# Dell PowerVault Network Attached Storage (NAS) Systems Running Windows Storage Server 2012 R2

## Administrator's Guide

# Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

**WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**



2014 - 02

Rev. A00

# Contents


1 Overview....7
iSCSI Deployment....7
Dell Supported Hardware And Software....8
Preinstalled Roles And Services Configurations On Your System....8
Roles and Role Services....8
Features....9
Contacting Dell....10
Related Documentation....10
Locating Your System Service Tag....11
Downloading Drivers and Firmware For Your System....11
Documentation Feedback....11

2 Initial Configuration Of Your NAS System....13
Server Manager Roles, Role Services and Features....13
Starting And Exiting Server Manager....14
Installing Or Uninstalling Server Manager Roles, Role Services And Features....14
Accessing Administrative Tools For Your NAS System....14
Accessing Computer Management....14
System Tools....14
Storage....15
Services and Applications....15
Work Folders....15
Installing the Work Folders....16
Creating A Sync Share For Work Folders....16
Creating A New DFS Namespace....16
Creating A New DFS Replication Group....17
Adding DFS Namespaces To Display....17
Adding Replication Groups To Display....17
File Server Resource Manager (FSRM)....17
Multipath I/O (MPIO)....18
Managing Devices On MPIO....18

3 Managing Your NAS System....19
Dell OpenManage Server Administrator....19
Remote Desktop For Administration....19
Activating Remote Desktop Connection....20
Creating And Saving A Remote Desktop Connection....20
Reinstalling The NAS Operating System....21

4 Using Your NAS System....23
Creating A Server Message Block Share....23
Modifying Message Block Shares....23
NFS Share....24
Windows 2003 Domain Controller As Identity Mapping Source....24
Windows 2008 Domain Controller As Identity Mapping Source....24
Windows 2012 Domain Controller As Identity Mapping Source....25
User Name Mapping Server As Identity Mapping Source....25
Active Directory Lightweight Directory Services As Identity Mapping Source....26
Configuring AD LDS For Services For NFS....26
Installing The AD LDS Server Role....27
Creating A New AD LDS Instance....27
Extending The AD LDS Schema To Support NFS User Mapping....28
Setting A Default Instance Name For AD LDS Instances....29
Updating The Active Directory Schema....29
Adding User And Group Account Maps From A UNIX-Based System To A Windows-Based System....30
Connecting To The Distinguished Name Or Naming Context....30
Adding User Account Maps....31
Adding Group Account Maps....31
Authorizing Appropriate Access To The ADS LDS Namespace Object....32
Configuring The Mapping Source....32
Debug Notes For NFS Account Mapping Problems....33
Restarting The Server For NFS....33
Creating The NFS Share....33
Creating Quotas And File Screens Using File Server Resource Manager....34
Creating A New Volume....34
Managing A Volume....34
Extending A Volume....35
Extending A Basic Volume Using The Windows Interface....35
Extending A Basic Volume Using CLI....35
Shrinking A Volume....35
Additional Considerations When Shrinking A Volume....36
Deleting A Volume....36
Additional Information When Deleting A Volume....36
Data Deduplication....36
Enabling And Configuring Shadow Copies Of Shared Folders....37
Performing Backup Of Your Server Using Windows Server Backup Feature....38
Choosing Volumes To Backup....38
Choosing A Storage Location....39
NIC Teaming....39

Configuring NIC Teaming On A Server.....40

1

# Overview

Windows Storage Server 2012 R2 is an advanced storage and file-serving solution that provides high-level performance and reliability. Dell Network Attached Storage (NAS) systems running Windows Storage Server 2012 R2 operating system are extremely cost effective and help in providing shared storage solutions with storage capabilities.

Following are the new features and functionalities:

- **Data Deduplication** — works at the volume level and stores more data in less physical space. Data Deduplication identifies duplicate data-chunks and maintains a single copy of each chunk. Redundant copies of data chunk are replaced by a reference to a single copy of the chunk.
- **Storage Spaces** — provides storage management functionality, including storage pools.
- **File Server Resource Manager (FSRM)** and **File Server Volume Shadow Copy Service (VSS) Agent Service** — enables you to create volume shadow copies of applications that store data files on the file server.
- Enhanced storage protocols:
  - **Server Message Block 3.0 (SMB)** — provides file services for network shares, improved SMB bandwidth limits management, and improved rebalancing of Scale-Out file server.
  - **Network File System (NFSv4)** — shares files with UNIX systems that use NFS protocol.
  - **iSCSI Software Target** — provides storage over TCP/IP network, enhanced virtual disk storage capacity, and converts Windows server into a storage device which provides shared block storage.
- **Resilient File System (ReFS)** — improves data integrity, availability, and scalability.

NOTE: Currently, Windows Storage Server 2012 R2, Windows Storage Server 2012 and Windows Server 2008 R2 operating systems are available.

## iSCSI Deployment

In Windows Storage Server 2012 R2, the iSCSI Software Target is integrated with the **Server Manager** . To access iSCSI, in **Server Manager**, double-click **File and Storage Services**.

iSCSI software target feature offers:

- Diskless network boot capabilities
- Continuous availability configurations
- Cost savings on operating system storage
- Controlled operating system images that are more secure and straight forward to manage
- Fast recovery
- Data corruption protection
- Heterogeneous storage to support non-Windows iSCSI initiators
- Converts a system running Windows Server into a network-accessible block storage device

NOTE: To configure the iSCSI Target Server for PowerVault storage systems, see **technet.microsoft.com/en-us/library/hh848268**.

# Dell Supported Hardware And Software

The following Dell NAS systems run Microsoft Windows Storage Server 2012 R2 operating system:

- Dell PowerVault NX3300
- Dell PowerVault NX3200
- Dell PowerVault NX400

Dell PowerVault NX3300, NX3200, and NX400 systems support the following Windows Storage Server 2012 R2 editions:

- Microsoft Windows Storage Server 2012 R2, Workgroup Edition, x64
- Microsoft Windows Storage Server 2012 R2, Standard Edition, x64

# Preinstalled Roles And Services Configurations On Your System

Based on your organization requirements, server roles, role services, and features are preinstalled and configured on your system.

## Roles and Role Services

Preinstalled roles and role services are:

| | |
|---|---|
| File and Storage Services | Manages file servers and storage. |
| File and iSCSI Services | Manages file servers and storage, replicate and cache files, reduces disk space utilization, and shares files using NFS protocol. |
| File Server | Manages shared folders and enables user to access files on the system from the network. |
| Data Deduplication | Works at the volume level and stores mode data in less physical space. Data Deduplication identifies duplicate data-chunks and maintains a single copy of each chunk. A redundant copy replaces the reference to a single copy. |
| DFS Namespaces | Groups shared folders located on different servers into one or more logically structured namespace. |
| DFS Replication | Synchronizes folders on multiple servers across Local or Wide Area Network (WAN) connections. |
| File Server Resource Manager (FSRM) | Manages files and folders on a file server by scheduling tasks and storage reports, classifying files, configuring quotas and defining file screening policies. |

| | |
|---|---|
| File Server VSS Agent Service | Performs volume shadow copies of applications that store data files on file server. |
| iSCSI Target Server | Provides services and management to iSCSI targets. |
| iSCSI Target Storage Provider (VDS and VSS hardware providers) | Enables applications on a server that is connected to an iSCSI target to perform volume shadow copies of data on iSCSI virtual disks. |
| Server for NFS | Shares files with UNIX-based systems and other systems that use the NFS protocol. |
| Work Folders | Facilitates users to access their work files from various devices and keeps them synchronised whether users access their files from inside the network or from across the internet. |
| Storage Services | Provides storage management functions. |

## Features

Preinstalled features are:

| | |
|---|---|
| .NET Framework 3.5 (includes .NET 2.0 and 3.0) and 4.5 Features | Uses Windows Communication Foundation (WCF) activation service to invoke the applications remotely on the network by using HTTP or TCP protocols. |
| Failover Clustering | Multiple servers work together to provide high availability. |
| Multipath I/O | Provides support for using multiple data paths to a storage device on Windows. |
| Remote Server Administration Tools (RSAT) | Manages roles and features remotely. |
| SMB 1.0/CIFS File Sharing Support | Supports file sharing protocol and computer browser protocol.<br>**NOTE:** SMB 1.0 is an optional feature for Windows Storage Server 2012 R2. |
| User Interfaces and Infrastructure | Provides the available user experience and infrastructure options. |

| | |
|---|---|
| Windows PowerShell (includes Windows PowerShell 4.0, 2.0 Engine, and PowerShell ISE) | Automates local and remote administration through hundreds of built-in commands. |
| WoW64 Support | Supports running 32–bit applications on Server Core installation. |

# Contacting Dell

NOTE: Dell provides several online and telephone-based support and service options. If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog. Availability varies by country and product, and some services may not be available in your area.

