



DELL EMC NX3340 PowerVault NX Series Network Attached Storage Systems Installation Guide

[Home](#) » [DELL EMC](#) » DELL EMC NX3340 PowerVault NX Series Network Attached Storage Systems Installation Guide 📄

DELL EMC NX3340 PowerVault NX Series Network Attached Storage Systems



Contents

- [1 Overview](#)
- [2 iSCSI deployment](#)
- [3 Supported hardware and software](#)
- [4 Preinstalled roles and services configurations on your system](#)
- [5 Configuring your NAS system](#)
- [6 Initial configuration of your NAS system](#)
- [7 Server Manager roles, role services, and features](#)

- 8 Starting and exiting Server Manager
- 9 Accessing administrative tools for your NAS systems
- 10 Accessing computer management
- 11 Work folders
- 12 Installing work folders
- 13 Creating sync share for work folders
- 14 Creating a new DFS namespace
- 15 Creating new DFS replication group
- 16 Adding DFS namespaces to display
- 17 Adding replication groups to display
- 18 File Server Resource Manager
- 19 Multipath I/O
- 20 Adding devices on MPIO
- 21 Managing your NAS system
- 22 Dell OpenManage Server Administrator
- 23 Remote Desktop for Administration
- 24 Creating and saving remote desktop connection
- 25 Reinstalling NAS operating system using a DVD
- 26 Deploying the OS using Dell Lifecycle Controller
- 27 Creating RASR USB recovery drive
- 28 Recovering the Operating System using RASR USB Recovery Drive
- 29 Using your NAS system
- 30 Creating server message block share
- 31 Modifying message block shares
- 32 NFS share
- 33 Windows domain controller as identity mapping source
- 34 User name mapping server as identity mapping source
- 35 AD LDS as identity mapping source
- 36 Configuring AD LDS for services for NFS
- 37 Installing AD LDS server role
- 38 Creating a new AD LDS instance
- 39 Extending the AD LDS schema to support NFS user mapping
- 40 Setting a default instance name for AD LDS instances
- 41 Connecting to the distinguished name or naming context
- 42 Adding user account maps
- 43 Adding group account maps
- 44 Authorizing access to the ADS LDS namespace object
- 45 Configuring the mapping source
- 46 Debug notes for NFS account mapping problems
- 47 Restarting the server for NFS
- 48 Creating quotas using File Server Resource Manager
- 49 Creating file screens using file Server Resource Manager
- 50 Creating a new volume
- 51 Managing a volume
- 52 Extending a volume
- 53 Extending a basic volume using the Windows interface
- 54 Extending a basic volume using CLI
- 55 Shrinking a volume
- 56 Additional considerations when shrinking a volume
- 57 Deleting a volume
- 58 Additional information when deleting a volume
- 59 Data deduplication
- 60 Performing backup of your server
- 61 Configuring NIC teaming on a server
- 62 Getting help
- 63 Contacting Dell
- 64 Locating your system service tag
- 65 Accessing system information using the QRL
- 66 Downloading drivers and firmware

Overview

Windows Storage Server 2016 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 2016 operating systems (OSs) are cost-effective and easy to manage storage solutions.

To view new features and functionalities for 2016, go to <https://technet.microsoft.com/en-us/windows-server-docs/storage/whats-new-file-storage-services-windows-server-2016>.

Topics:

- iSCSI deployment
- Supported hardware and software
- Preinstalled roles and services configurations on your system

iSCSI deployment

In Windows Storage Server, 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 OS storage
- Controlled OS images that are more secure and straight forward to manage
- Fast recovery
- Protection to data from getting corrupted
- Heterogeneous storage to support non-Windows iSCSI initiators
- Converts a system running Windows server into a network-accessible block storage device



NOTE: For information about how to configure the iSCSI Target Server for NX NAS systems, go to <https://technet.microsoft.com/en-us/library/hh848268>.

Supported hardware and software

The following PowerVault NX Series systems run Microsoft Windows Storage Server 2016 operating systems:

Windows editions	PowerVault NX systems supported
Microsoft Windows Storage Server 2016, Standard Edition, x64	NX3340, NX3330, NX3240, NX3230, NX440, NX430
Microsoft Windows Storage Server 2016, Workgroup Edition, x64	NX440, NX430

Preinstalled roles and services configurations on your system

Server roles, role services, and features are preinstalled and configured on your system based on your organization's requirements.

Roles and Role Services

Preinstalled roles and role services include:

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 disk 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 on different servers into one or more logically structured namespaces.
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 the 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	Allows users to access their work files from various devices and keeps them synchronized whether users access their files from inside the network or from across
Storage Services	Provides storage management functions.

Features

Preinstalled features include:

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.
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/CIFS File Sharing Support	Supports file sharing protocol and computer browser protocol.
Windows PowerShell (includes Windows PowerShell 5.1, 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 the Server Core installation.

Configuring your NAS system

After your initial configuration, use Server Manager to configure roles, role service, and features. Topics:

- Initial configuration of your NAS system Server Manager roles, role services, and features
- Installing or uninstalling Server Manager roles, role services, and features
- Accessing administrative tools for your NAS systems
- Accessing computer management
- Work folders
- Creating a new DFS namespace
- Creating new DFS replication group
- Adding DFS namespaces to display
- Adding replication groups to display
- File Server Resource Manager
- Multipath I/O

Initial configuration of your NAS system

Initial configuration of your NAS system includes cabling the system, turning it on and the configuring the system using Server Manager. Follow these steps to complete the configuration of your NAS system.

