DFS

Distributed File System or DFS as touched on in the introduction provides the ability to logically group shares found on multiple servers and to transparently link shares into a single hierarchical namespace. This is organized in a treelike structure. DFS supports multiple modes including both **stand-alone** and **domain-based** DFS services.

Usage of domain-based namespaces is required when you want to provide high availability of the namespace. As with other Microsoft technologies that are replicated along with Active Directory, with DFS, the topology data for a DFS namespace is stored in Active Directory.

DFS uses the Windows Server file replication service to copy changes between replicated targets. When users modify files stored on one target, DFS replication propagates the changes across to the other designated targets in the DFS infrastructure. The most recent changes are preserved.

DFS namespaces organized?

This is really up to the needs of the business. Common DFS organization may be related to the business organizational unit, the geographical location, combinations of both, or perhaps other custom business entities to define a DFS namespace.

What is included with the DFS topology data?

Components of the DFS tree structure include:

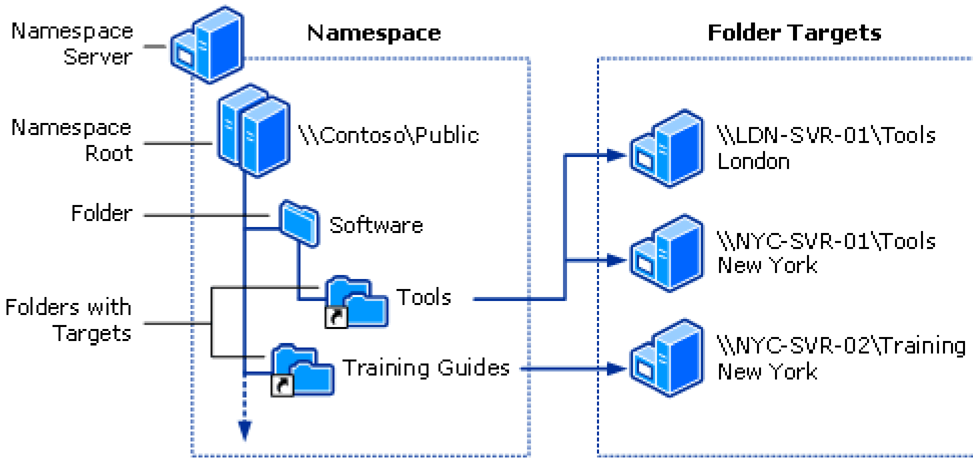
- **DFS Root** – This is a DFS server running the DFS service
- **DFS links** – DFS links point to network shares consolidated in DFS
- **DFS Targets** – The targets are the actual network shares the DFS links point to

The components making up a **DFS namespace** include the following:

- **Namespace server** – This is the DFS server that hosts a namespace. This can be a member server or a domain controller.
- **Namespace root** – This is the starting point of the DFS namespace tree. In the case of a domain-based DFS topology, it will start with the domain name. With domain-based DFS topologies, the DFS metadata is stored in Active Directory and replicated between

the ADDS servers. You can have multiple namespace servers hosting the DFS namespace.

- **Folder** – There are two types of folders in the DFS namespace – folders without targets and folders with targets. The folders without targets are simply for the organization of the structure. Folders with targets link to the actual content that end users can access.
- **Folder targets** – Folder targets are the actual UNC paths to a shared folder associated with the folder in a DFS namespace. The folder target is where data is actually found. The great thing about domain-based DFS namespaces, the DFS namespace is **Active Directory Site** aware. If a user in one geographic location accesses the same DFS namespace folder target, they will be directed to the server hosting the data in the same site which enhances the user experience and prevents unnecessary WAN traffic traversing across.



High-level overview of the DFS namespace components (Image courtesy of Microsoft)

Domain-based DFS Namespaces

There are a couple of use cases for using the domain-based DFS namespaces.

We have already touched briefly on why a domain-based DFS namespace would be beneficial, however, choose domain-based DFS namespaces for the following:

- **Is the high-availability for the DFS namespace needed?** Use domain-based in this case. By replicating the namespace between DFS namespace servers, HA is achieved.