To contact Dell for sales, technical support, or customer-service issues:

1. Visit **dell.com/support**.
2. Select your country from the drop-down menu on the top left corner of the page.
3. For customized support:
   a) Enter your system service tag in the **Enter your Service Tag** field.
   b) Click **Submit**.
   The support page that lists the various support categories is displayed.
4. For general support:
   a) Select your product category.
   b) Select your product segment.
   c) Select your product.
   The support page that lists the various support categories is displayed.

# Related Documentation

**WARNING: See the safety and regulatory information that shipped with your system. Warranty information may be included within this document or as a separate document.**

NOTE: For all PowerVault documentation, go to **dell.com/powervaultmanuals** and enter the system Service Tag to get your system documentation.

NOTE: For all Dell OpenManage documents, including the Dell OpenManage Server Administrator User Guide, go to **dell.com/openmanagemanuals**.

NOTE: For all operating system documents, go to **dell.com/operatingsystemmanuals** .

Your product documentation includes:

- The *Getting Started Guide* — provides an overview of system features, setting up your system, and technical specifications. This document is also shipped with your system.
- The *Owner's Manual* — provides information about system features and describes how to troubleshoot the system and install or replace system components.

- The *Administrator's Guide* — provides information about configuring and managing the system.
- The *Troubleshooting Guide* — provides information about troubleshooting the software and the system.
- The *Dell OpenManage Server Administrator User's Guide* — provides information about using the OpenManage Server Administrator to manage your PowerVault NAS system.

NOTE: Always check for updates on **dell.com/support/manuals** and read the updates first because they often supersede information in other documents.

# Locating Your System Service Tag

Your system is identified by a unique Express Service Code and Service Tag number. The Express Service Code and Service Tag are found on the front of the system by pulling out the information tag. Alternatively, the information may be on a sticker on the chassis of the system. This information is used by Dell to route support calls to the appropriate personnel.

# Downloading Drivers and Firmware For Your System

When upgrading your system, it is recommended that you download and install the latest BIOS, drivers, and systems management firmware on your system from **dell.com/support**.

# Documentation Feedback

If you have feedback for this document, write to **documentation_feedback@dell.com**. Alternatively, you can click on the **Feedback** link in any of the Dell documentation pages, fill up the form, and click **Submit** to send your feedback.

# 2
# Initial Configuration Of Your NAS System

Initial configuration of your NAS system includes:

- Cabling the system or solution using iSCSI
- Powering-up and connecting your NAS solution
- System configuration using **Server Manager**

To complete initial configuration of your NAS system:

1. When you start your NAS system running Windows Storage Server 2012 R2 for the first time, press **OK** on the **Default Password** screen.

   NOTE: Before changing the password, ensure that you change the system language according to your preference.

2. To change the default language, navigate to **C:\Dell_OEM\MUI**, and run the appropriate language batch file. Follow the on-screen prompts to install your preferred language.

   NOTE: Your system is configured with default user name `administrator` and password `Stor@ge!`.

3. To change your administrator password, press <Ctrl><Alt><Del> and click **Change a Password**.

   **Server Manager** starts automatically when you log on the first time.

4. In **Server Manager**, click **Configure this local server** to:

   – Change the computer name
   – Specify the domain
   – Check for latest Windows updates
   – Specify the time zone
   – Configure Remote Desktop

   NOTE: Click on the left bottom corner of the screen to locate the **Start** screen to navigate to a particular application.

## Server Manager Roles, Role Services and Features

**Server Manager** is a management console that manages remote and local servers from a desktop without physical access or Remote Desktop protocol (RDP) connections. Windows Storage Server 2012 R2 **Server Manager** is completely redesigned with Metro User Interface (MUI) style displaying applications in tiled interface and colors.

Server Manager allows you to:

- Add remote servers to a pool of servers.
- Create or edit a group of servers (for a specific purpose or geographic location).
- Install or uninstall roles, role services and features and view or make changes to local or remote servers.

- Get status of your servers and roles remotely.
- Determine server status, identify critical events, analyze and troubleshoot configuration issues or failures.
- Customize the events, performance data, services, and Best Practices Analyzer (BPA) results that are displayed on the **Server Manager** dashboard.
- Perform tasks on multiple servers at one time.

### Starting And Exiting Server Manager

**Server Manager** starts by default when a administrators logs on to the system. If you close **Server Manager**, you can restart in one of the following ways:

- On the Windows Start screen, click **Server Manager** tile.
- On the Windows taskbar, click **Server Manager** icon.
- In Windows PowerShell environment, at the command prompt, type `servermanager` (case insensitive).

To exit the **Server Manager**, close the **Server Manager** window.

## Installing Or Uninstalling Server Manager Roles, Role Services And Features

In Windows Storage Server 2012 R2, the **Server Manager** console and **Windows PowerShell** cmdlets for **Server Manager** enable you to install roles, role services, and features. You can install multiple roles and features by using **Add Roles and Features Wizard** or **Windows PowerShell** session.

NOTE: To install or uninstall roles, roles services, and features using the **Add Roles And Features Wizard** and **Windows PowerShell** cmdlets, see: **technet.microsoft.com/en-us/library/hh831809.aspx#BKMK_installarfw**.

## Accessing Administrative Tools For Your NAS System

Many Microsoft Management Console (MMC) snap-ins are listed in the **Administrative Tools** folder.

To access Administrative Tools folder follow any one of the steps below:

- In the **Server Manager** menu bar, click **Tools** to access the Administrative Tools.
- Press the Windows logo key. On the start menu, click **Administrative Tools** tile.
- From the start menu, open **Control Panel**, click **System and Security** → **Administrative Tools**.

## Accessing Computer Management

To access **Computer Management** tools, the **Server Manager** menu bar, click **Computer Management**. The **Computer Management** window is displayed which has all the tools segregated into three groups. These tools are described below.

### System Tools

| | |
|---|---|
| Task Scheduler | Is used to create new tasks and manage basic tasks that the system performs automatically at specific times. Tasks created are stored in Task scheduler library. It also tracks the **Task Status** and **Active Tasks** that are not expired. |

| | |
|---|---|
| **Event Viewer** | Is used to create or import custom views and view events that have occurred in a particular node or log. It also displays **Summary of Administrative log**, **Recently Viewed Nodes**, and **Log Summary**. |
| **Shared Folders** | Is used to centrally manage file shares on a system. Shared Folders enable you to create file shares and set permissions, in addition to viewing and managing open files and users. |
| **Local Users and Groups** | Is used to create and manage users and groups that are stored locally on a computer. |
| **Performance** | Is used to monitor performance in real time or through a log. Configuration data is collected and events traced to analyze results and view reports. |
| **Device Manager** | Manages the technologies that support the installation of hardware and the device driver software that enables the hardware to communicate with the Windows operating system. |

### Storage

| | |
|---|---|
| **Windows Server Backup** | Is a feature that uses command-line tools and Windows PowerShell cmdlets for your day-to-day backup and recovery needs. The data backup can de done locally and online. To run **Windows Server Backup**, you must install the **Windows Server Backup** feature. |
| **Disk Management** | Is a system utility for managing hard disks and the volumes or partitions that they contain. Management allows you to create and attach virtual hard disks, initialize disks, create volumes, and format volumes with the FAT, FAT32, or NTFS file systems. It also helps perform most disk-related tasks without restarting the system or interrupting users. Most configuration changes take effect immediately. |

### Services and Applications

| | |
|---|---|
| **Routing and Remote Access Service** | Technology combines three networking services into one unified server role, Direct Access, Routing, and Remote Access. |
| **Services** | Is used to manage services such as file serving, event logging and so on that are running on local or remote computers. You can also manage services using the `sc config` command. |

# Work Folders

Work Folders is a role service for file servers using Windows Storage Server 2012 R2.