About this task



NOTE: The NX Series systems support only BIOS mode. Do not change the boot mode to UEFI because the system will not load the appliance OS when in UEFI mode.

Steps

1. Start your NAS system running Windows Storage Server 2016. The first time that you start up, click OK on the Default Password screen.

NOTE: Before changing the password, ensure that you change the system language according to your preference. Your system is configured with default user name administrator and password Storage!

2. To change your administrator password, press Ctrl+Alt+Delete, and then click Change a Password. Server Manager starts automatically when you log in the first time.
3. 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: To go to a particular application, click the lower-left corner of the screen to locate the Start icon.
4. To change the default language, go to C:\Dell_OEM\MUI, and then run the appropriate language batch file. To install your preferred language, complete the on-screen instructions.

5. Dell recommends creating a Dell Rapid Appliance Self Recovery image after completing the initial setup (NX3230, NX3240, NX3330, NX3340 systems only). For more information, see Dell Rapid Appliance Self Recovery (RASR) section in this document.

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.

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 change local or remote servers.
- Get the status of your servers and roles remotely.
- Use the server status to identify critical events and 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 an administrator logs in to the system. If you exit Server Manager, perform any one of the following tasks to restart:

- On the task bar, click Server Manager.
- On the Start screen, click Server Manager.
- In the Windows PowerShell environment, at the command prompt, enter server manager (case-insensitive).

To exit Server Manager, close the Server Manager window.

Installing or uninstalling Server Manager roles, role services, and features In Windows Storage Server use the Server Manager console and Windows PowerShell cmdlets to install roles, role services, and features. You can install multiple roles and features using the Add Roles and Features Wizard or using a Windows PowerShell session.



NOTE: For information about 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 systems

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

Access the administrative tools folder using one of the following methods:

- In Server Manager, click Tools.
- Click the Windows logo key. In the Start menu, click Administrative Tools tile.
- In the start menu, click Control Panel, click System and Security > Administrative Tools.

Accessing computer management

To access the Computer Management tools, in Server Manager, go to Tools > Computer Management. The Computer Management window displays tools options grouped by System tools, Storage, and Services and applications.

System tools

Task Scheduler

Used to create and manage basic tasks that the system performs automatically at specific times. Tasks created are stored in the Task Scheduler library. It also tracks the Task Status and Active Tasks that are not expired.

Event Viewer

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 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

Used to create and manage users and groups that are stored locally on a computer. Performance Used to monitor performance in real time or through a log. Configuration data is collected, and events are 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 OS.

Storage

Windows Server Backup

Feature that uses command line interface (CLI) and Windows PowerShell cmdlets for day-to-day backup and recovery requirements. The data backup can be performed locally and online. To run Windows Server Backup, install the Windows Server Backup feature.

Disk Management

System utility for managing hard disk drives and the volumes or partitions that they contain. Management allows you to create and attach virtual 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 that combines three Networking services into one unified server role: Direct Access, Routing, and Remote Access.

Services

Used to manage services such as file serving and event logging that are running on local or remote computers. You can also manage services by running the `sc config` command.

Work folders

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 about Work Folders, go to technet.microsoft.com/en-us/library/dn265974.aspx.

Installing work folders

To install Work Folders:

Steps

1. In Server Manager, 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 one of the following and then click Next.
 - Role-based or feature-based installation to install all parts of roles or features
 - Remote Desktop Services installation to install either a virtual machine-based desktop infrastructure or a session based desktop infrastructure for Remote Desktop Services
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 is already installed, and then click Next.
5. In the Select Server Roles window, click File and Storage Services > File and iSCSI Services > Work Folders. The Add features that are required for Work Folders dialog box is displayed.
6. If additional features are required for installing Work Folders, click Add Features to continue, and then click Next.
7. In the Work Folders window, review the summary information, and then click Next.
8. In the Confirm Installation Selections window, read any informational messages, and then click Install.
9. To verify if the installation is successfully completed, review the Installation Results window.
10. Click Close to close the wizard.

The Work Folders role is created in the Server Manager > Files and Storage Services folder.

Creating sync share for work folders

To create a sync share for the work folders:

Steps

1. In Server Manager, click File and Storage Services > Work Folders.
A page with Work Folders, Users, Volume, and Quota panes is displayed.
2. To create a sync share, in the Work Folders section, perform any one of the following tasks:
 - Click To create a sync share for Work Folders, start the New Sync Share Wizard
 - Select New Sync Share from the Tasks drop-down menu.The New Sync Share Wizard window is displayed.
3. Complete the on-screen instructions, and create a sync share for the Work folders. For information about deploying work folders, go to technet.microsoft.com/en-us/library/dn528861.aspx#step3.

Creating a new DFS namespace

To create a new DFS namespace:

Steps

1. In Server Manager, click Tools > DFS Management.
The DFS Management window is displayed.
2. Under Actions, click New Namespace.
The New Namespace Wizard is displayed.
3. Complete the tasks in the New Namespace Wizard and close the wizard.



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

Creating new DFS replication group

To create a new DFS replication group:

Steps

1. In Server Manager, 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. Complete the tasks in the New Replication Group Wizard and close the wizard.