- Domain-based DFS namespaces also provide a really easy way to abstract the underlying DFS server name by simply presenting the share in the \\< Domain Name >\namespace format. Coupled with Access-based Enumeration or ABE, users are only presented with the files in a namespace that they have access to.

To use the domain-based DFS namespace topology:

- Make sure your Active Directory forest functional level is Windows 2008 or higher
- Domain functional level needs to be at Windows Server 2008 or higher
- Namespace servers must be running Windows Server 2008 or higher

How Distributed File System (DFS) Works

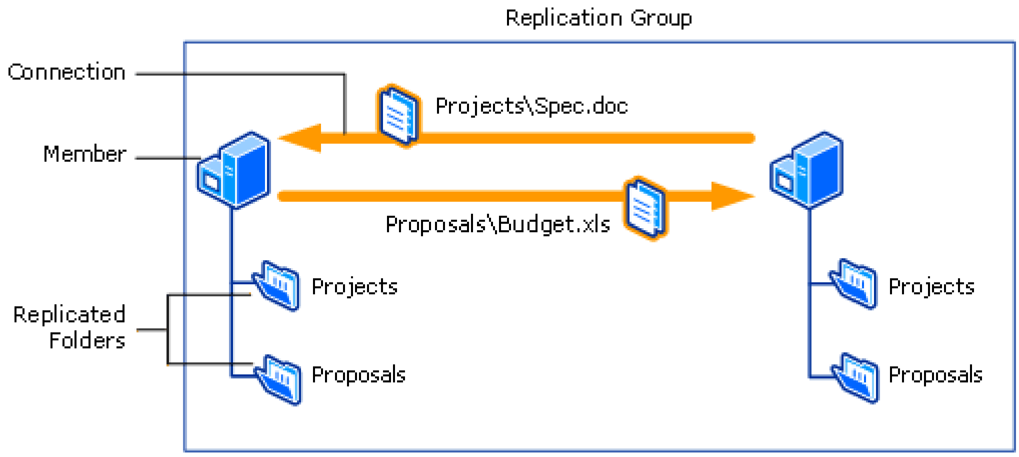
A key component to the DFS working is **DFS Replication**.

DFS Replication in Windows Server is a role service that allows replicating the folders referred to by a DFS namespace path across multiple servers and sites. DFS replication is configured as a **multi-master** replication technology meaning any member of the **DFS replication group** can make changes to the data.

DFS replication makes use of an efficient compression algorithm called **Remote Differential Compression** (RDC) to detect changes to data. RDC is extremely efficient in that it can detect changes to a file and only copy the **changed file blocks** instead of recopying the entire file.

A DFS replication group mentioned earlier is a group of servers that participates in the replication of one or more replicated folders. A replicated folder stays synchronized between the members included in the DFS replication group. The communication between the various DFS replication group members forms the DFS replication topology.

The settings for the replication group including its topology, schedule, and bandwidth throttling are applied to the replicated folders contained in the DFS replication group.



DFS Replication Group (Image courtesy of Microsoft)

Each replicated folder in the DFS replication group has unique settings including the file and subfolder filters to filter out different files and subfolders for each replicated folder. Replicated folder can be located on different volumes in the member and do not need to be shared folders or part of a namespace. DFS Replication can be managed by using the DFS Management console, DfsrAdmin and Dfsrdiag commands or scripts that call WMI.

DFS Installation

We'll immediately emphasize that the installation, as part of this example, will be performed on an already configured domain controller.

Open the server manager. In the main part of the window, click on "**Add Roles and Components**".

In the new window, go to the item "**Installation Type**", select the parameter "**Install Roles and Components**", click the button "**Next**".

In the updated window, select the current server and click on the button "**Next**".

The next step, in the list of available roles we find "**File Services and Storage Services**" and open the list in which you need to find "**File Services and iSCSI** Services". We also expand the list of parameters. We tick off "**DFS** Namespaces" and "**DFS** Replication". In the window that appears, click "**Add Components**". Press the button “**Next**” several times and wait for the installation to complete.

Creating a DFS Namespace

Before you start creating a DFS namespace, you must create at least one network directory on any of the servers in the domain. In our case, we will use the directory created on the same domain controller.

To make the folder accessible from the network, right-click on it, select "**Share**" in the context menu, then "**Separate people**".

