Deploy Network File System

Applies To: Windows Server 2012

Network File System (NFS) provides a file sharing solution that enables you to transfer files between computers running Windows Server 2012 and UNIX operating systems using the NFS protocol. This topic describe the steps you should follow to deploy NFS.

The following improvements are available for NFS in Windows Server 2012:

- **Support for NFS version 4.1**. This protocol version includes the following enhancements.
  - Navigating firewalls is easier which improves accessibility.
  - Supports the RPCSEC_GSS protocol which provides stronger security, and the ability for clients and servers to negotiate security.
  - Supports UNIX and Windows file semantics.
  - Takes advantage of clustered file server deployments.
  - Supports WAN friendly compound procedures.
- **NFS module for Windows PowerShell**. The availability of built-in NFS cmdlets makes it easier to automate various operations. The cmdlet names are consistent with other Windows PowerShell cmdlets (using verbs such as ‘Get’ and ‘Set’) which makes it easier for users familiar with Windows PowerShell to learn to use new cmdlets.
- **NFS management improvements**. A new centralized UI-based management console simplifies configuration and management of SMB and NFS shares, quotas, file screens and classification, in addition to managing clustered file servers.
- **Identity Mapping improvements**. New UI support and task-based Windows PowerShell cmdlets for configuring identity mapping, which allows administrators to quickly configure an identity mapping source, and then create individual mapped identities for users. Improvements make it easy for administrators to set up a share for multi-protocol access over both NFS and SMB.
- **Cluster resource model restructure**. This improvement brings consistency between the cluster resource model for the Windows NFS and SMB protocol servers and simplifies administration. For NFS servers that have many shares, the resource network and the

number of WMI calls required fail over a volume containing a large number of NFS shares are reduced.

- **Integration with Resume Key Manager**. The Resume Key Manager is a component that tracks file server and file system state and enables the Windows SMB and NFS protocol servers to fail over without disrupting clients or server applications that store their data on the file server. This improvement is a key component of the continuous availability capability of the file server running Windows Server 2012.

Scenarios for using Network File System

NFS supports a mixed environment of Windows-based and UNIX-based operating systems. The following deployment scenarios are examples of how you can deploy a continuously available Windows Server 2012 file server using NFS.

Provision file shares in heterogeneous environments

This scenario applies to organizations with heterogeneous environments that consist of both Windows and other operating systems, such as UNIX or Linux-based client computers. With this scenario, you can provide multi-protocol access to the same file share over both the SMB and NFS protocols. Typically, when you deploy a Windows file server in this scenario, you want to facilitate collaboration between users on Windows and UNIX-based computers. When a file share is configured, it is shared with both the SMB and NFS protocols, with Windows users accessing their files over the SMB protocol, and users on UNIX-based computers typically access their files over the NFS protocol.

For this scenario, you must have a valid identity mapping source configuration. Windows Server 2012 supports the following identity mapping stores:

- Mapping File

- Active Directory Domain Services (AD DS)

- RFC 2307 compliant LDAP stores such as Active Directory Lightweight Directory Services (AD LDS)

- User Name Mapping (UNM) server

Provision file shares in UNIX-based environments

In this scenario, Windows file servers are deployed in a predominantly UNIX-based environment to provide access to NFS file shares for UNIX-based client computers. An Unmapped UNIX User Access (UUUA) option was initially implemented for NFS shares in Windows Server 2008 R2 so that Windows servers can be used for storing NFS data without creating UNIX-to-Windows account mapping. UUUA allows administrators to quickly provision and deploy NFS without having to configure account mapping. When enabled for NFS, UUUA creates custom security identifiers (SIDs) to represent unmapped users. Mapped user accounts use standard Windows security identifiers (SIDs) and unmapped users use custom NFS SIDs.

