

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

This FAQ answers commonly asked questions about the Distributed File System (DFS) for the Windows Server 2003 family. For information about DFS Replication in Windows Server 2003 R2, see the DFS Replication Frequently Asked Questions on the Microsoft Web site. Click a question to view its answer. To view all the answers at one time, select the View all answers check box.

Defining DFS

Q. What is Distributed File System (DFS)?

A. Distributed File System (DFS) allows administrators to group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. A namespace provides numerous benefits, including increased availability of data, load sharing, and simplified data migration.

Q. What are the new DFS features in Windows Server 2003 Service Pack 1 (SP1)?

A. Changes to DFS in Windows Server 2003 SP1 are described in the document titled "Changes to Functionality in Microsoft Windows Server 2003 Service Pack 1". New features include DFS consolidation roots, target failback, target priority, and the ability to move and rename links. Improvements include better delegation and a change that allows the Time to Live value to expire without being refreshed in some clients. (See the question "How has the Time to Live (TTL) value for referrals changed in DFS clients running Windows XP with Service Pack 2 (SP2) and Windows Server 2003 with Service Pack 1 (SP1)?," below, for more details.)

Q. Where can I find more information about DFS?

A. The information provided in this article is covered in more detail in Chapter 2, "Designing and Deploying File Servers," of the Windows Server 2003 Deployment Kit. To download this book, see Windows Server 2003 Deployment Kit: Planning Server Deployments in the Microsoft Download Center. For technical information about DFS, see the DFS Technical Reference at the Microsoft Web site.

DFS Site Discovery and Target Selection

Q. What is DFS site discovery?

A. Site discovery, also called site awareness, is the process that DFS uses to determine which site a root target, link target, or client belongs to. A site is one or more TCP/IP subnets as defined in Active Directory. DFS uses this site information to determine the order in which to order the targets in a referral.

Detailed information about the site discovery process is described in the section "How Site Discovery Works" in the DFS Technical Reference.

Q. How does DFS target selection work?

A. In Windows Server 2003, DFS offers three methods of target selection: default target selection, restricted same-site target selection, and least expensive target selection (also called site-costing).

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

Default Target Selection

By default, DFS lists referrals in the following order:

- Link or root targets in the same site as that of the client. Within this set, DFS lists the targets randomly.
- Link or root targets in sites other than that of the client. Within this set, DFS lists the targets randomly.

Essentially, the client connects to a target in its site if a target is available. If no targets are available in the client's site, the client connects to a random target outside its site regardless of the bandwidth cost, connection speed, or the target server's processing load.

Restricted Same-site Target Selection

By using Dfsutil.exe with the /InSite parameter, you can limit client access to only those targets that are in the same site as the client. You enable this feature on a DFS root or on individual links in the namespace. If you enable this feature on the root, referrals for any link in the namespace return only targets that are in the same site as the client. If this functionality is disabled on the root, the individual settings on each link are used.

When using this feature, plan to have at least one target (or at least two targets, for fault tolerance) in every site, and plan to monitor servers to make sure they are online and accessible. If no same-site targets exist, clients in that site are denied access to the data in the namespace.

The /InSite parameter takes effect after you stop and restart the DFS service on each root server or when the service reads the DFS metadata, which happens every hour by default. Also, note that the /InSite parameter does not work for links that point to a domain-based DFS namespace (this type of link is known as an interlink). As a result, clients can access a target outside of the client's site if the interlink points to a domain-based DFS namespace.

Least Expensive Target Selection (Site-costing)

If you create a stand-alone or domain-based DFS root on a server running Windows Server 2003, and the domain controller acting as the Intersite Topology Generator (ISTG) is also running Windows Server 2003, you can use the /SiteCosting parameter in Dfsutil.exe to enable DFS to choose an alternate target based on connection cost if no same-site targets are available.

Windows Server 2003 uses the site and costing information in Active Directory to determine whether sites are linked by inexpensive, high-speed links or by expensive wide area network (WAN) links.

When site-costing is not available, the default target selection method is used instead as in the following situations:

- When a stand-alone DFS namespace is hosted on a server that is not part of any domain.
- When the root server is running Microsoft Windows 2000.
- When the closest domain controller acting as the ISTG is running Windows 2000 Server. This situation occurs when the only domain controllers running Windows 2000 Server are in

Distributed File System Frequently Asked Questions (Microsoft Corporation)

the site of the DFS root server, or when no domain controllers are in the site of the DFS root server, and the closest site with at least one domain controller has only Windows 2000 Server domain controllers in that site. The closest site is defined in Active Directory.