Work Folders allow users to store and access files on their personal systems or work devices from any location, referred to as bring-your-own-device (BYOD). Work Folders can be deployed with existing deployments of Folder Redirection, Offline Files, and home folders. User files are stored in a folder on the server called a *sync share*. For more information on Work Folders, see: **technet.microsoft.com/en-us/library/dn265974.aspx**.

## Installing the Work Folders

To install the Work Folders:.

1. In the **Server Manager** menu bar, click **Manage** → **Add Roles and Features**.
   The **Add Roles and Features Wizard** is displayed.
2. Click **Next**.

   NOTE: In the **Before you begin** window, verify the destination server, network environment for the role and feature that you want to install.
3. In the **Select installation type** window, select **Role-based or feature-based installation** to install all parts of roles or features, or select **Remote Desktop Services installation** to install either a virtual machine-based desktop infrastructure or a session-based desktop infrastructure for Remote Desktop Services and click **Next**.
4. In the **Select destination server** window, select a server from the server pool or select an offline Virtual Hard disk (VHD) on which Windows Storage Server 2012 R2 is already installed, and click **Next**.
5. In the **Select Server Roles** window, select the **File and Storage Services** → **File and iSCSI Services** → **Work Folders** .
   The **Add features that are required for Work Folders** pop-up window is displayed.
6. If additional features are required for installing Work Folders, click **Add Features** to continue, and click **Next**.
7. In the **Work Folders** window, review the summary information, and click **Next**.
8. In the **Confirm Installation Selections** window, read any informational messages, and click **Install**.
9. Review the **Installation Results** window to verify if the installation has succeeded.
10. Click **Close** to exit the wizard.
    The **Work Folders** role is created in the **Sever Manager** → **Files and Storage Services** folder.

## Creating A Sync Share For Work Folders

To create a sync share for Work folders:

1. In **Server Manager**, go to **File and Storage Services** → **Work Folders** .
   A page with **Work Folders**, **Users**, **Volume** and **Quota** panes is displayed.
2. To create a new sync share, in the **Work Folders** section, perform any one of the steps below:
   - Click **To create a sync share for Work Folders, start the New Sync Share Wizard** link
   - Select **New Sync Share** from the **Tasks** drop down list.

   The **New Sync Share Wizard** window is displayed.
3. Follow the wizard instructions and create a new sync share for Work folders. For information on *Deploying Work Folders*, see: **technet.microsoft.com/en-us/library/dn528861.aspx#step3**.

# Creating A New DFS Namespace

To create a new DFS namespace:

1. In the **Server Manager** menu bar, click **Tools** → **DFS Management** .
   The **DFS Management** window is displayed.
2. Under **Actions**, click **New Namespace**.
   The **New Namespace Wizard** is displayed.

3. Follow the instructions in the **New Namespace Wizard** and complete the wizard.

   NOTE: A namespace server cannot be created if the server is offline.

# Creating A New DFS Replication Group

To create a new DFS replication group:

1. In the **Server Manager** menu bar, click **Tools** → **DFS Management** .
   The **DFS Management** window is displayed.
2. Under **Actions**, click **New Replication Group**.
   The **New Replication Group Wizard** is displayed.
3. Follow the instructions in the **New Replication Group Wizard** and complete the wizard.

# Adding DFS Namespaces To Display

To add DFS namespaces to display:

1. In the **Server Manager** menu bar, click **Tools** → **DFS Management** .
   The **DFS Management** window is displayed.
2. Under **Actions**, click **Add Namespaces to Display**.
   The **Add Namespaces to Display** window is displayed.
3. Under **Scope**, click **Browse** and locate the parent domain.
4. Click **Show Namespaces** and select the namespace that is on the parent domain. Click **OK**.
   The namespace should be displayed in the form of `\\parentdomain\rootname` in the DFS management.

# Adding Replication Groups To Display

To add replication groups to display:

1. In the **Server Manager** menu bar, click **Tools** → **DFS Management** .
   The **DFS Management** window is displayed.
2. Under **Actions**, click **Add Replication Groups to Display**.
   The **Add Replication Groups to Display** window is displayed.
3. Click **Browse** and locate the parent domain.
4. Click **Show Replication Groups** and select the replication groups that is on the parent domain. Click **OK**.
   The replication groups should be displayed in the form of `\\parentdomain\rootname` in the DFS management.

# File Server Resource Manager (FSRM)

FSRM is a collection of tools for Windows Storage Server 2012 R2 that allows administrators to understand, control, and manage the quantity and type of data that is stored on their system. By using FSRM, administrators can place quotas on folders and volumes, actively screen files, and generate comprehensive storage reports. This set of advanced instruments not only helps the administrator

efficiently monitor existing storage resources, but it also aids in the planning and implementation of future policy changes. FSRM tasks include:

- Quota Management
- File Screening Management
- Storage Report Management
- Classification Management

# Multipath I/O (MPIO)

Microsoft Multipath I/O (MPIO) is a framework provided by Microsoft, which enables storage providers to develop multipath solutions that contain the hardware-specific information. It is required to optimize connectivity with their storage arrays. These modules are called **Device-Specific Modules (DSMs)**. MPIO is protocol-independent and can be used with Fibre Channel, Internet SCSI (iSCSI), and Serial Attached SCSI (SAS) interfaces in Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

MPIO provides the following features:

- High application availability through failover clustering
- High availability for storage arrays
- SAS disk compatibility
- The ability to perform MPIO tasks through Windows PowerShell cmdlets

NOTE: To work with the DSM provided by Microsoft, storage must be SCSI Primary Commands-3 (SPC-3) compliant.

## Managing Devices On MPIO

To manage devices on MPIO:

1. In the **Server Manager** menu bar, click **Tools** → **MPIO** .

   The **MPIO Properties** window is displayed.
2. On the **MPIO Devices** tab, click **Add** and enter the **Device hardware ID** of the device you want to add MPIO support for and click **OK**.
3. The device hardware ID's are seen in the **Discover Multi-Paths** tab.

   NOTE: A device hardware ID is a combination of vendor's name and a product string that matches the device ID that is maintained by MPIO in its supported device list. The vendor and product IDs are provided by the storage provider, and they are specific to each type of hardware.
4. On the **DSM Install** tab, enter the **DSM INF** file and click **Install or Uninstall** to install/Uninstall a DSM.
5. On the **Configuration Snapshot** tab, capture the snapshot of the current MPIO configuration on the system, specify a filename for the information to be captured and click **Capture**.

3

# Managing Your NAS System

The following management tools are pre-installed on your system:

- Dell OpenManage Server Administrator
- Remote Desktop for Administration

## Dell OpenManage Server Administrator

Dell OpenManage Server Administrator provides a comprehensive, one-to-one system management solution in two ways:

- **Integrated web browser-based GUI**—through the Server Administrator home page
- **Command line interface (CLI)**—through the operating system

Server Administrator allows you to manage NAS systems on a network locally and remotely.

Server Administrator provides information about:

- Systems that are operating properly and systems that have problems
- Systems that require updates
- Systems that require remote recovery operations

NOTE: For more information on Dell OpenManage Server Administrator, see the *Dell OpenManage Server Administrator User's Guide* for the relevant version at **dell.com/openmanagemanuals**.

## Remote Desktop For Administration

You can remotely administer a storage appliance by using Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode). You can use it to administer a system from virtually any system on your network. Based on the terminal services technology, remote desktop for administration is specifically designed for server management.

NOTE: Remote desktop for administration does not require the purchase of special licenses for client computers that access the server. It is not necessary to install Terminal Server Licensing when using remote desktop for administration.

You can use remote desktop for administration to log on to the server remotely using any of the tools below:

- Remote Desktop Connection
- Remote Web Administration
- Microsoft Windows Server Remote Administration Applet

NOTE: For secure connections, it is recommended to obtain a certificate for the server and use HTTPS connections to connect to Windows Storage Server.