Adding DFS namespaces to display

To add DFS namespaces to display:

Steps

1. In Server Manager, 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:

Steps

1. In Server Manager, 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 group 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

The File Server Resource Manager (FSRM) is a collection of tools for Windows Storage Server. File Server Resource Manager allows administrators to understand, control, and manage the quantity and type of data that is stored on their system. Administrators can use FSRM to place quotas on folders and volumes, to actively screen files, and to generate comprehensive storage reports. These tools help the administrator to efficiently monitor existing storage resources, and aids in the planning and implementation of future policy changes. FSRM tasks include:

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

Multipath I/O

Microsoft Multipath I/O (MPIO) is a framework provided by Microsoft which enables storage providers to develop multipath solutions that contain hardware-specific information. 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 OS. MPIO is required to optimize connectivity to storage arrays.

MPIO provides the following features:

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



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

Adding devices on MPIO

To add or remove devices on MPIO:

Steps

1. In Server Manager, click Tools > MPIO.
The MPIO Properties window is displayed.
2. In the MPIO Devices tab, click Add, enter the Device hardware ID of the device you want to add MPIO support for, and then click OK.
3. The device hardware IDs are listed 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. In the DSM Install tab, type the DSM INF file and click Install or uninstall to install or Uninstall a DSM.
5. In 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 then click Capture.

Managing your NAS system

The following tools can be used to manage your system:

NOTE: The NX Series systems support only BIOS mode. Do not change the boot mode to UEFI because the system will not load the appliance OS when in UEFI mode.

Topics:

- Dell OpenManage Server Administrator
- Remote Desktop for Administration
- Reinstalling NAS operating system using a DVD
- Dell EMC Rapid Appliance Self Recovery

Dell OpenManage Server Administrator

Dell OpenManage Server Administrator can be downloaded from the Dell Technologies support site. Dell OpenManager Server

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

- Integrated web browser-based user interface—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 about Dell OpenManage Server Administrator, see the Dell EMC OpenManage Server

Administrator User's Guide for the relevant version at Dell.com/openmanagemanuals.

Remote Desktop for Administration

You can remotely administer a storage system using Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode). Based on the terminal services technology, Remote Desktop for Administration is designed for server management.



NOTE: Remote desktop for administration does not require you to purchase 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 in to the server remotely by using any of the following tools:

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



NOTE: For secure connections, Dell EMC recommends obtaining a certificate for the server and use HTTPS connections to connect to Windows Storage Server.

Activating remote desktop connection

To activate a remote desktop connection:

Steps

1. In Server Manager, click Local Server.
2. In the Properties window, click the Enabled link next to the Remote Desktop option.

In Windows Storage Server, remote management is enabled by default.

The System Properties window is displayed.

3. In the Remote tab, in the Remote Desktop section, select Allow remote connections to this computer.



NOTE: Remote desktops with an authenticated network level are allowed to connect to the system.

4. Click Select Users. The Remote Desktop Users window is displayed
5. Click Add or Remove to give access to users, and then click OK.
6. Click Apply, and then click OK.

Creating and saving remote desktop connection

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

Steps

1. On the taskbar, click Start, and then type Run in the search box and press enter.
The Run dialog box is displayed.
2. In the Run dialog box, type MSTSC, and then 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 system, and then click Options.
The Connection Settings window is displayed.
4. In the Remote Desktop Connection window, click Save As in the Connection Settings dialog box.
The Save As window is displayed.
5. In File name, type a name for the connection, and leave the extension as.rdp.
6. From 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 NAS operating system using a DVD

If you are reinstalling the NAS operating system onto new OS drives, you will also need to partition the new drives. This section describes both how to repartition the new OS drives and how to reinstall the NAS operating system.



CAUTION: Back up the internal disk drives on your system before reinstalling or upgrading the NAS Operating System. The DVD reinstall process formats or deletes the OS disks (virtual disk 0) resulting in loss of any data or installed applications. The DVD reinstall process does not install RASR USB Recovery application.

The standard RAID configuration varies depending on the system:

- **NX430:** OS-only – RAID 5
- **NX440:** OS-only – RAID 5
- **NX3230:** OS HDDs – RAID 1 (on rear 2.5 in. HDDs)
- **NX3240:** OS HDDs – RAID 1 (on rear 2.5 in. HDDs)

- **NXb3330:** OS-only – RAID 1 (two HDDs) or RAID 5 (four HDDs)
- **NX3340:** OS-only – RAID 1 (two HDDs) or RAID 5 (four HDDs)

Refer to your original, as-shipped configuration for details about your specific RAID configuration.

Recovering an OS partition

Follow this procedure to recover your OS partition if becomes corrupt.

Prerequisites

- Failed OS drives have been replaced with new, blank HDDs.



CAUTION: Do not remove or delete the original partitions on the data drives or their associated physical drives.

Steps

1. Turn on or restart your system, and press F2 to boot into System Setup.
2. Click Device Settings.
3. Click Integrated RAID Controller 1: Dell PERC Configuration Utility.
4. In the Configuration Utility menu, click Virtual Disk Management.
5. Verify the following:
 - Your original Data partition or partitions are shown
 - No OS partition is listed
6. Click Back without making any changes to the data partitions.
7. In the Configuration Utility, click Create Virtual Disk.
8. In the Create Virtual Disk dialog box, select the RAID Level and Capacity options.
 - Select RAID Level — See the standard RAID configurations above.
 - Select Physical Disks From — Unconfigured Capacity.
9. Click Select Physical Disks, choose the drives to configure for RAID.
10. Click Apply Changes.
11. Wait for the Success screen to display The operation has been performed successfully, and then click OK.
12. Under Create Virtual Disk Parameters set the following options and leave remaining options set to their default settings:
 - Virtual Disk Name — enter a unique name such as OS
 - Virtual Disk Size — in GB (currently this partition is 140GB).
 - Default Initialization — Fast (for example)
13. Click Create Virtual Disk.
14. In the Warning screen, select Confirm and click Yes.
15. When the message appears that the virtual disk was created successfully, click OK.
16. Click Back two times to return to the Configuration Utility Main Menu.
17. Click Virtual Disk Management.