If you plan to enable site-costing, review the following factors:

- Site-costing is enabled on a per-namespace basis.
- The ISTG role is given automatically to the domain controller running Windows Server 2003 if domain controllers running Windows 2000 Server and Windows Server 2003 exist in a site.
- Site-costing is affected when you have a mix of root servers running Windows 2000 and Windows Server 2003.

Q. How do target selection and site discovery differ in Windows 2000 Server and Windows Server 2003?

A. Target selection in Windows 2000 Server is limited to default target selection and restricted same-site target selection, whereas Windows Server 2003 additionally supports least expensive target selection (site-costing).

Site discovery in Windows 2000 Server differs from site discovery in Windows Server 2003 in a number of ways:

- Root servers running Windows 2000 query the link target server to determine what site that target is in. Link target servers running Microsoft Windows NT 4.0 do not support this query and do not return a site name. Therefore, no site information is available for any link target on a server running Windows NT 4.0. Root servers running Windows Server 2003 use the IP address of the link target server to determine site membership, so Windows Server 2003 root servers can correctly determine the site membership of any DFS link target.
- In Windows 2000, DFS maintains static site information. After the site information for a particular target is known, DFS uses that information indefinitely, regardless of any changes to the site information of the target. If you move a target to another site, you must remove the target from the namespace, and then add it back to update the site information. To do this, see Knowledge Base article 260857, DFS Site Information Is Not Updated When You Move Server to a New Active Directory Site. In Windows Server 2003, if you move a target from one site to another, the site information for that target is updated within 25 hours.

Q. How do I enable least expensive target selection (site-costing) in DFS?

A. You use the command-line tool Dfsutil.exe that is included in the Windows Server 2003 Support Tools. Use the following syntax:

```
Dfsutil /Root:<DfsName> /SiteCosting /Enable
```

Distributed File System Frequently Asked Questions (Microsoft Corporation)

You can run this command from any computer running Windows XP or Windows Server 2003 where the Windows Server 2003 Support Tools are installed. For example, to enable least expensive target selection on the \\Contoso.com\Public namespace, at the command prompt type:
Dfsutil /Root:\\Contoso.com\Public /SiteCosting /Enable

For more information about using Dfsutil.exe, see the Windows Support Tools Help for Dfsutil.exe.

- Q. How does the RestrictAnonymous registry entry affect site discovery?
- A. Root servers that run Windows 2000 Server or Windows Server 2003 and that are not domain controllers cannot determine a DFS client computer's site when the restrictanonymous registry entry is set to 2 on domain controllers running Windows 2000 Server. (This registry entry is located at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet/Control/Lsa.) As a result, these DFS root servers sort targets in link referrals and root referrals randomly, regardless of the namespace type (stand-alone or domain-based), target selection method, or client operating system.