## Activating Remote Desktop Connection

To activate Remote Desktop connection on Windows Storage Server 2012 R2:

1. In the **Server Manager**, click **Local Server**.
   Alternatively, you can right-click my computer, select **Properties** → **Remote Settings** .
   The **Properties** window is displayed.
2. In the **Properties** window, click **Enabled** hyperlink for the **Remote Desktop**.
   In Windows Storage Server 2012 R2, remote management is enabled by default.
   The **System Properties** window is displayed.
3. In the **Remote** tab, from the **Remote Desktop** section, select **Allow remote connections to this computer**.

   NOTE: The remote desktops with an authenticated network level are allowed to connect to the system.
4. Click **Select Users** button.
   The **Remote Desktop Users** window is displayed
5. Click **Add** or **Remove** button to give access to users and click **OK**.
6. Click **Apply** and **OK**.

## Creating And Saving A Remote Desktop Connection

Administrators can access systems running Windows Storage Server 2012 R2 from a Windows-based system by using Remote Desktop Connection. To facilitate access, administrators can create a remote desktop connection and save it to the desktop of the system that is used for administration.

To create and save a remote desktop connection to Windows Storage Server 2012 R2:

NOTE: For more information about configuring your remote desktop connection, click **Help** in the **Remote Desktop Connection** window.

1. Click **Start** → **Run**.
   The **Run** dialog box is displayed.
2. In the **Run** dialog box, type `MSTSC` and click **OK**.
   The **Remote Desktop Connection** window is displayed.
3. In the **Remote Desktop Connection** window, type the *computer name or IP address* of the storage appliance, and click **Options**.
   The **Connection Settings** window is displayed.
4. In the **Remote Desktop Connection** window, click **Save As** in the **Connection Settings** box.
   The **Save As** window is displayed.
5. In **File name**, type a name for the connection, and leave the extension as **.rdp**.
6. In the **Save-in** drop-down menu, select **Desktop** and click **Save**.
   For more information about configuring your remote desktop connection, click **Help** in the **Remote Desktop Connection** window.

# Reinstalling The NAS Operating System

**CAUTION: You must backup the internal disk drives on your system before reinstalling or upgrading the NAS Operating System.**

1. Backup any internal disk drives or data on external storage arrays.
2. If applicable, connect the external USB DVD drive to your NAS system.
3. Insert your *Dell PowerVault NAS Operating System* resource media into your NAS system.
4. Power down your NAS system.
5. Restart your NAS system and ensure that your NAS system boots from the resource media.

   The operating system reinstallation begins and proceeds without any user intervention if no errors are encountered. This process takes around 30 to 45 minutes to complete. Errors encountered are flagged on the front panel LCD of your device. To resolve issues, see the *Dell PowerVault Network Attached Storage (NAS) Systems Troubleshooting Guide* at **dell.com/support/manuals**.
6. After the operating system is reinstalled, follow the initial configuration steps listed in Initial Configuration Of Your NAS System topic.

# 4

# Using Your NAS System

## Creating A Server Message Block Share

Windows Storage Server 2012 R2 introduces Server Message Block (SMB) 3.0 protocol. It is a network file sharing protocol that allows applications to read and write to files and requests services from server programs in a network. SMB file shares can also store user database files and dynamically migrates VMs or databases.

To create an SMB share using Server Manager:

1. In **Server Manager**, go to **File and Storage Services** → **Shares** .
   A page with **Shares**, **Volume** and **Quota** panes is displayed.
2. To create a new share, in the **Shares** section, perform any one of the steps below:
   - Click **To create a file share, start the New Share Wizard** link
   - Select **New Share** from the **Tasks** drop down list.

   The **New Share Wizard** page is displayed.
3. In the **Select the Profile for this share** window, select the **File Share profile (SMB Share – Quick, Advanced or Applications)** based on requirements and click **Next**.
4. In the **Select the server and path for this share** window, select the **Server name** and **Share location** for this new share and click **Next**.
   The share location can be selected either by **Volume** or by **Typing a custom path**.
5. In the **Specify share name** window, enter the **Share name** and **Share description**, and click **Next**.
   If a share folder does not exist, the local path to share creates a folder automatically.
6. In the **Configure share settings** window, select the required settings, and click **Next**.
7. In the **Specify permissions to control access** window, set the folder permissions in various combinations as required and click **Next**.
8. In the **Confirm selections** window, confirm the settings and click **Create**.
   The **View results** window displays a successful creation of share.
9. Click **Close** to exit the wizard.
   The newly-created SMB shared folder can be accessed from a Windows-based client.

## Modifying Message Block Shares

To modify the properties of an existing share:

1. In **Server Manager**, go to **File and Storage Services** → **Shares** .
2. Select the share from the **Shares** section.
3. Right-click and select **Properties**.
   The <*share name*> **Properties** windows is displayed.

4. You can select different tabs such as **General**, **Permissions**, **Settings**, and **Management Properties** to change the properties of the share.

# NFS Share

Network File System (NFS) protocol provides access control (for UNIX-based file systems) and is implemented by granting permissions to specific client systems and groups, using network names.

Before creating the NFS share, the administrator must configure Identity Mapping. The identity mapping source can be any one of the following:

- Microsoft Active Directory domain name server (Microsoft Windows Server 2003 domain controller, Microsoft Windows Server 2008 domain controller, or Microsoft Windows Server 2012 domain controller)
- User Name Mapping (UNM) server
- Active Directory Lightweight Directory Services (AD LDS)

For more information on NFS share, see topic Creating The NFS Share.

# Windows 2003 Domain Controller As Identity Mapping Source

1. Go to the **Windows 2003 Domain Controller** and install Identity Management for UNIX.

   NOTE: You may need the Windows 2003 SP 2 resource media.

   If required, insert the Windows 2003 SP 2 resource media.
2. Click **Add or Remove Programs** → **Add or Remove Windows Components** → **Active Directory Services**.
3. Click **Details**.
4. Select **Identity Management for UNIX** and click **Next** to complete the installation.

   NOTE: Restart your system after the installation is complete.

# Windows 2008 Domain Controller As Identity Mapping Source

To install and configure **Identity Management for UNIX**:

1. Go to the **Windows 2008 Domain Controller** and install **Identity Management for UNIX** using **Server Manager** → **Roles** → **Add Role Services**.

   NOTE: To activate this service, restart Windows 2008 Domain Controller.
2. Go to **NFS client**, note down the user name, group name, UID, and GID details.
3. Go to the **Domain Controller**.
4. Open **Active Directory Users and Computers**, and create the UNIX user name and group.
5. Add the user to the group created in the step 4.
6. Select the newly-created user, go to **Properties** → **UNIX Attributes** . Modify the UID, GID, shell, home directory, and domain details (captured earlier from the NFS client).
7. Select the newly-created group, check the GID (ensure it matches the UNIX GID), modify the UNIX properties, add the members and users that you added in the step 6 and click **Apply**.

8. Go to **PowerVault NAS Windows Storage Server 2012 (NFS) Server**.
9. Click **Start** → **Administrative Tools** → **Services for Network File System**.
10. Select **Services for NFS**, right-click **Properties** → **Active Directory domain name** as your Identity mapping source, type the Windows 2008 domain name and click **Apply**.

# Windows 2012 Domain Controller As Identity Mapping Source

To install and configure **Identity Management for UNIX** using **Dism.exe**:

1. On the domain controller, right-click **Windows PowerShell** and click **Run as Administrator**.
2. To install the administration tools for Identity Management for UNIX, type the following command and press enter: **Dism.exe /online /enable-feature /featurename:adminui /all**

   NOTE: A system restart is required after Identity Management for UNIX is installed. The **/quiet** parameter restarts the system automatically after the installation is finished.
3. Go to **NFS client**, note down the user name, group name, UID, and GID details.
4. Go to the **Domain Controller**.
5. Open **Active Directory Users and Computers**, and create the UNIX user name and group.
6. Add the user to the group created in the step 4.
7. Select the newly-created user, go to **Properties** → **UNIX Attributes** . Modify the UID, GID, shell, home directory, and domain details (captured earlier from the NFS client).
8. Select the newly-created group, check the GID (ensure it matches the UNIX GID), modify the UNIX properties, add the members and users that you added in the step 6 and click **Apply**.
9. Go to **PowerVault NAS Windows Storage Server 2012 R2 (NFS) Server**.
10. Click **Start** → **Administrative Tools** → **Services for Network File System**.
11. Select **Services for NFS**, right-click **Properties** → **Active Directory domain name** as your Identity mapping source, type the Windows 2012 domain name and click **Apply**.