In the input field, specify "**Users of the domain**", click the button "**Add**", then "**Share**".

Sharing the folder is ready. Click on the button "**Done**".

Now the server is available along the path: WINSERVER2019net_share

Create a DFS namespace.

To do this, select "**Windows Administration Tools**" in the menu "**Start**". It is also possible through **the control Panel→System and Security→Administration**.

In the window that opens, select "**DFS Management**".

In the new window "**DFS Management**", on the right side click on "**New namespace**...".

In the wizard window, specify the server name. It can be found both in the window that opens when you click the "**Browse**" button and in the system properties on the "**Computer Name**" tab. Click “Next”.

The next step is the namespace name. In our case, let it be "**MyDFS**." Press the button "**Change settings**...”.

In a new window, pay attention to the line "**Local path of the Local path of the shared folder**", if necessary, change it. In the same window, set the switch to the value "**Use user permissions**" and click the button "**Configure**".

In the window that opens, allow full access for everyone and click the button "**OK**".

Close the window for changing settings by clicking on the button “**OK**”, in the wizard window, click the button “**Next**”.

At the new stage of choosing the type of namespace, set the switch to the value "**Domain Namespace**", click the button "**Next**".

We carefully review the settings. Everything suits - click "**Create**".

Click the button "**Close**".

Add a new directory to the existing namespace

There is no sense in the above if you do not add directories to an existing namespace. In the example, the process will be executed on the same server, however, the method is applicable to all servers in the domain.

In the DFS control window, in its left part, expand the DFS control tree to an existing one, click on the necessary one. In the right part of the window, in the action section, select "**Create folder**...".

In the opened window “**Create Folder**” specify the name, in our case “**Test**” and click the button “**Add**”.

In the new window, add the path to the existing network folder. The list of available directories can be viewed by clicking on the button "**Overview**...". In the end, press the button "OK".

The result will be

Click “**OK**”.

Access to DFS can be obtained from any address bar (Start-> Run, or from the address bar of any folder) using the template:
<server_ domain name><DFS_space_name>

For example:
laa.testMyDFS

Configure DFS Replication

To perform data replication, you need to add a second server to the same domain and install the server role "**DFS Replication**" using the server manager.

On the same server, create a folder and allow shared access to it. Data from the directory located on the domain controller server will be replicated to this folder.

When you open access later, in the folder properties menu you can see the network path to the directory.

We return to the domain controller and the DFS namespace deployed on it. Open the window "**DFS Management**", already familiar from the examples above. In the left part of the window, expand the tree to the created namespace. In the right part of the window, select "**Add destination folder object**...". In the new window, enter the address to the shared directory on another server (which was created earlier). Press the button “ **OK** ”.

The system will ask if you want to create a replication group. Press the button “ **OK** ”.

We are waiting for the completion of the progress. The result will be an open window "**Folder Replication Wizard**". You must verify the name of the replication group, as well as the name of the directory that will be replicated. Go to the next step by clicking on the button "**Next**".

At this stage, we check the paths to network directories and click "**Next**".

The next step is to select the main node from the drop-down list. This is the node from which data will be replicated. In the case of the example, the primary member of the server replication named WINSERV2016 is the server on which the domain controller is raised. A specific example once again reminds us of the need to determine friendly names for servers and other network nodes. Click “**Next**”.

Now you have to choose the connection topology between replication members. We select the available one - “**Full grid**", however, if you want to create your replication topology later, then choose "**Notopology**”. Click “**Next**”.

The configuration is coming to an end and at this step, you should decide on the frequency of data replication. Choose the option with continuous replication. The advantages of this method are that the data will be duplicated immediately. The disadvantage is that it loads the local network with large amounts of information, as well as the load on the hard drive.

The second option offers to configure replication on a schedule. The disadvantage of this method is that the data will be synchronized “later”. Select the desired option and click "**Next**".

The program offers a view of the selected parameters. If everything suits you, click the "**Create**" button.

Click the button "**Close**".

The system will remind you of replication delays. In order not to receive this message again, if desired, check the box in the appropriate place. Press the button “ **OK** ”.

Distributed file system configuration, as well as data replication, can be considered complete.