System requirements

Server for NFS can be installed on any version of Windows Server 2012. You can use NFS with UNIX-based computers that are running an NFS server or NFS client if these NFS server and client implementations comply with one of the following protocol specifications:

1. NFS Version 4.1 Protocol Specification (as defined in RFC 5661)

2. NFS Version 3 Protocol Specification (as defined in RFC 1813)

3. NFS Version 2 Protocol Specification (as defined in RFC 1094)

Deploy NFS infrastructure

You need to deploy the following computers and connect them on a local area network (LAN):

- One or more computers running Windows Server 2012 on which you will install the two main Services for NFS components: Server for NFS and Client for NFS. You can install these components on the same computer or on different computers.

- One or more UNIX-based computers that are running NFS server and NFS client software. The UNIX-based computer that is running NFS server hosts an NFS file share or export, which is accessed by a computer that is running Windows Server 2012 as a client using Client for NFS. You can install NFS server and client software either in the same UNIX-based computer or on different UNIX-based computers, as desired.

- A domain controller running at the Windows Server 2008 R2 functional level. The domain controller provides user authentication information and mapping for the Windows environment.

- When a domain controller is not deployed, you can use a Network Information Service (NIS) server to provide user authentication information for the UNIX environment. Or, if you prefer, you can use Password and Group files that are stored on the computer that is running the User Name Mapping service.

Install Network File System

To install Network File System on the server using Server Manager:

1. From the Add Roles and Features Wizard, under Server Roles, select **File and Storage Services** if it has not already been installed.

2. Under **File and iSCSI Services**, select **File Server** and **Server for NFS**. Click **Add Features** to include selected NFS features.

3. Click **Install** to install the NFS components on the server.

To install Network File System on the server using Windows PowerShell:

1. Start Windows PowerShell. Right-click the PowerShell icon on the taskbar, and select **Run as Administrator**.

2. Run the following Windows PowerShell commands:

```
3. PS C:\> Import-Module ServerManager
4. PS C:\> Add-WindowsFeature FS-NFS-Services
5. PS C:\> Import-Module NFS
6.
```

Configure NFS authentication

When using the NFS version 4.1 and NFS version 3.0 protocols, you have the following authentication and security options.

RPCSEC_GSS:

- **Krb5**. Uses the Kerberos version 5 protocol to authenticate users before granting access to the file share.

- **Krb5i**. Uses Kerberos version 5 protocol to authenticate with integrity checking (checksums), which verifies that the data has not been altered.

- **Krb5p** Uses Kerberos version 5 protocol, which authenticates NFS traffic with encryption for privacy.

AUTH_SYS:

You can also choose not to use server authorization (AUTH_SYS), which gives you the option to enable unmapped user access. When using unmapped user access, you can specify to allow unmapped user access by UID / GID, which is the default, or allow anonymous access.

Instructions for configuring NFS authentication on discussed in the following section.

Create an NFS file share

You can create an NFS file share using either Server Manager or Windows PowerShell NFS cmdlets.

To create an NFS file share by using Server Manager

1. Log on to the server as a member of the local Administrators group.
2. Server Manager will start automatically. If it does not automatically start, click **Start**, type **servermanager.exe**, and then click **Server Manager**.
3. On the left, click **File and Storage Services**, and then click **Shares**.

4. Click **To create a file share, start the New Share Wizard**.
5. On the **Select Profile** page, select either **NFS Share – Quick** or **NFS Share - Advanced**, and click **Next**.
6. On the **Share Location** page, select a server and a volume, and click **Next**.
7. On the **Share Name** page, specify a name for the new share, and click **Next**.
8. On the **Authentication** page, specify the authentication method you want to use for this share.
9. On the **Share Permissions** page, click **Add**, and then specify the host, client group or netgroup you want to grant permission to the share.
10. In **Permissions**, configure the type of access control you want the users to have, and click **OK**.
11. On the **Confirmation** page, review your configuration, and click **Create** to create the NFS file share.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

On the server, type the following to configure an NFS file share (where `nfs1` is the name of the share and `C:\shares\nfsfolder` is the path):

```
New-NfsShare -name nfs1 -Path C:\shares\nfsfolder
```