# User Name Mapping Server As Identity Mapping Source

To install and configure User Name Mapping:

1. On your **NAS** system, in the **Server Manager** menu bar, click **Tools** → **Services for Network File System (NFS)** .

   The **Services for Network file System** window is displayed.
2. Right-click **Services for NFS** and select **Properties**.

   The **Services for NFS Properties** window is displayed.
3. Select **User Name Mapping** as the Identity mapping source and type the Hostname of your User Name Mapping server.
4. Go to the **UNM** server, copy the password, and group the files you collected in the previous step to a local disk.
5. Go to **Add or Remove Programs** → **Add Windows Components** → **Select Other Network File and Print Services**.
6. Click **Details**.
7. Select **Microsoft Services for NFS**, click **Details** and select **User Name Mapping**.

8. Click **Next** and complete the installation.

   NOTE: Restart your system after the installation is complete.
9. Go to the **NFS client**, obtain the **/etc/passwd** and **/etc/group files** and copy them to a USB key.
10. Go to the UNM server and copy the UNIX files from the USB key to a local hard disk.
11. Open **Microsoft Services for NFS**.
12. Select **User Name Mapping** and right-click **Properties**.
13. Go to **UNIX User Source** tab and select the **Use Password and Group Files** option.
14. Click the **Browse** button, select the password and group files that you had copied in the previous step.
15. Go to the **Simple Mapping** tab, select the **Use simple maps** option, and click **Apply**.
16. Select **User Maps**, and right-click **Create Map**.
17. Click **List Windows Users** and **List UNIX Users** options.
18. Map the users (select one user at a time) and add to the list. Repeat this step for other listed users.
19. Open **Group Maps → Create Maps**.
20. List **Windows & UNIX groups**, map them and add to the list.
21. Open the **.maphosts** file **(C:\Windows\msnfs** and **C:\Windows\amd64\cmpnents\r2** and look for the **.maphosts** file) and add the NFS server details (IP 4 address or host name, if DNS exists) and save the file.

# Active Directory Lightweight Directory Services As Identity Mapping Source

Active Directory Lightweight Directory Services (AD LDS) is used for identity mapping on systems that run Windows Storage Server 2012 R2 in an environment where no Active Directory exists to support user mapping.

Before you start AD LDS mapping:

- Determine the users and groups on the UNIX-based system that must be mapped to users and groups on the Windows-based system.
- Determine the UID and GID for each UNIX user, and the GID for each UNIX group.
- Create a user or group on the Windows-based computer for each UNIX user or group to be mapped.

NOTE: Each UID and GID requires a unique mapping. You cannot use one-to-many or many-to-one mappings.

# Configuring AD LDS For Services For NFS

To configure AD LDS for services for NFS:

1. Install the AD LDS server role. For more information, see Installing The AD LDS Server Role
2. Create a new AD LDS instance.
3. Extend the AD LDS schema to support NFS user mapping.
4. Set a default instance name for AD LDS instances.
5. Update the active directory schema.
6. Add user and group account maps from a UNIX-based computer to a Windows-based computer.
7. Authorize appropriate access to the ADS LDS namespace object.
8. Configure the mapping source.

# Installing The AD LDS Server Role

To install the AD LDS Server Role:

1. In the **Server Manager** menu bar, click **Manage → Add Roles and Features**.
   The **Add Roles and Features Wizard** is displayed.
2. Click **Next**.
   NOTE: In the **Before you begin** window, verify the destination server, network environment for the role and feature that you want to install.
3. In the **Select installation type** window, select **Role-based or feature-based installation** to install all parts of roles or features, or select **Remote Desktop Services installation** to install either a virtual machine-based desktop infrastructure or a session-based desktop infrastructure for Remote Desktop Services and click **Next**.
4. In the **Select destination server** window, select a server from the server pool or select an offline Virtual Hard disk (VHD) on which Windows Storage Server 2012 R2 is already installed, and click **Next**.
5. In the **Select Server Roles** window, select the **Active Directory Lightweight Directory Services**.
   The **Add features that are required for AD LDS?** pop-up window is displayed.
6. If additional features are required for installing AD LDS, click **Add Features** to continue, and click **Next**.
7. In the **Active Directory Lightweight Services** window, review the summary information, and click **Next**.
8. In the **Confirm Installation Selections** window, read any informational messages, and click **Install**.
9. Review the **Installation Results** window to verify if the installation has succeeded.
10. Click **Close** to exit the wizard.
    The **Active Directory Lightweight Directory Services** role is created in the **Sever Manager** dashboard page.

# Creating A New AD LDS Instance

To create a new AD LDS Instance:

1. On the **Server Manager** menu bar, click **Tools → Active Directory Lightweight Directory Services Setup Wizard** .
   The **Active Directory Lightweight Directory Services Setup Wizard** is displayed.
2. Click **Next**.
3. In the **Setup Options** window, select **A unique instance**, and click **Next**.
4. In the **Instance Name** window, enter the **Instance name**, and click **Next**.
   NOTE: For this example, you can use *nfsadldsinstance* as the instance name.
5. In the **Ports** window, enter the **LDAP port number**, **SSL port number**, and click **Next**.
   NOTE: The default LDAP port number is `389` and the default SSL port number is `636`.
6. In the **Application Directory Partition** window, select the **Yes, create an application directory** partition.

7. In the **Partition name** text box, use the following format to type a partition name that does not already exist in this instance: `CN=<Partition>, DC=<Computer name>`

   NOTE: By convention, this string is based on the fully qualified domain name. For example, if the instance name is *nfsadldsinstance* and the server name is *server1*, the partition name would be represented as follows: `CN=nfsadldsinstance, DC=server1`.

8. After typing the partition name, click **Next**.
9. In the **File Locations** window, type or browse to the locations where you want to store files associated with AD LDS in the **Data files** and the **Data recovery files** field, and click **Next**.
10. In the **Service Account Selection** window, select **Network service account**, and click **Next**.

    NOTE: If the system is not a member of a domain, the following message is displayed: `AD LDS instance cannot replicate data with AD LDS instances on other computers while using this service account.`

11. Click **Yes** to continue or **No** to cancel.
12. In the **AD LDS Administrators** window, select the currently logged on user: <*Username*> option, and click **Next**.
13. In the **Importing LDIF Files** window, select the **.LDF** file names that you want to import, and click **Next**.

    NOTE: MS-InetOrgPerson.LDF and MS-User.LDF are required.

14. In the **Ready to Install** window, under **Selections**, review the listed selections, and click **Next**.

    The AD LDS service starts installing.

15. Click **Finish** to exit the wizard.

    NOTE: After the AD LDS installation, if any problems have occurred during setup they are listed in the completion window.

16. To verify if an active AD LDS instance exists, go to **Control Panel** → **Programs** → **Programs and Features**. All the AD LDS instances created are listed here.

# Extending The AD LDS Schema To Support NFS User Mapping

To extend the AD LDS schema to support NFS mapping:

1. Press the Windows logo key on the keyboard.
2. Type `CMD`.

   **Command Prompt** application is displayed.

3. Right-click **Command Prompt** and select **Run as administrator** to open an elevated command prompt.
4. Navigate to the C:\WINDOWS\ADAM directory, and run the command:

   ```
   ldifde -i -u -f MS-AdamSchemaW2K8.LDF -s localhost:389 -j . -c
   "cn=Configuration,dc=X" #configurationNamingContext
   ```

   This command imports the MS-AdamSchemaW2K8.LDF file.

   NOTE: This example uses the default LDAP port number `389` for the AD LDS instance. The strings `cn=Configuration,dc=X` and `#configurationNamingContext` must not be modified.