Virtual Private Network (VPN)

Introduction

A virtual private network (VPN) extends a private network across a public network so that you will be able to access your data remotely through the public network securely. You can also use a VPN to secure your internet activity by using the VPN server as a proxy server.

Set up a PPTP VPN on Windows Server 2016

Follow these easy instructions to set up your own VPN server.

Prerequisites

You will need a Windows Server machine. We will be using a Windows Server 2016 as an example.

Step 1 Routing and Remote Access

First, start with installing and setting up Routing and Remote Access. We will add the required features with the help of Server Manager. Open server manager and navigate to Manage>Add Roles and Features.

We want to add Remote access so proceed with checking ”Remote Access” in the Server Roles tab.

We will need the VPN role as well as Routing. We will be able to configure an internal NAT to assign internal IP addresses. Check ”DirectAccess and VPN(RAS)” and “Routing” in the Role services tab.

Check and proceed to the installation by confirming on the next screen.

We can now start with the setup of Routing and Remote access. Go to Tools> Routing and Remote Access. And Right-click on your server name. This will open a menu where you can select ”Configure and Enabling Routing…..”

We will continue with Deploy VPN only this time to make this guide easy. Select “Deploy VPN only” in the new window

It’s important to select “Custom Configuration” in the next screen

We have now the option to select the services which we need. Select “VPN access” and ”NAT” and proceed.

Start the service and finish the setup. This can take a couple of minutes as the services are starting.

Step 2: Windows Firewall

It is possible that you will need to manually configure the Firewall. Please proceed if that’s the case Open Windows Firewall with Advanced Security and go to Inbound rules > New Rule and select Predefined: Routing and Remote Access

Check the boxing according to the connection type you will use. We will check all three of the connection types in this case as we will have multiple clients which will need each of them. But you can limit it depending on your use to make it more secure.

Select ”Allow Connection” and Finish to complete the setup of the firewall.

Step 3: Configuring the IP range

We will now configure the IP range which the server will assign to the incoming VPN clients.

Open the Routing and Remote Access in Server Manager> Tools >Routing and Remote Access and right-click on your server name and go to Properties.

Go the IPv4 tab and select ”Static address pool” as the type of IPv4 address assignment.

Add the range according to your needs. Each client will need his own IPv4 address. We will add a local range with 249 addresses. And click OK and OK to close the configuration

Step 4: Enable NAT

Configure the NAT to give your VPN clients internet access from the VPN. This is important if you want your users to be able to connect to the web. Right-click on NAT and add New Interface

Select your main external interface. This is the interface that is connected to the outbound network.

Check the following boxes to enable your clients to send and receive data using this interface.

Go to the ”Service and Ports” Tab and select the following services. These services are required for a working NAT.

Beware each time you select a service a windows will pop-up. Fill in the address field ” 127.0.0.1” and continue. This is the IPv4 address for your local network. You want to configure this was as this will enable your clients to use your VPN as the gateway.

Step 5: Configure access

You will need to grant access for your local user(s) so that VPN users can use this account to authenticate.

Open your Computer management and go to Local Users and Groups. Right-click >”your user” and go to Properties.

Go to the tab Dial-in a select “Allow Access”

Step 6: Testing

You can check if the configuration works within the server and by testing it. Open the Remote access Management console dashboard to see if all operation is up and running. You should see green icons next to the operations. Server Manager Tools &Remote access Management> Dashboard

Connect to the VPN with your local machine. In this case, we will connect using a Windows 10machine.

Go to Settings>Network &Internet> VPN > Add a VPN connection And fill in the form

Save it then select the connection and click connect and done. You can continue by adding a VPN connection to your client-side machine.

Install and configure the Network Policy Server (NPS)

Network Policy Server (NPS) for processing of connection requests that are sent by the VPN server:

- Perform authorization to verify that the user has permission to connect.
- Performing authentication to verify the user's identity.
- Performing accounting to log the aspects of the connection request that you chose when you configured RADIUS accounting in NPS.