DFS Clients

- Q. When a DFS client running Windows XP attempts to open an executable (.exe) file from a DFS path, the user is prompted to confirm whether to run the executable file. Why does DFS require the user to confirm whether to run the file?
- A. Windows shell displays this message when you try to run an executable file from any path that includes a fully qualified domain name, regardless of whether the path is hosted by DFS. To prevent this message from occurring, add the domain to the list of trusted intranet zones on the client.
- Q. What can cause clients to be referred to unexpected targets?
- A. Even when least expensive or same-site target selection is enabled, clients might still access high-cost or out-of-site targets. Also, when default target selection is enabled, a client computer might access a target server outside of its own site, even though a same-site target exists. These problems are typically caused by one of the following situations:
- The same-site target is temporarily unavailable (due to server or network issues), and the client fails over to the next target, which could be outside of the client's site.
 - DFS uses the IP address-to-site mappings in Active Directory to determine the site of a target. If a target's IP address is not mapped to its current site, DFS cannot properly order that target in a referral. Incorrect site mappings can occur when subnets are not configured correctly or when a server or domain controller is moved to another site in the Active Directory Sites and Services snap-in, but the server's or domain controller's IP address still maps to the subnet of the previous site. Incorrect site mappings often occur when domain controllers are not moved to the site that corresponds to their IP address or when domain controllers are left in the default first site or the site where they originally belonged.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- If no same-site targets exist and a client unexpectedly chooses a high-cost target, it might be caused by an incorrect site cost setting.
- The client's IP address is not in a subnet that is defined in Active Directory and so DFS cannot obtain site information about the client.
- The target's IP address is not in a subnet that is defined in Active Directory and so DFS cannot obtain site information about the target.
- DNS lookup issues on the DFS root server are causing DNS name-to-IP address mappings to fail. The problem might be caused by DNS issues or when a server has multiple IP addresses but not all of those addresses are mapped to sites in Active Directory.
- The client is using a cached referral that has become outdated due to target change,, site changes, or both. For example, a target was added or removed from a link or root, or a target was moved from one site to another. The client will obtain an updated referral and after the referral expires, the client's cache is cleared (using the Dfsutil.exe /pktflush command), or the client is rebooted.
- Site information has changed, but the old site information is still cached on the root server or domain controller in the target site cache, client site cache, or site cost cache.
- The DFS object is not up-to-date when the root server polls a domain controller. This can be caused by Active Directory replication latency or failure.
- The Bridge all site links option is disabled. (This option is available in the Active Directory Sites and Services snap-in) Turning off Bridge all site links can affect the ability of DFS to refer client computers to target computers that have the least expensive connection cost. An Intersite Topology Generator that is running Windows Server 2003 relies on the Bridge all site links option being enabled to generate the intersite cost matrix that DFS requires for its site-costing functionality. If you turn off this option, you must create site links between the Active Directory sites for which you want DFS to calculate accurate site costs. Any sites that are not connected by site links will have the maximum possible cost. For more information about site link bridging, see Active Directory Replication Topology Technical Reference.
- Site awareness is not working correctly because the restrictanonymous registry entry located at HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa is set to two on Windows 2000 domain controllers. If this registry entry is set to two, DFS root servers that are not domain controllers (and are running either Windows 2000 Server or Windows Server 2003) randomly sort the targets in a referral, regardless of the namespace type (stand-alone or domain-based), target selection method, or client operating system.
- Domain controllers do not consistently provide site-costed SYSVOL referrals because the SiteCostedReferrals registry entry was not set on all domain controllers.

Q. Which clients can access DFS namespaces?

A. Clients running the following operating systems can access stand-alone and domain-based DFS

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

namespaces:

- Windows Server 2003 family
- Windows XP Professional family
- Windows 2000 Server family
- Windows 2000 Professional
- Windows NT Server 4.0 Service Pack 6a (SP6a)
- Windows NT Workstation 4.0 Service Pack 6a (SP6a)

The following operating systems have additional requirements for accessing DFS namespaces:

- Windows 98. The client for stand-alone DFS is included; install the Active Directory client extension for Windows 95 or Windows 98 to access domain-based DFS namespaces. The client extension is described in Knowledge Base article 323455, Directory Services Client Update for Windows 98.
- Windows Millennium Edition (Me). The client for stand-alone DFS is included. Because Windows Me is designed specifically for home use, no domain-based DFS client is provided.

Q. What is DFS client "stickiness"?

A. Client "stickiness" refers to the behavior that occurs after a client receives a refreshed referral after the current referral expires. DFS looks to see if the current active target is also in the new referral. If it is, the target is marked active in the new referral, and the client "sticks" to this target, even if more desirable (e.g., lower cost) targets appear in the new referral.

Client stickiness was designed into DFS for a purpose: to give end users a consistent experience as they read and write files on a target in the namespace. If the client computer were to connect to a different target each time the referral expired, the end user might see different files on the new target depending on whether replication has completed with respect to the previous target. In addition, any open handles to the previous target would be maintained (assuming Offline Files is not used), so clients could potentially access both targets while reading and writing different files.

In some situations, though, client stickiness is not desirable. For example, if a client fails over from a local server to a remote server (such as when the local server fails), the client will continue to access the remote server, even after the local server is restored. The new client failback functionality in Windows Server 2003 SP1 was designed to give administrators more control over failback, allowing them to configure clients to fail back to a local target after the client's referral expires. Handles to the remote server will still be maintained if Offline Files is not used, however, so this feature should only be used when the need for clients to access a local server outweighs the issues described earlier.

Stickiness is also an important consideration for laptop computers that are taken from one site to another and are frequently hibernated. When the laptop comes out of hibernation, it will prefer the active target from the previous site unless the laptop is rebooted or has its cache cleared using the `dfsutil /pkflush` command.

Q. How has the Time to Live (TTL) value for referrals changed in DFS clients running Windows XP

Distributed File System Frequently Asked Questions (Microsoft Corporation)

with Service Pack 2 (SP2) and Windows Server 2003 with Service Pack 1 (SP1)?