18. Verify that both the newly-created OS partition and the existing data partitions are present.
19. Click Back to return to the Configuration Utility Main Menu.
20. Click Controller Management.
21. For Select Boot Device select OS Partition.
22. Click Back to return to the Configuration Utility Main Menu and click Finish.
23. Click Finish again and reboot the system.
24. During the restart, press F2 to boot into System Setup .
25. On the System Setup Main Menu, click System BIOS.
26. In the System BIOS options, select Boot Settings > BIOS Boot Settings.
27. Verify that the Integrated RAID Controller 1: PERC H730P Mini is present and is selected as the Boot Option.
28. Back-out of the BIOS, saving any changes as needed.
29. Restart the system and press F10=Lifecycle Controller to proceed to deploying the OS.

Deploying the OS using Dell Lifecycle Controller

Follow this procedure to deploy the OS using Dell Lifecycle Controller.

Prerequisites

- OS drives are installed and have been partitioned.
- External USB DVD ROM is available.
- Windows Storage Server 2016 product key is available. This should be attached to the system cover.

Steps

1. If not completed already, restart the system and press F10=Lifecycle Controller.
2. In the left navigation pane, select OS Deployment.
The OS Deployment wizard starts.
3. On the Select Deployment path page select Go directly to OS Deployment and click Next.
4. On the Select an Operating System page accept the default settings:
 - Boot Mode — BIOS
 - Secure Boot — Disabled
 - Secure Boot Policy — Standard
 - Available Operating Systems — Microsoft Windows Server 2016
5. Click Next.
The system assembles the OS drivers. This process takes less than five minutes.
6. On the Select Installation Mode page, select Manual Install and click Next.
The OS Media page is displayed.
7. Insert the DVD Reinstall media disk for Windows Storage Server 2016 (Workgroup or Standard) into the external drive and
click Next.
The system performs an OS media validation and opens the Reboot the System page.
8. Verify the selections and click Finish.
9. When prompted, press any key to boot to the operating system media.

The system reboots and starts the operating system installation wizard.

10. On the language selections page select the applicable language and click Next.
11. Select Install Now and click Next.
12. On the product activation page enter your product key and click Next.
13. On the license acceptance page select I accept the license terms and click Next.
14. On the next page select Custom: Install the newer version of Storage Server only (advanced).
15. In the Where do you want to install Storage Server? option, select the 140 GB drive that was created in the OS partition recovery steps.



NOTE: Do not select an existing data drive for OS installation. Make sure the drive selected is the new OS drive created for this purpose.

16. In the OS Target-Drive option select Unallocated Space (the default) and click Next.
The installation begins and takes 60 – 90 minutes to complete. Errors encountered are flagged on the front panel LCD of your device.
17. Finish the installation by completing the initial configuration steps described in the product Installation and Service Guide.
Go to dell.com/support to download drivers and OpenManage Server Administrator software as needed.

Dell EMC Rapid Appliance Self Recovery

Dell EMC Rapid Appliance Self Recovery (RASR) provides a method by which the administrator can restore the PowerVault NAS system to the factory default settings. The process uses a bootable USB recovery drive that is created from your system.



NOTE:

- This option is available only on NX3230, NX3240, NX3330, and NX3340 systems.
- Dell EMC highly recommends creating a RASR USB drive immediately after completing the NAS initial system configuration.
- To prevent data or application loss, back up the operating system drives before reinstalling NAS operating system.
- This option is only available from factory configuration and not available if the system is restored from DVD.

Creating RASR USB recovery drive

To create an RASR USB recovery drive, a USB drive must be installed and recognized by the system before starting the application. An 8 GB USB drive is sufficient.

Prerequisites

Operating system drives are backed up.

Steps

1. Insert a USB drive into the system.



NOTE: Creating an RASR USB recovery drive deletes all data on the USB drive.

2. Start the application by double-clicking the Create RASR USB Recovery Drive icon on the Windows Desktop. The Dell EMC NX#### – Rapid Appliance Self Recovery (RASR) page is displayed. RASR displays information for each USB drive that the RASR Recovery application identifies.
3. If more than one USB drive is detected, select the USB drive on which you want to install the RASR application.
4. To install the RASR application on the USB drive, complete the on-screen instructions that are displayed on the Create RASR USB Recovery Drive application.
5. After the RASR USB drive is successfully created, verify that the USB drive boots properly by booting to the USB drive.
6. Complete the instructions in the Recovering OS using RASR USB Recovery Drive section.
7. After the RASR application has started, exit the application without performing any of the recovery actions and restart the system. This procedure completes verification that the USB recovery drive has been successfully created. Store the RASR USB drive in a safe place for future use.

Recovering the Operating System using RASR USB Recovery Drive

Follow this procedure to recover the operating system from the RASR drive.

Prerequisites

Any failed hard drives have been replaced.

Steps

1. Insert the RASR USB drive into a USB port on the system.
2. Boot the system and during the Power On Self-Test (POST), press F11 to select Boot Manager.
3. In the Boot Manager screen, select One-shot BIOS Boot Menu.
4. Select the RASR USB drive as the boot device.
5. The system boots the RASR USB drive.
6. To start RASR:
 - a. Select the keyboard layout.
 - b. Click the Troubleshoot icon.
 - c. Click the Rapid Appliance Self Recovery icon.
 - d. Click the Windows Server 2016 icon.