# Setting A Default Instance Name For AD LDS Instances

To set a default Instance Name for AD LDS Instance:

1. In the **Server Manager** menu bar, click **Tools** → **ADSI Edit (Active Directory Service Interface)**.
   The **ADSI Edit** console is displayed.
2. In the console, right-click **ADSI Edit** and click **Connect to**.
   Alternatively, in the ADSI Edit console, you can navigate to **Actions** → **More Actions** → **Connect to**
   The **Connection Settings** dialog box is displayed.
   a. Under **Connection Point**, select the **Select a well known Naming Context** option, and select **Configuration** from the drop-down menu.
   b. Under **Computer**, select the **Select or type a domain or server option**, and type the following in the text box: `localhost:389`

   NOTE: This example uses the default LDAP port number 389. If you specified a different port number in the **Active Directory Lightweight Directory Services Setup Wizard**, use that value instead.
3. Click **OK**.
   **ADSI Edit** refreshes to display the new connection.
4. In the resulting tree, under the **Configuration** node, click **CN=Configuration**, click **CN=Sites**, click **CN=Default-First-Site-Name**, click **CN=Servers**, click **CN=server1$ nfsadldsinstance**, and click **CN=NTDS Settings**.
5. Right-click **CN=NTDS Settings**, and click **Properties**.
6. In the **Properties** dialog box, click **msDs-DefaultNamingContext**, and click **Edit**.
7. In the **String Attribute Editor**, in the **Value** text box, type `CN=nfsadldsinstance, dc=server1`, and click **OK**.
8. Close **ADSI Edit**.

# Updating The Active Directory Schema

To update the active directory schema:

1. Press the Windows logo key on the keyboard.
2. Type `CMD`.
   **Command Prompt** application is displayed.
3. Right-click **Command Prompt**, and select **Run as administrator** to open an elevated command prompt.
4. Navigate to the C:\WINDOWS\ADAM directory, and run the command:
   ```
   regsvr32 schmmgmt.dll
   ```
   This command enables the Active Directory plug-in, schmmgmt.dll.
5. Click **Start** → **Run**, and type MMC to open the Microsoft Management Console (MMC).
6. On the **File** menu, click **Add/Remove** Snap-in.
7. In the **Add or Remove Snap-ins** dialog box, click **Active Directory Schema**.
8. Click **Add**, and click **OK**.
9. Right-click the **Active Directory Schema** node, and click **Change Active Directory Domain Controller** to connect to the AD LDS instance that was previously created.

10. In the **Change Directory Server** dialog box, under **Change to**, click **This Domain Controller or AD LDS instance**.
11. In the **Name** column, replace the placeholder text <*Type a Directory Server name[:port] here*> with the server and port number (for example, localhost:389).
12. Click **OK**.
13. Add the **gidNumber** and **uidNumber** attributes to the user class as follows:
    a. Expand the **Active Directory Schema** node, expand the **Classes** node, right-click **User**, and click **Properties**.
    b. In the **Properties** dialog box, click the **Attributes** tab.
    c. Click **Add** to open the **Select Schema Object** dialog box.
    d. Click **gidNumber**, and click **OK**.
    e. Click **Add** to open the **Select Schema Object** dialog box.
    f. Click **uidNumber**, and click **OK**.
    g. Click **OK**.
14. Add the **gidNumber** attribute to the group class as follows:
    a. Expand the **Active Directory Schema** node and the **Classes** node.
    b. Right-click **Group**, and click **Properties**.
    c. In the group **Properties** dialog box, click the **Attributes** tab.
    d. Click **Add** to open the **Select Schema Object** dialog box.
    e. Click **gidNumber**, and click **OK**.
    f. Click **OK**.
15. Close the MMC, and click **Save**.

# Adding User And Group Account Maps From A UNIX-Based System To A Windows-Based System

The following steps are included in this procedure:

- Connecting to the Distinguished Name or Naming Context. Follow Connecting To The Distinguished Name Or Naming Context procedure to set a default naming context and create a container to hold your account mappings from UNIX to the Windows operating system.
- Adding User Account Maps. Follow Adding User Account Maps procedure to create a user-class object in the CN=Users container, to map the **uidNumber**, **gidNumber**, and **sAMAccountName** attributes.
- Adding Group Account Maps. Follow Adding Group Account Maps procedure to create a group-class object in the CN=Users container, to map the **gidNumber** and **sAMAccountName** attributes.

# Connecting To The Distinguished Name Or Naming Context

To connect to the distinguished naming context:

1. In the **Server Manager** menu bar, click **Tools** → **ADSI Edit** .
   The **ADSI Edit** console is displayed.
2. In the console, right-click **ADSI Edit** and click **Connect to**.
   Alternatively, in the ADSI Edit console, you can navigate to **Actions** → **More Actions** → **Connect to**.
   The **Connection Settings** dialog box is displayed.

3. Under **Connection Point**, select the **Select a well known Naming Context** option.

   By default, **Default naming context** option is selected from the drop-down menu.

4. Under **Computer**, select the **Select or type a domain or server** option, and enter the server name and port number in the text box, separated by a colon (for example, `localhost:389`).

5. Click **OK**.

   **ADSI Edit** refreshes to display the new connection.

6. In the resulting tree, under the **Default naming context** node, right-click the partition name, point to **New**, and click **Object**.

   NOTE: For this example, under the Default naming context `[localhost:389]`, select the following properties: `CN=nfsadldsinstance, DC=server1`.

7. In the **Create Object** dialog box, select the **Container** class, and click **Next**.

8. In the **Value** text box, type `Users`, and click **Next**.

   This value specifies the name of the container object that is used to hold your user account mappings.

9. Click **Finish**.

# Adding User Account Maps

To add user account maps:

1. In **ADSI Edit**, expand the **Default naming context** node, and expand the partition name.
2. Right-click **CN=Users**, point to **New**, and click **Object**.
3. In the **Create Object** dialog box, select the **User** class, and click **Next**.
4. In the **Value** text box, type the user's name, and click **Next**.

   NOTE: The user's name is not associated with the Windows or UNIX user, and can be a random entry.

5. Click the **More Attributes** button to edit the uidNumber, gidNumber, and sAMAccountName attributes of this user account.

   NOTE: The **uidNumber** and **gidNumber** represent the UID and GID of the UNIX user who is being mapped, and **sAMAccountName** must match the name of a local Windows user on the computer that is running Server for NFS. If, after selecting the More Attributes button, the **uidNumber** and **gidNumber** do not appear, close and open the **ADSI Edit** MMC.

6. Click **OK**.

# Adding Group Account Maps

To add group account maps:

1. In **ADSI Edit**, expand the **Default naming context** node, and expand the partition name.
2. Right-click **CN=Users**, point to **New**, and click **Object**.
3. In the **Create Object** dialog box, select the **Group** class, and click **Next**.

   NOTE: Ensure that the group object's name matches the name of the group account for which group account mapping is desired.

4. Set the **gidNumber** and **sAMAccountName** attributes for the new group object.

   NOTE: The **gidNumber** is the GID of the UNIX group that is being mapped, and **sAMAccountName** must match the name of a local group on the Windows-based computer that is running Server for NFS. If, after selecting the **More Attributes** button, the **uidNumber** and **gidNumber** do not appear, close and open the **ADSI Edit** MMC.

5. Click **OK**, and click **Finish** to exit the wizard.

# Authorizing Appropriate Access To The ADS LDS Namespace Object

To connect to the Configuration partition:

1. Press the Windows logo key on the keyboard.
2. Type `CMD`.

   **Command Prompt** application is displayed.
3. Right-click **Command Prompt**, and select **Run as administrator** to open an elevated command prompt.
4. Navigate to the C:\WINDOWS\ADAM directory, and run the dsacls command to grant the **Everyone** group read access to the mapping data store as follows:

   ```
   dsacls "\\server1:389\CN=nfsadldsinstance,dc=server1" /G everyone:GR /I:T
   ```
5. Optionally, if you are setting up a shared AD LDS store to allow multiple NFS servers to query the account mapping database, add the mapping data store to the ACL to allow Read permissions for the Anonymous Logon account as follows:

   ```
   dsacls "\\server1:389\CN=nfsadldsinstance,dc=server1" /G "anonymous
   logon":GR /I:T
   ```

   NOTE: You can skip this step if there is no shared access between computers to the mapping data store.