Steps to configure:

1. In Server Manager, select **Manage**, then select **Add Roles and Features**. The Add Roles and Features Wizard opens.
2. In Before You Begin, select **Next**.
3. In Select Installation Type, ensure that **Role-Based or feature-based installation** is selected, and select **Next**.
4. In Select destination server, ensure that **Select a server from the server pool** is selected.
5. In Server Pool, ensure that the local computer is selected and select **Next**.
6. In Select Server Roles, in **Roles**, select **Network Policy and Access Services**. A dialog box opens asking if it should add features required for Network Policy and Access Services.
7. Select **Add Features**, then select **Next**
8. In Select features, select **Next**, and in Network Policy and Access Services, review the information provided, then select **Next**.
9. In Select role services, select **Network Policy Server**.
10. For features required for Network Policy Server, select **Add Features**, then select **Next**.
11. In Confirm installation selections, select **Restart the destination server automatically if required**.
12. Select **Yes** to confirm the selected, and then select **Install**.

The Installation progress page displays the status during the installation process. When the process completes, the message "Installation succeeded on *ComputerName*" is displayed, where *ComputerName* is the name of the computer upon which you installed Network Policy Server.

13. Select **Close**.

Configure NPS

After installing NPS, you configure NPS to handle all authentication, authorization, and accounting duties for connection request it receives from the VPN server.

Register the NPS Server in Active Directory

In this procedure, you register the server in Active Directory so that it has permission to access user account information while processing connection requests.

Procedure:

1. In Server Manager, select **Tools**, and then select **Network Policy Server**. The NPS console opens.
2. In the NPS console, right-click **NPS (Local)**, then select **Register server in Active Directory**.

   The Network Policy Server dialog box opens.

3. In the Network Policy Server dialog box, select **OK** twice.

For alternate methods of registering NPS, see Register an NPS Server in an Active Directory Domain.

Configure Network Policy Server Accounting

In this procedure, configure Network Policy Server Accounting using one of the following logging types:

- **Event logging**. Used primarily for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.

- **Logging user authentication and accounting requests to a local file**. Used primarily for connection analysis and billing purposes. Also used as a security investigation tool because it provides you with a method of tracking the activity of a malicious user after an attack. You can configure local file logging using the Accounting Configuration wizard.
- **Logging user authentication and accounting requests to a Microsoft SQL Server XML-compliant database**. Used to allow multiple servers running NPS to have one data source. Also provides the advantages of using a relational database. You can configure SQL Server logging by using the Accounting Configuration wizard.

To configure Network Policy Server Accounting, see Configure Network Policy Server Accounting.

Add the VPN Server as a RADIUS Client

In the Configure the Remote Access Server for Always On VPN section, you installed and configured your VPN server. During VPN server configuration, you added a RADIUS shared secret on the VPN server.

In this procedure, you use the same shared secret text string to configure the VPN server as a RADIUS client in NPS. Use the same text string that you used on the VPN server, or communication between the NPS server and VPN server fails.

Procedure:

1. On the NPS server, in the NPS console, double-click **RADIUS Clients and Servers**.
2. Right-click **RADIUS Clients** and select **New**. The New RADIUS Client dialog box opens.
3. Verify that the **Enable this RADIUS client** check box is selected.
4. In **Friendly name**, enter a display name for the VPN server.
5. In **Address (IP or DNS)**, enter the NAS IP address or FQDN.

   If you enter the FQDN, select **Verify** if you want to verify that the name is correct and maps to a valid IP address.

6. In **Shared secret**, do:
    1. Ensure that **Manual** is selected.
    2. Enter the strong text string that you also entered on the VPN server.
    3. Reenter the shared secret in Confirm shared secret.
7. Select **OK**. The VPN Server appears in the list of RADIUS clients configured on the NPS server.

Configure NPS as a RADIUS for VPN Connections

In this procedure, you configure NPS as a RADIUS server on your organization network. On the NPS, you must define a policy that allows only users in a specific group to access the Organization/Corporate network through the VPN Server - and then only when using a valid user certificate in a PEAP authentication request.

Procedure:

1. In the NPS console, in Standard Configuration, ensure that **RADIUS server for Dial-Up or VPN Connections** is selected.
2. Select **Configure VPN or Dial-Up**.

   The Configure VPN or Dial-Up wizard opens.