NOTE: Replace any failed hard drives before running the RASR application.

7. On the Welcome to Dell Rapid Appliance Self Recovery (RASR) page, click Next to start the recovery process.
8. Under Recovery Mode Selection, select one of the following the options:
 - System Recovery—Enabled if a Windows backup is found on any of the system hard drives. System Recovery restores

the operating system from a Windows backup. If a Windows Backup image is not found, this option is disabled.

- Windows Recovery Wizard—Starts the Windows backup application. Use this option if you want to recover the system from a Windows Backup image that is on a network drive.
- Factory Reset—Restores the Windows operating system from the image residing on the RASR USB drive. Use this option if the operating system has become unstable and must be reinstalled or if the operating system has failed because of a catastrophic hard drive failure.

9. In the Warning message that is displayed, click Yes to continue the operating system recovery. If you click No, the system stops the RASR process.

A window opens showing the operating system restoration progress. The recovery process may take up to 40 minutes depending on the speed of the USB drive.

10. Click Finish to stop the recovery process.

11. Click Yes to restart the system.

The operating system recovery process is finished, and the system is successfully recovered.

Using your NAS system

Topics:

- Creating server message block share
- Modifying message block shares
- NFS share
- Windows domain controller as identity mapping source
- User name mapping server as identity mapping source
- AD LDS as identity mapping source
- Configuring AD LDS for services for NFS
- Installing AD LDS server role
- Creating a new AD LDS instance
- Extending the AD LDS schema to support NFS user mapping
- Setting a default instance name for AD LDS instances
- Updating active directory schema
- Adding user and group account maps from a UNIX-based system to a Windows-based system
- Authorizing access to the ADS LDS namespace object
- Configuring the mapping source
- Debug notes for NFS account mapping problems
- Restarting the server for NFS
- Creating the NFS share
- Creating quotas using File Server Resource Manager
- Creating file screens using file Server Resource Manager
- Creating a new volume
- Managing a volume

- Extending a volume
- Shrinking a volume
- Deleting a volume
- Data deduplication
- Enabling and configuring shadow copies of shared folders
- Performing backup of your server
- NIC teaming

Creating server message block share

Windows Storage Server supports 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:

Steps

1. In Server Manager, click File and Storage Services > Shares.
A page with Shares, Volume, and Quota panes is displayed.
2. To create a share, in the Shares section, perform any one of the following tasks:
 - Click the To create a file share, start the New Share Wizard link.
 - Select New Share from the Tasks drop-down menu.
 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) check box based on requirements, and then 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.
You can select the share location either by volume or by typing a custom path.
5. In the Specify share name window, type the share name and share description, and then 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 then click Next.
7. In the Specify permissions to control access window, set the folder permissions in various combinations as required, and
then click Next.
8. In the Confirm selections window, confirm the settings, and then click Create.
The View results window displays a successful creation of share.
9. Click Close to close 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:

Steps

1. In Server Manager, click File and Storage Services > Shares.
2. Select the share from the Shares section.
3. Right-click and select Properties. The Properties windows is displayed.
4. You can click 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, by using network names.

Before creating NFS shares, 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 and Microsoft Windows Server 2016 domain controller)
- User Name Mapping (UNM) server
- Active Directory Lightweight Directory Services (AD LDS)

Related tasks

Creating the NFS share

Windows domain controller as identity mapping source

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

Steps

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, run the following command and press Enter: `Dism.exe /online /enable-feature /featurename:adminui /all`



NOTE: After Identity Management for UNIX is installed, restart the system. The /quiet parameter restarts the system automatically after the installation is completed.

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 then create the UNIX user name and group.
6. Add the user to the group created in the previous step.
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 task 6, and then click Apply.
9. Go to PowerVault NAS Windows Storage Server 2016 (NFS) Server.
10. Click Start > Administrative Tools > Services for Network File System.
11. Select Services for NFS..
12. Right-click Properties and select Active Directory domain name as your Identity mapping source.
13. Type the Windows Storage Server domain name, and then click Apply.

User name mapping server as identity mapping source

To install and configure User Name Mapping:

Steps

1. On your NAS system, in Server Manager, 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 task to a local disk.
5. Click 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 then select User Name Mapping.
8. Click Next and complete the installation.
NOTE: Restart your system after the installation is complete.
9. Go to NFS client, obtain the /etc/passwd and /etc/group files and copy them to a USB drive.
10. Go to the UNM server and copy the UNIX files from the USB drive to a local hard disk.
11. Start 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 task.
15. Go to the Simple Mapping tab, select the Use simple maps option, and then 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 task 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 then save the file.

AD LDS as identity mapping source

Active Directory Lightweight Directory Services (AD LDS) is used for identity mapping on systems that run Windows Storage

Server 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:

Steps

1. Install the AD LDS server role.
2. Create an 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.

Related tasks

Installing AD LDS server role

Installing AD LDS server role

To install the AD LDS Server Role:

Steps

1. In Server Manager, 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, click Role-based or feature-based installation to install all parts of roles or features. Or click Remote Desktop Services installation to install either a VM-based desktop infrastructure or a session-based desktop infrastructure for Remote Desktop Services, and then 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 2016 is already installed, and then 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? dialog box is displayed.
6. If additional features are required for installing AD LDS, click Add Features to continue, and then click Next.
7. In the Active Directory Lightweight Services window, review the summary information, and then click Next.
8. In the Confirm Installation Selections window, read any informational messages, and click Install.
9. To verify if the installation is successfully completed. Review the Installation Results window.
10. Click Close to exit the wizard.