# Configuring The Mapping Source

To configure the mapping source:

1. Press the Windows logo key on the keyboard.
2. Type `CMD`.

   **Command Prompt** application is displayed.
3. Right-click **Command Prompt**, and select **Run as administrator** to open an elevated command prompt.
4. Run the following command, where <*Computer*>is the name of the computer where the AD LDS instance was created,<*Port*> is the port that the AD LDS instance uses:

   ```
   nfsadmin mapping config adlookup=yes addomain=<Computer>:<Port>
   ```

   NOTE: For this example, use the following:

   ```
   nfsadmin mapping config adlookup=yes addomain=server1:389
   ```
5. Test the setup by accessing the NFS resources and verifying that the user and group account mappings work as expected.

# Debug Notes For NFS Account Mapping Problems

Server for NFS can be made to log account mapping failures to the Windows Event Log service by setting the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\nfsserver\Parameters
\VerboseMappingFailureLogging INVALID USE OF SYMBOLS REG_DWORD = 1
```

After you create the key, you must restart the Server for NFS.

# Restarting The Server For NFS

To restart the server for NFS:

1. Press the Windows logo key on the keyboard.
2. Type `CMD`.

   **Command Prompt** application is displayed.
3. Right-click **Command Prompt**, and select **Run as administrator** to open an elevated command prompt.
4. Run the following command:

   ```
   nfsadmin server stop && nfsadmin server start
   ```

# Creating The NFS Share

To create an NFS share:

1. In **Server Manager** window, go to **File and Storage Service** server role and click **Shares**.

   A page with **Shares**, **Volume** and **Quota** panes is displayed.
2. To create a new share, in the Shares section, perform any one of the steps below:

   – Click **To create a file share, start the New Share Wizard** link
   – Select **New Share** from the **Tasks** dropdown list.

   The **New Share Wizard** window is displayed.
3. On **Select the Profile for this share** page, select the **File Share profile (NFS Share – Quick or Advanced)** based on requirements and click **Next**.
4. On **Select the server and path for this share** window, select the **Server name** and **Share location** for this new share and click **Next**.

   The share location can be selected either by **Volume** or by **Typing a custom path**.
5. On **Specify share name** window, enter the **Share name** and **Share description** and click **Next**.

   If a share folder does not exist, the local path to share creates a folder automatically.
6. On **Specify the authentication methods** window, select the authentication method for NFS share and click **Next**.

   NOTE: Only the UNIX user (who was added in the domain user list) has access to the NFS share. If you have enabled Anonymous access for the NFS share, all UNIX users have access to the share.
7. On **Configure share settings** window, select the required settings and click **Next**.
8. On **Specify permissions to control access** window, set the permissions on the file shares and click **Next**.

9. Set the folder permissions in various combinations as required and click **Next**.
10. On **Confirm selections** window, confirm the settings and click **Create**.

    The **View results** window is displayed showing the successfully creation of share.
11. Click **Close** to exit the wizard.

# Creating Quotas And File Screens Using File Server Resource Manager

Quotas and File Screens can be created using the **File Server Resource Manager** tool.

1. In the **Server Manager** menu bar, click **Tools** → **File Server Resource Manager**.

   The **File Server Resource Manager** console is displayed.
2. Double-click **Quota Management** to display **Quotas** and **Quota Template**.
3. Double-click **Quota**, either right-click or use the **Create Quota** option from the right pane.
4. Follow the wizard, select the path (volume or folder in which you want to create the quota), set your preferred **Quota Properties** and click **Create**.

   The newly-created quota is displayed in the central pane.
5. Select any of the existing quotas and right-click or use the options in the right pane to change the quota properties.
6. Click **File Screening Management** → **File Screens**.
7. Either right-click or use **Create File Screen** option from the right pane.
8. Follow the wizard, select the path (volume or folder in which you want to create the file screen), select your preferred **File Screen Properties** and click **Create**.

   The newly-created file screen is displayed in the central pane.
9. Select any of the existing file screens and right-click or use the options in right-most panes to change the file screen properties.

# Creating A New Volume

To create a new volume:

NOTE: Backup Operator or Administrator is the minimum membership required to perform this configuration.

1. In the **Server Manager**, click **Files and Storage Services** server role and select **Volumes**.
2. In the **Volumes** pane from **Tasks** drop-down menu, select **New Volume**.

   The **New Volume Wizard** window is displayed.
3. Follow the instructions on the wizard, select the **volume size**, assign the **drive letter**, choose the **file system type**, type in the **volume label**, select the **format option**, and **Data Deduplication** settings.
4. Confirm the volume creation settings and click **Create**.

   The new volume created is displayed in the **Volumes** pane.

# Managing A Volume

Disk Management is used to manage disks and volumes. To access Disk Management, open the **Server Manager**, click on the **Tools** menu, and select **Computer Management** → **Storage** → **Disk Management**.

- You can initialize disks, create volumes, and format volumes with the FAT, FAT32, or NTFS file systems using Disk Management.

- Disk Management enables you to perform most disk-related tasks without restarting the system or interrupting users.

# Extending A Volume

You can add more space to existing primary partitions and logical drives by extending them into adjacent un-allocated space on the same disk. To extend a basic volume, it must be raw or formatted with the NTFS file system.

## Extending A Basic Volume Using The Windows Interface

**NOTE:** If you do not have un-allocated space in your disk, use Dell OpenManage Server Administrator to extend your LUN before you extend your volume.

To extend a basic volume using the Windows interface:

1. Open the **Server Manager**, click on the **Tools** menu, and select **Computer Management → Storage → Disk Management**.
2. In **Disk Management**, right-click the **Basic Volume** you want to extend.
3. Click **Extend Volume**.
   The **Extend Volume Wizard** window is displayed.
4. Follow the instructions on your screen. Choose the disks, type in the amount of space and complete the wizard.

## Extending A Basic Volume Using CLI

To extend a basic volume using CLI:

1. Open a command prompt window and type `diskpart`.
2. At the DISKPART prompt, type `list volume`.
3. Make note of the basic volume you want to extend.
4. At the DISKPART prompt:
   a) Type `select volume` <volume number> to select the basic volume number that you want to extend into contiguous, empty space on the same disk
   b) Type `extend` [size=<size>] to extend the selected volume by size megabytes (MB).

# Shrinking A Volume

You can decrease the space used by primary partitions and logical drives by shrinking them into adjacent, contiguous space on the same disk. For example, if you need an additional partition but do not have additional disks, you can shrink the existing partition from the end of the volume to create new un-allocated space that can then be used for a new partition.

To shrink a volume:

1. Open the **Server Manager**, click on the **Tools** menu, and select **Computer Management → Storage → Disk Management**.
2. In **Disk Management**, right-click the **Basic Volume** you want to shrink.
3. Click **Shrink Volume**.
   A **Shrink <volume name>** window is displayed.

4. Follow the instructions on your screen and click **Shrink**.

   NOTE: You can only shrink basic volumes that have no file system or use the NTFS file system.

### Additional Considerations When Shrinking A Volume

- When you shrink a partition, unmovable files (for example, the page file or the shadow copy storage area) are not automatically relocated and you cannot decrease the allocated space beyond the point where the unmovable files are located.
- If the number of bad clusters detected by dynamic bad-cluster remapping is too high, you cannot shrink the partition. If this occurs, you should consider moving the data and replacing the disk.
- Do not use a block-level copy to transfer the data. The block-level copy also copies the bad sector table and the new disk treats the same sectors as bad even though they are normal.
- You can shrink primary partitions and logical drives on raw partitions (those without a file system) or partitions using the NTFS file system.

## Deleting A Volume

To delete a volume:

**CAUTION: You must delete all shares and shadow copies from your volume before deleting it. If a volume is removed before all shares of that volume have been removed, the Server Manager might not display shares correctly.**

1. Open the **Server Manager**, click on the **Tools** menu, and select **Computer Management → Storage → Disk Management**.
2. In **Disk Management**, right-click the **Volume** you want to delete and select the **Delete Volume** option.

   **Delete Simple Volume** confirmation window is displayed.
3. Select **Yes** on the confirmation screen to delete the volume.