- A. For DFS clients that are not running Windows XP with SP2 or Windows Server 2003 with SP1, the Time to Live (TTL) value for referrals determines the earliest time that a client will request a new referral if the existing cached referral expires before it is accessed again. Clients that use a cached referral will renew the TTL value of the referral and, thus, use the referral indefinitely until the client's referral cache is cleared or the client is restarted.

This behavior has changed for clients running Windows XP with SP2 or Windows Server 2003 with SP1. Specifically, the TTL value is not renewed each time a client accesses a target using a cached referral. Instead, the referral expires after the TTL value lapses. One benefit of this change is that DFS clients running Windows XP with SP2 or Windows Server 2003 with SP1 will more quickly discover changes to links and roots. For example, if the link targets of a link named Current are changed daily, DFS clients without Windows XP with SP2 or Windows Server 2003 with SP1 would refresh the TTL value each time they access the Current link, causing them to continue to reference stale link targets well beyond the TTL value associated with the initial referral request.

This change has several effects:

- Clients running Windows XP with SP2 or Windows Server 2003 with SP1 will request referrals more frequently than other DFS clients, which can cause a moderately increased load on the domain-based DFS root servers, stand-alone root servers, and domain controllers.
- Because DFS clients running Windows XP with SP2 or Windows Server 2003 with SP1 request new referrals more frequently, they will discover namespace updates more quickly than other DFS clients that are not running Windows XP with SP2 or Windows Server 2003 with SP1.
- In terms of DFS failover, this new behavior can cause DFS clients to fail over to a new target if the previously active target is not in the new referral, such as when the namespace is changed to remove the target that the client had accessed.

DFS Limits

Q. What are the DFS size limits and recommendations for Windows Server 2003?

- A. The following table describes the DFS size limits and recommendations for Windows Server 2003.
DFS Size Limits and Recommendations

Microsoft Supported DFS, Offline Files, and FRS Deployments		
Description	Limit or Recommendation*	Explanation
Number of characters in path limit	Fewer than 260 characters	Win32 application programming interfaces (APIs)

Distributed File System Frequently Asked Questions (Microsoft Corporation)

		<p>have a maximum path limit of 260 characters.</p> <p>Applications fail when trying to access a namespace that goes beyond that limit. If the path length of a DFS namespace exceeds the Win32 API limit of 260 characters, users must map part of the namespace to a drive letter and access the longer namespace through the mapped drive letter.</p>
<p>Number of DFS roots per server running Windows Server 2003 Standard Edition</p>	<p>One, unless a hotfix is installed</p>	<p>Windows Server 2003 Standard Edition, is limited to one root per server. To create multiple domain-based namespaces on a server running Windows Server 2003 Standard Edition, install the hotfix described in article 903651 in the Microsoft Knowledge Base on the Microsoft Web site.</p>
<p>Number of DFS roots per server running Windows Server 2003 Enterprise Edition, or Windows Server 2003 Datacenter Edition</p>	<p>Varies</p>	<p>There is no limit to the number of DFS roots you can create on a server running Windows Server 2003 Enterprise Edition, or Windows Server 2003 Datacenter Edition. However, as you increase the number of roots per server, the DFS service</p>

Distributed File System Frequently Asked Questions (Microsoft Corporation)

		takes longer to start and uses more memory.
Number of root targets per domain-based DFS root	No fixed limit	If you do not enable root scalability mode, we recommend using 16 or fewer root targets to limit traffic to the server acting as the primary domain controller (PDC) emulator master.
Number of links per DFS namespace	<ul style="list-style-type: none"> • 5,000 for domain-based DFS • 50,000 links for stand-alone DFS 	When the number of links exceeds the recommended limit, you might experience performance degradation when making changes to the DFS configuration. For stand-alone DFS, namespace initialization after server startup might also be delayed.
Size of each DFS Active Directory object (applies to domain-based DFS namespaces only)	5 megabytes (MB)	The size of the DFS Active Directory object is determined by the number and path length of roots, links, comments, and targets in the namespace. We recommend using no more than 5,000 links in a domain-based namespace to prevent the DFS Active Directory object from exceeding 5 MB. Limiting the size of the Active Directory object is important because large

Distributed File System Frequently Asked Questions (Microsoft Corporation)

		domain-based DFS configurations can cause significantly increased network traffic originating from updates made to those roots, links, and targets.
Maximum amount of data that the File Replication service (FRS) can replicate in a domain-based DFS namespace	See recommended limits at http://support.microsoft.com/default.aspx?scid=kb;en-us;840675 .	It is important that you review the FRS design guidelines before enabling replication. See the chapter "Designing and Deploying File Servers," in the Microsoft Windows Server 2003 Deployment Kit. Doing so will help you optimally deploy and configure FRS for your environment.