The Active Directory Lightweight Directory Services role is created on the Server Manager dashboard page.

Creating a new AD LDS instance

To create a new AD LDS Instance:

Steps

1. In Server Manager, 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 then click Next.
4. In the Instance Name window, enter the instance name in the Instance name box, and then 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 option.
7. In the Partition name box, use the following format to type a partition name that does not already exist in this instance: CN=, DC=



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 is represented as 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 then click Next.
10. In the Service Account Selection window, select Network service account, and then 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. To continue, click Yes.
12. In the AD LDS Administrators window, select the currently logged on user: option, and then click Next.
13. In the Importing LDIF Files window, select the .LDF file names that you want to import, and then 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 then click Next. The AD LDS service starts installing.
15. Click Finish to close 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, click Control Panel > Programs > Programs and Features. All the AD LDS instances created are listed.

Extending the AD LDS schema to support NFS user mapping

To extend the AD LDS schema to support NFS mapping:

Steps

1. On the taskbar, click Start, and then type cmd in the search box.
2. Right-click Command Prompt and select Run as administrator.
3. 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:

Steps

1. In Server Manager, 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, click 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 then 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 box:

localhost:389

NOTE: This example uses the default LDAP port number 389. If you specify a different port number in 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-FirstSite-Name, click CN=Servers, click CN=server1\$nfsadldsinstance, and then click CN=NTDS Settings.

5. Right-click CN=NTDS Settings, and then click Properties.

6. In the Properties dialog box, click msDs-DefaultNamingContext, and then click Edit.

7. In the String Attribute Editor, in the Value box, type CN=nfsadldsinstance, dc=server1, and then click OK.

8. Close ADSI Edit.

Updating active directory schema

To update the active directory schema:

Steps

1. On the taskbar, click Start, and then type cmd in the search box.

2. Right-click Command Prompt, and select Run as administrator

3. Navigate to the C:\WINDOWS\ADAM directory, and run the command:

regsvr32 schmmgmt.dll

This command enables the Active Directory plug-in, schmmgmt.dll.

4. Click Start and then type Run.

5. Open the Run dialog and type MMC to start the Microsoft Management Console (MMC).

6. In the Console window, select File > Add/Remove Snap-in.

7. In the Add or Remove Snap-ins dialog box, click Active Directory Schema.

8. Click Add, and then click OK.

9. Right-click the Active Directory Schema node, and then click Change Active Directory Domain Controller to connect to the AD LDS instance that was previously created.



CAUTION: If you click (instead of right-click) and get an error, you have to restart MMC. These steps do not work if you accidentally click instead of right-click.

10. In the Change Directory Server dialog box, under Change to, click This Domain Controller AD LDS instance.

11. In the Name column, replace the placeholder text with the server and port number (for example, localhost:389).

NOTE: Press Enter after typing this information (or double-click the text). If you do not press enter, the OK button is not displayed.

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 then 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 then click OK.
- e. Click Add to open the Select Schema Object dialog box.
- f. Click uidNumber, and then click OK.
- g. Click OK.



CAUTION: If you accidentally left-click instead of right-click on User, after you do step g, you receive an error and have to start over again. To prevent this, either right-click or go back up to the Active Directory Schema node and click on it, then repeat step a.

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 then 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 then click OK.
 - f. Click OK.
15. Exit MMC, and then click Save.

Adding user and group account maps from a UNIXbased system to a Windows-based system

This section describes the following procedures that are required to add user and group account maps to a Windows-based system:

- Connecting to the Distinguished Name or Naming Context: Setting a default naming context and creating a container to hold your account mappings from UNIX to the Windows operating system.
- Adding User Account Maps: Mapping the uidNumber, gidNumber, and sAMAccountName attributes, to create a userclass object in the CN=Users container.
- Adding Group Account Maps: Creating 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:

Steps

1. In Server Manager, 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, click New, and then 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 then click Next.
8. In the Value box, type Users, and then 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:

Steps

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

NOTE: The user 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, exit and start the ADSI Edit MMC.

6. Click OK.

Adding group account maps

To add group account maps:

Steps

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



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

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, exit and start ADSI Edit MMC.

5. Click OK, and click Finish to close the wizard.

Authorizing access to the ADS LDS namespace object

To grant access to the namespace object:

Steps

1. On the taskbar, click Start, and then type cmd in the search box.
2. Right-click Command Prompt, and select Run as administrator.
3. Navigate to the C:\WINDOWS\ADAM directory, and run the dscls command to grant the Everyone group read access to the mapping data store as follows:
`dscls "\\server1:389\CN=nfsadldsinstance,dc=server1" /G everyone:GR /I:T`
4. 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: `dscls "\\server1:389\CN=nfsadldsinstance,dc=server1" /G "anonymous logon":GR /I:T`



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

Configuring the mapping source

To configure the mapping source:

Steps

1. On the taskbar, click Start, and then type cmd in the search box.
2. Right-click Command Prompt, and select Run as administrator.
3. Run the following command, where is the name of the computer where the AD LDS instance was created, is the port that the AD LDS instance uses: `nfsadmin mapping config adlookup=yes addomain=:`



NOTE: For this example, use the following: `nfsadmin mapping config adlookup=yes addomain=server1:389`

4. 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:

Steps


1. On the taskbar, click Start, and then type cmd in the search box.
2. Right-click Command Prompt, and select Run as administrator.
3. Run the following command:

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

Creating the NFS share

To create an NFS share:

Steps

1. In Server Manager, 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 following tasks:
 - Click To create a file share, start the New Share Wizard .
 - Select New Share from the Tasks drop-down menu.The New Share Wizard window is displayed.
 3. On the Select the Profile for this share page, select the File Share profile (NFS Share – Quick or Advanced) 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 then 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 Specify the authentication methods window, select the authentication method for NFS share, and then 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. In the Configure share settings window, select the required settings, and then click Next.
 8. On the Specify permissions to control access window, set the permissions on the file shares, and then click

Next.