### Additional Information When Deleting A Volume

New features of disk management include:

| | |
|---|---|
| Simpler partition creation | When you right-click a Volume, you can choose whether to create a basic, spanned, or striped partition directly from the menu. |
| Disk conversion options | When you add more than four partitions to a basic disk, you are prompted to convert the disk to dynamic or to the GUID Partition Table (GPT) partition style. |
| Extend and shrink partitions | You can extend and shrink partitions directly from the Windows interface. |

## Data Deduplication

Data Deduplication feature works at a sub-file level and stores more data in less space by segmenting files into small chunks, identifying duplicate data, and maintaining a single copy of each data chunk. The files are compressed and organized in special container files in the System Volume Information folder.

After enabling a volume for deduplication and optimizing the data, the volume contains unoptimized files, optimized files, chunk store and additional free space.

Data Deduplication in Windows Storage Server 2012 R2 supports optimized remote storage for Virtual Desktop Infrastructure (VDI) deployments. Data deduplication with VDI improves the IO performance of the storage subsystems resulting in the better utilization of existing subsystems for general file servers and VDI storage.

NOTE: Data Deduplication replaces SIS (Single Instance Storage) feature in Windows Storage Server 2012 R2. When using Data Deduplication feature for the first time or migrating from a previous version of Windows Storage Server to Windows Storage Server 2012 R2. For more information on *Data Deduplication Interoperability*, see : **technet.microsoft.com/en-us/library/hh831454.aspx**.

NOTE: To set up a server, enable data deduplication, and optimize a volume, see *Install and Configure Data Deduplication* at: **technet.microsoft.com/en-us/library/hh831434.aspx**.

# Enabling And Configuring Shadow Copies Of Shared Folders

**Shadow Copies** are used to view the previous content of the shared folders. If you enable **Shadow Copies** of shared folders on a volume using the default values, tasks are scheduled to create shadow copies at 7:00 A.M. and noon. The default storage area is on the same volume and its size is 10 percent of the available space.

You can only enable **Shadow Copies** of shared folders on a per-volume basis; you cannot select specific shared folders and files on a volume to be copied or not copied.

NOTE: Creating shadow copies is not a replacement for creating regular backups.

**CAUTION: There is a limit of 64 shadow copies per volume. When this limit is reached or when storage area limits are reached, the oldest shadow copy is deleted. When deleted, the shadow copy cannot be retrieved.**

1. Open the **Server Manager**, click on the **Tools** menu, and select **Computer Management → Storage → Disk Management**.

   A list of volumes on your system is displayed in the middle pane of the storage console.
2. Right-click the volume and select the **Properties**.

   The selected<*Volume*> properties window is displayed.
3. Click on the **Shadow Copies** tab.
4. Select the volume you want to enable **Shadow Copies** of shared folders and click **Enable**.
5. Click **Create Now** to create the Shadow Copies of the selected volume.
6. Click **Settings**, to change the storage location, space allocation, and schedule.

# Performing Backup Of Your Server Using Windows Server Backup Feature

**Windows Server Backup** is a feature that provides a set of tools and wizard to perform basic backup and recovery tasks for the servers installed on your system. The data backup can be done to a local or online location.

To install **Windows Server Backup** feature on your system:

1. Open the **Server Manager**, click on the **Manage** menu, and select **Add Roles and Features**.

   The **Add Roles and Features Wizard** is displayed.
2. Follow the **Add Roles and Features Wizard** step by step, on the **Select features** window, select the **Windows Server Backup** check box and click **Next**
3. Confirm the feature to install and click **Install**.

   The **Windows Server Backup** feature is now installed on your system.
4. To access **Windows Server Backup** feature:

   – Open the **Server Manager**, click on the **Tools** menu, and select **Windows Server Backup** from the list.

   – Alternatively, open the **Server Manager**, click on the **Tools** menu, and select **Computer Management → Storage → Windows Server Backup** .

   The **Windows Server Backup** console is displayed in the middle pane of the window.

   The following backup options are available:

   – Local Backup : To perform single backup or schedule a regular backup using **Backup Schedule Wizard** or the **Backup Once Wizard** on your system.

   NOTE: In the **Windows Server Backup** feature, use the **Recovery Wizard** to recover files, applications, volumes, or the system state from a backup that was created earlier.

   – Online Backup : To perform online backup by registering your system for the Windows Azure Online Backup. For more information, see: **technet.microsoft.com/en-us/library/hh831419.aspx**.

# Choosing Volumes To Backup

To create a backup, you need to specify the volumes that you want to include. The volumes you select impact what you can recover. You have the following volume and recovery options.

| Volume Options | Recovery Options |
|---|---|
| Full server (all volumes) | Back up all volumes if you want to be able to recover the full server—all the files, data, applications, and the system state. |
| Critical volumes | Back up just critical volumes (volumes containing operating system files) if you only want to be able to recover the operating system or system state. |
| Non-critical volumes | Back up just individual volumes if you only want to be able to recover files, applications, or data from that volume. |

# Choosing A Storage Location

To store the backups that you create, you need to specify a location. Depending on the type of storage you specify, you should be aware of the following issues.

| Storage Type | Details |
|---|---|
| Shared Folder | If you store your backup in a remote shared folder, your backup is overwritten each time you create a new backup. Do not choose this option if you want to store a series of backups.<br>If the backup process fails while you are trying to create a backup to a shared folder that already contains a backup, you might be left without any backups. To work around this, you can create subfolders in the shared folder to store your backups. |
| DVD, other optical media, or removable media | If you store your backup on optical or removable media, you can only recover entire volumes, not applications or individual files. In addition, backing up to media that has less than 1 GB of free space is not supported. |
| Local hard disk | If you store your backup on an internal hard disk, you can:<br>• Recover files, folders, applications, and volumes.<br>• Perform system state and operating system recoveries if the backup used contains all the critical volumes.<br>However, you cannot perform an operating system recovery if the backup is on the same physical disk as one or more critical volumes.<br>Also, the local disk you choose is dedicated for storing your scheduled backups and is not visible in Windows Explorer. |
| External hard disk | If you store your backup on an external hard disk, you can:<br>• Recover files, folders, applications, and volumes.<br>• Perform system state and operating system recoveries if the backup used contains all the critical volumes.<br>• Easily move backups offsite for disaster protection.<br>If you store your scheduled backups on an external hard disk, the disk is dedicated for storing your backups and is not visible in Windows Explorer.<br>This enables users to move disks offsite for disaster protection and ensure backup integrity. |

# NIC Teaming

NIC teaming, also known as Load Balancing/Failover (LBFO) is a built-in feature of Windows Storage Server 2012 R2 that allows fault tolerance for your network adapters. NIC teaming allows multiple network adapters to work together as a team, preventing connectivity loss if one NIC fails.

The advantage of built-in NIC teaming is that it works with all NICs and provides a set of management tools for all adapters. The outbound traffic can be distributed among the available network adapters by using **Switch-independent mode** and **Switch-dependent mode** for network traffic distribution.

## Configuring NIC Teaming On A Server

NOTE: **Broadcom Advanced Control Suite (BACS)** is installed when a Broadcom NIC is detected and **Intel PROSet** drivers are installed when Intel NIC is detected.

NOTE: Microsoft recommends use of the built in NIC teaming functionality in **Server Manager**.

To configure NIC teaming on a server:

1. From the **Server Manager**, select **Local Server**.
   The properties of Local Server is displayed.
2. Click on the status next to the **NIC Teaming**.
   The **NIC Teaming** window is displayed.
3. In **Adapters and Interfaces** section, the list of available adapters that can be teamed are displayed.
4. Select the adapters to be added to a team. Right-click and select **Add to New Team**.
5. In the **NIC Teaming** window, enter **Team name** for the adapters to be added in.
6. In **Additional properties**, select the **Teaming Mode**, **Load balancing mode**, **Standby adapter**, and click **OK**.
   The new-created NIC team is displayed in the **Teams** section of the same window.
7. After creating and configuring a NIC team, go to **Open Network and sharing Center → Change Adapter Settings**
   The new-created NIC team is displayed in this window.