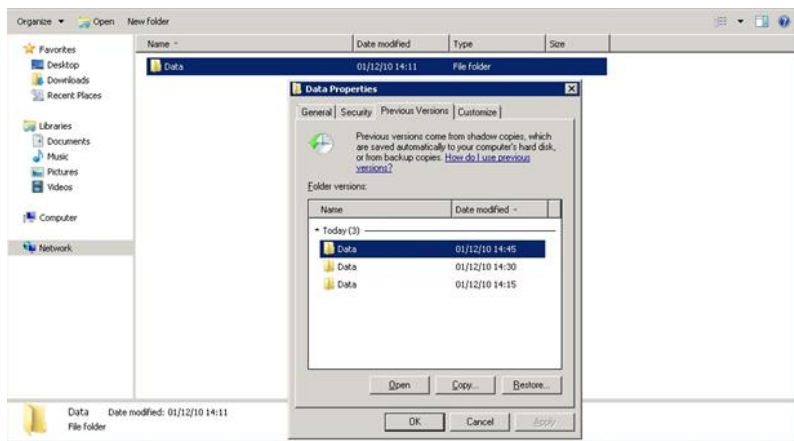
## Snapshots/Shadow Copies

Snapshots technology is widely used in storage environments to enable the system administrator and the user to instantly restore previous versions of data. Snapshots technology is an integral part of the PowerVault NX3500 system.

To allow flexibility and space management, Snapshots policies are applied at a NAS volume level. The administrator can schedule automatic periodic snapshots (as frequently as every five minutes) and initiate manual snapshots at any time.

When data files are updated in the timeframe between snapshots, space is consumed from the NAS volume to store snapshots data. The administrator can monitor space consumption of snapshots via the system GUI.

Snapshots technology lets users restore files from snapshots using the Microsoft volumes Shadows Copy Service client application. Users can restore a previous version of their files independently using the standard Windows GUI. The administrator of the PowerVault NX3500 system can roll back the entire NAS volume to a previous taken snapshot using the system GUI.



Accessing shadow copies of a shared folder

## Quotas

The PowerVault NX3500 system supports quota on space usage per NAS file system. The Administrator can define space usage quota per user, group, or any user in a group. A default quota for a NAS File System can also be configured and applied for all users or groups. A soft quota setting alerts the administrator when file usage exceeds a predefined percentage of a quota policy. Once a user or a group exceeds a quota limit,

writing to the specific NAS file system is not permitted. NAS file system space taken by snapshots is not included in quota calculations.

### **Data Migration Strategies**

Data migration is the process of making a copy of the data and moving it from one system to another, preferably without disturbing the business activity. Consolidating data from several file servers, or data islands, to the PowerVault NX3500 storage system can optimize utilization of storage resources, reduce the storage management overhead and allow for simple and easy future growth.

The optimal data migration process varies according to the migrated data classification, size and location. The main things to consider when planning a data migration include:

1. Data migration scope:
  - a. Sources of the dataset
    - i. Data location (servers, tapes, other)
    - ii. Network bandwidth between source and PowerVault NX3500 storage system)
  - b. Classification of data (e.g. home folders, application data, scratch area etc.)
  - c. Dataset size (per data classification)
  - d. Data usage and update frequency, i.e. how frequently data changes are applied to the dataset (hourly/daily/weekly changes).
  - e. Current snapshots and quota policy, and what is the planned policy using the PowerVault NX3500
2. What will be the ACL permissions structure on the PowerVault NX3500 storage system. You may decide to rebuild the ACL structure or migrate the data along with its ACL (the data migration utility should support this)?
3. How long will it take to migrate the data?
4. Which data migration utility is going to be employed (for example Microsoft Robocopy utility)?
5. Current and future network shares configuration
6. Verification of migrated data integrity - How do we validate the post-migration environment and confirm that all expectations have been met?
7. Setting user expectations and educate them on how to use the PowerVault NX3500 features (such as Shadows copies)

An example of data migration scope analysis table:

<b>Data Classification</b>	<b>Data Source Location</b>	<b>Dataset Size</b>	<b>Data Update Frequency</b>	<b>NX3500 NAS volume Destination</b>	<b>Network Bandwidth</b>	<b>Dataset Migrate Operation Time Estimate</b>
Home Directories A	FileServer01	800GB	Daily	Home-Directories	1Gb	111 hours
Home Directories B	FileServer02	450GB	Daily	Home-Directories	1Gb	62.5 hours
Application Data	FileServer02	500GB	Hourly	Application Data	10Gb	69.4 hours

Data may be migrated in several ways:

1. All at once
2. By data classification (home directories, application data, etc.)
3. In phases (copy the dataset in the background, then copy dataset incremental changes from source to PowerVault NX3500)

Migration plan complexity varies between migration projects, environments and organizations. Many vendors offer applications/utilities to support data migration processes (such as Microsoft’s Robocopy utility); your IT department has a many options to choose from. There is no one right way.

## Backup

Traditionally, network-based backup relies on backup agents that are installed on servers accessing the NAS; data is sent from the servers to the backup server via the network. This approach creates additional network traffic as data travels once from the NAS to the client over the network and then again from the client to the backup server.

Network Data Management Protocol (NDMP) is an open protocol for backing up NAS devices. It allows for direct communication between the backup software, the NAS device and the target destination for the backup. Data can be directed over the network directly to the destination device in an efficient manner. The PowerVault NX3500 NAS system supports NDMP.

Dell has certified the following backup applications for use with the PowerVault NX3500:

Vendor	Application suite	Version
Symantec	NetBackup	7.0
Symantec	Backup Exec	2010R3
CommVault	Simpana	9

## Summary

This technical report provided an overview of the Dell PowerVault NX3500 storage system’s integration in the Microsoft Windows environment. The flexibility of PowerVault NX3500 NAS volumes, along with its data protection and management features, enable you to consolidate your organization’s data islands and reduce management overhead.