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

The View results window is displayed showing the successful creation of share.

11. Click Close to close the wizard.

Creating quotas using File Server Resource Manager

Use the File Server Resource Manager tool to create quotas.

Steps

1. In Server Manager, click Tools > File Server Resource Manager.
The File Server Resource Manager console is displayed.
2. Double-click Quota Management to display the Quotas folder and Quota Template.
3. Double-click the Quotas folder and either do one of the following:
 - Right-click on Quotas folder and select Create Quota.
 - Select Create Quota from the Actions pane.
4. Complete the on-screen instructions, select the path (volume or folder in which you want to create the quota), set your preferred Quota Properties, and then click Create.

The newly-created quota is displayed in the central pane.

Creating file screens using file Server Resource Manager

Use the File Server Resource Manager tool to create File Screens.

Steps

1. In Server Manager, click Tools > File Server Resource Manager.
The File Server Resource Manager console is displayed.
2. Double-click File Screening Management.
3. Double-click the File Screens folder and either do one of the following:
 - Right-click on Create File Screen folder and select Create File Screen.
 - Select Create File Screen from the Actions pane.
4. Complete the on-screen instructions, select the path (volume or folder in which you want to create the file screen), select your preferred file screen properties, and then click Create.
The newly-created file screen is displayed in the working pane.
5. Select any of the existing file screens and right-click or use the options in right panes to change the file screen properties.

Creating a new volume

To create a new volume:

About this task



NOTE: You must have Backup Operator or Administrator privileges to create a new volume.

Steps

1. In 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. Select the Server and the Disk where the volume will be created.
4. Follow the instructions in the wizard to set the following parameters:
 - volume size
 - drive letter
 - file system type
 - volume label
 - format option
 - Data Deduplication
5. Confirm the volume creation settings and click Create. The new volume is displayed in the Volumes pane.

Managing a volume

Disk Management is used to manage disks and volumes. To access Disk Management, start the Server Manager, from the Tools menu, click 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

To extend a basic volume using the Windows interface:

Prerequisites

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

Steps

1. Start Server Manager, from the Tools menu, click 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. Complete the on-screen tasks, select the disks, type the disk space, and close the wizard.

Extending a basic volume using CLI

To extend a basic volume using CLI:

Steps

1. Open the CLI window and enter diskpart.
2. At the DISKPART prompt, enter list volume.
3. Make note of the basic volume you want to extend.
4. At the DISKPART prompt:
 - a. Type select volume to select the basic volume number that you want to extend into contiguous, empty space on the same disk.
 - b. Type extend [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 require 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:

Steps

1. Start Server Manager, from the Tools menu, select Computer Management > Storage > Disk Management.
2. In Disk Management, right-click the Basic Volume you want to shrink.
3. Click Shrink Volume. The Shrink window is displayed.
4. Complete 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 more, 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

Follow these steps to delete a volume.

Prerequisites

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.

Steps

1. Start Server Manager, from the Tools menu, click Computer Management > Storage > Disk Management.
2. In Disk Management, right-click the Volume you want to delete and select the Delete Volume option.
The Delete Simple Volume confirmation window is displayed.
3. Select Yes on the confirmation screen to delete the volume.

Additional information when deleting a volume

Additional features of disk management include:

- Simpler partition creation—When you right-click a Volume, you can choose 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 works at a sub-file level and stores more data in less space by segmenting files into small chunks. This feature identifies duplicate data and maintains 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 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) that was used in Windows Storage Server 2008. For more information about using Data Deduplication for the first time or when migrating from an environment using SIS, refer to Data Deduplication Interoperability section at technet.microsoft.com/en-us/library/hh831454.aspx.



NOTE: To set up a server, enable data deduplication, and optimize a volume, see the Install and Configure Data Deduplication section 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.

About this task

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 arealimits are reached, the oldest shadow copy is deleted. When deleted, the shadow copy cannot be retrieved.

Steps

1. Start the Server Manager.
2. From the Tools menu, click Computer Management > Storage > Disk Management. A list of volumes on your system is displayed in the middle pane of the storage console.
3. Right-click the volume and select the Properties. The selected Properties window is displayed.
4. Click the Shadow Copies tab.
5. Select the volume you want to enable Shadow Copies of shared folders and click Enable.
6. Click Create Now to create the shadow copies of the selected volume. 7. Click Settings to change the storage location, space allocation, and schedule.

Performing backup of your server

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. You can backup data to either a local or online location.

Prerequisites

To install Windows Server Backup on your system:

Steps

1. Start Server Manager, from the Manage menu, select Add Roles and Features.
The Add Roles and Features Wizard is displayed.