3. Select **Virtual Private Network (VPN) Connections**, and select **Next**.
4. In Specify Dial-Up or VPN Server, in RADIUS clients, select the name of the VPN Server that you added in the previous step. For example, if your VPN server NetBIOS name is RAS1, select **RAS1**.
5. Select **Next**.
6. In Configure Authentication Methods, complete the following steps:
    1. Clear the **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** check box.
    2. Select the **Extensible Authentication Protocol** check box to select it.
    3. In Type (based on the method of access and network configuration), select **Microsoft: Protected EAP (PEAP)**, then select **Configure**.

       The Edit Protected EAP Properties dialog box opens.

    4. Select **Remove** to remove the Secured Password (EAP-MSCHAP v2) EAP type.
    5. Select **Add**. The Add EAP dialog box opens.
    6. Select **Smart Card or other certificate**, then select **OK**.
    7. Select **OK** to close Edit Protected EAP Properties.
7. Select **Next**.
8. In Specify User Groups, complete the following steps:
    1. Select **Add**. The Select Users, Computers, Service Accounts, or Groups dialog box opens.
    2. Enter **VPN Users**, then select **OK**.
    3. Select **Next**.
9. In Specify IP Filters, select **Next**.
10. In Specify Encryption Settings, select **Next**. Do not make any changes.

    These settings apply only to Microsoft Point-to-Point Encryption (MPPE) connections, which this scenario doesn't support.

11. In Specify a Realm Name, select **Next**.
12. Select **Finish** to close the wizard.

Group Policy Management Console

This lesson will introduce you to the **Group Policy Management Console** (GPMC), which is an application used to centrally control many options and features of Windows operating systems using group policy objects (GPOs).

Defining the GPO

Imagine that you're setting up multiple new Windows computers at your workplace. There might be many required changes to the operating system, such as installing software and configuring the operating system (OS) and performing these processes for more than one computer is quite repetitive and uninteresting.

Doing everything manually will take quite a lot of time since there might be many things you have to change, depending on the purpose a computer will have in the organization. This lesson will show you a better, quicker, and easier way to manage multiple computers.

Rather than making the options change one by one, you can use **group policy objects** to specify the various changes for the computers. GPOs, aka group policies, are basically bundles of Windows settings managed by the Group Policy Management Console. They come in two flavors: computer settings and user settings. The difference is one applies to the system itself while the other applies to each user that logs on to the PC. GPOs rely on the **organizational unit** (OU), which is a collection of computers or users (or both) grouped together. OUs can be managed by the Active Directory Users and Computers utility or the GPMC itself.

Though you still have to install the OS and software and join each machine to the domain yourself (group policies can't do everything for you), the time savings will make GPOs quite useful.

Let's move on to showing you how to implement some centralized policies.

Creating the GPO With the GPMC

The Group Policy Management Console comes bundled with an Active Directory domain controller, which is where the centralized policies are actually stored (in the domain's SYSVOL share). Domain Admin credentials are also required to use it. Run the GPMC using the command gpmc.msc or from the Start Menu under the Windows Administrative Tools folder.

You can also install the Remote Server Administration Tools to enable the GPMC (and other admin utilities) on a client computer.

Create your first GPO by following these steps and pictures.

- Highlight the desired OU and right-click it. Then click on "Create a GPO in this domain and link it here" as shown in this image here.

- Give the new GPO a name.

- Right-click on the new GPO and select "Edit" so you can modify the settings that will be applied to computers in this OU.

- The GPMC editor opens. You can change both user and computer settings here.

- Disable the Windows Tips feature. Drill down in the Editor to the Cloud Content folder as shown. Here you can edit any settings presented in this window, though right now they are all "Not Configured."

- By double-clicking on the GPO, or right-clicking and selecting "Edit," the configuration window opens. Here you can change the status of a GPO and read about what it does. Let's enable this GPO.

- Exiting the GPO editor, the GPO is set to Enabled. Based on the description, setting this GPO to Enabled will disable Windows Tips.

Here are some example changes you can do with GPOs. You can specify computers in a particular OU to have a particular background image on the desktop. You can set every computer's browser homepage to your favourite search engine, just by adding a GPO to that effect in an OU with every computer added to it. You can even set a custom inactivity lockout or password change timer to protect the systems if you work at a security-conscious business. All of these examples and more are possible using the GPMC.