2. Complete the on-screen instructions in the Add Roles and Features Wizard, in the Select features dialog box, select the Windows Server Backup check box, and then 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, start Server Manager and do one of the following.
 - From the Tools menu, select Windows Server Backup.
 - From the Tools menu, select Computer Management > Storage > Windows Server Backup . The Windows Server Backup console is displayed in the working pane of the window.
The following backup options are available:
 - Local Backup—To perform a single backup or schedule a regular backup using the Backup Schedule Wizard or the Backup Once Wizard on your system.
NOTE: In Windows Server Backup, use the Recovery Wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.
 - Online Backup—To perform an online backup, register your system for the Windows Azure Online Backup. For more information, go to technet.microsoft.com/en-us/library/hh831419.aspx.

Selecting volumes to back up

To create a backup, 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 critical volumes (volumes containing OS files) if you only want to be able to recover the OS or system state.

Non-critical volumes

Back up individual volumes if you only want to be able to recover files, applications, or data from that volume.

Selecting a storage location

Consider the following storage type details when choosing a storage location for your backups.

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 select this option if you want to store a series of backups.

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 disk space is not supported.

Local hard disk

If you store your backup on an internal hard disk, you can:

- Recover files, folders, applications, and volumes.
- Perform system state and operating system recoveries if the backup used contains all the critical volumes.

However, you cannot perform an OS recovery if the backup is on the same physical disk as one or more critical volumes.

Storage Type

Details

Also, the local disk you select 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:

- Recover files, folders, applications, and volumes.
- Perform system state and operating system recoveries if the backup used contains all the critical volumes.
- Easily move backups offsite for disaster protection.

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.

using external hard disks allows you 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

2016. This feature

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 stops functioning.

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

Follow these steps to configure NIC teaming on a server.

About this task

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.

Steps

1. Start Server Manager, select Local Server.
The properties of Local Server is displayed.
2. Click the status next to NIC Teaming.
The NIC Teaming window is displayed.
3. In the 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, type a team name in the Team name box for the adapters to be added in.
6. In Additional properties, select Teaming Mode, Load balancing mode, Standby adapter, and then 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 newly created NIC team is displayed in this window.

Getting help

This section provides information about how to contact Dell EMC technical support, how to access information using the system QR code, and documentation resources available from Dell EMC.

Topics:

- Contacting Dell
- Locating your system service tag
- Accessing system information using the QRL
- Downloading drivers and firmware
- Documentation feedback

Contacting Dell

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 about 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 assistance, or customer service issues:

Steps

1. Go to Dell.com/support/home.
2. Select your country or region from the drop-down menu on the lower 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 and documentation:
 - 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.
5. For contact details of Dell Global Technical Support:
 - a. Go to Dell.com/support/incidents-online.
 - b. The Contact Technical Support page is displayed with details to call, chat, or e-mail the Dell EMC Global Technical Support team.

Locating your system service tag

You can identify your system using the unique Express Service Code and Service Tag. Pull out the information tag in front of the system to view the Express Service Code and Service 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.

Accessing system information using the QRL

You can use the Quick Resource Locator (QRL) to get immediate access to information about your system. The QRL is located on the top of the system cover and provides access to generic information about your system. To find information specific to your system, such as configuration and warranty, access the QR code located on the system Information tag.

Prerequisites







Ensure that your mobile device has a QR code scanner installed.

The QRL includes the following information about your system:

- How-to videos
- Reference materials, including the Installation and Service Manual, LCD diagnostics, and mechanical overview
- A direct link to Dell EMC to contact technical support and sales teams

Steps

1. Go to <https://QRL.dell.com> and Browse to your specific product or,
2. Use your mobile device to scan the QR code on your system or scan the applicable QR code below:

 <p>Quick Resource Locator</p> <p>www.dell.com/QRL/Storage/NX3330</p>	 <p>Quick Resource Locator</p> <p>www.dell.com/QRL/Storage/NX3340</p>
<p>NX3330</p>	<p>NX3340</p>
 <p>Quick Resource Locator</p> <p>www.dell.com/QRL/Storage/NX3230</p>	 <p>Quick Resource Locator</p> <p>www.dell.com/QRL/Storage/NX3240</p>
<p>NX3230</p>	<p>NX3240</p>
 <p>Quick Resource Locator</p> <p>www.Dell.com/QRL/Storage/NX430</p>	 <p>Quick Resource Locator</p> <p>www.dell.com/QRL/Storage/NX440</p>
<p>NX430</p>	<p>NX440</p>

Downloading drivers and firmware

Dell EMC recommends that you download and install the latest BIOS, drivers, and systems management firmware on your system.

Prerequisites

Ensure that you clear the web browser cache before downloading the drivers and firmware.

Steps

1. Go to www.dell.com/support/drivers.
2. In the Drivers & Downloads section, type the Service Tag of your system in the Service Tag or Express Service Code box, and then click Submit.

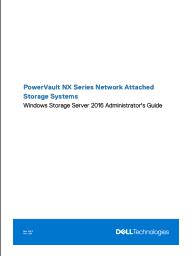


NOTE: If you do not have the Service Tag, select Detect My Product to allow the system to automatically detect your

Service Tag, or in General support, navigate to your product.

3. Click Drivers & Downloads.
The drivers that are applicable to your selection are displayed.
4. Download the drivers to a USB drive, CD, or DVD.

Documents / Resources

	<p>DELL EMC NX3340 PowerVault NX Series Network Attached Storage Systems [pdf] Installation Guide</p> <p>NX3340 PowerVault NX Series Network Attached Storage Systems, NX3340, PowerVault NX Series Network Attached Storage Systems, Network Attached Storage Systems, Attached Storage Systems, Storage Systems</p>
---	---

References

- [User Manual](#)