* The figures in this table are based on information gathered in a test environment. The numbers in an operational DFS configuration might exceed the numbers described here and still provide acceptable performance.

Q. How many root servers can host a domain-based DFS namespace?

A. Use 16 or fewer root targets unless you enable root scalability mode by using the /RootScalability parameter in Dfsutil.exe. When root scalability mode is enabled, DFS root servers get updates from the closest domain controller instead of from the server acting as the primary domain controller (PDC) emulator master. As a result, root scalability mode reduces network traffic to the PDC emulator master at the expense of faster updates to all root servers. With this mode enabled, you can have as many root targets as you need, as long as the size of the DFS Active Directory object (for each root) is less than 5 MB.

Note that the PDC emulator master is not removed entirely from DFS operations. The PDC emulator master is still used as follows:

- When you make changes to the namespace, the changes are made on the PDC emulator master also, but the root servers no longer poll the PDC emulator master hourly for those changes. Instead, they poll the closest domain controller. If the root server is a domain controller, the root server uses itself as the source. If the root server is not a domain controller and is in the same site as the PDC emulator master, the root server treats the PDC emulator master as it would any other domain controller.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- When the DFS service starts on a root server, the DFS Active Directory object is accessed on the PDC emulator master. On the next polling interval, DFS accesses the closest domain controller, which might or might not be the PDC emulator master.

Do not use root scalability mode if any of the following conditions exist in your organization:

- Your namespace changes frequently, and users must have a consistent view of the namespace.
- Domain controller replication is slow. Slow replication increases the amount of time it takes for the PDC emulator master to replicate DFS changes to other domain controllers, which in turn replicate changes to the root servers. Until this replication is complete, the namespace remains inconsistent on all root servers.

Note: The number of root targets running Windows 2000 should be limited to 16 for any one namespace. After you enable root scalability mode in a namespace with root servers running Windows 2000 and Windows Server 2003, root servers running Windows 2000 Server still obtain updates from the PDC emulator master.

Q. How do I measure the size of an existing DFS namespace?

A. You can use the command-line tool Dfsutil.exe that is included in the Windows Server 2003 Support Tools. Use the following syntax:
Dfsutil /Root:\dfsname\root /View

Q. How can I work around the DFS size limits?

A. You can use the following methods:

- Keep comments to a minimum. When you add a root target or link target in the Distributed File System snap-in, you can enter comments that describe the target. If you plan to create a large namespace, use minimal comments, if any, because they can increase the overall size of the namespace.
- Create multiple namespaces. If you need to create more than 5,000 links in a domain-based DFS namespace, you can create multiple DFS namespaces that meet the recommended sizes, and then link them together. This method is often referred to as cascaded DFS, and links pointing to another namespace are often called interlinks. For more information, see the following question "What are the rules for using interlinks?"
- Enable root scalability mode. When root scalability mode is enabled, you can use more than 16 root targets. For more information, see "How many root servers can host a domain-based DFS namespace?"
- Migrate root servers running Windows 2000 Server to Windows Server 2003. Root servers running Windows Server 2003 do not add site information to the DFS Active Directory object. As a result, if all root servers run Windows Server 2003, DFS can store more root and link

Distributed File System Frequently Asked Questions (Microsoft Corporation)

information to the DFS Active Directory object before reaching the recommended 5-MB limit. After you migrate your Windows 2000 root servers to Windows Server 2003, you can remove the static site information from the DFS Active Directory object by using the /PurgeWin2kStaticSiteTable parameter in Dfsutil.exe.

Q. What are the rules for using interlinks?

A. Windows Server 2003 supports creating links that point to other DFS namespaces. This kind of link is often referred to as an interlink. Instead of specifying a shared folder as a link target, you can specify a DFS root or link within another namespace, allowing you to create a hierarchy of namespaces, also called a cascaded DFS. Linking to other namespaces is often done in the following scenarios:

- To increase DFS scalability. Organizations can combine the availability benefits of domain-based DFS namespaces with the scalability of stand-alone DFS namespaces. For example, if an organization needs to create 10,000 links but does not want to divide these between two domain-based DFS namespaces, the organization can take the following steps:
 - Create a stand-alone DFS namespace with 10,000 links.
 - Create a domain-based DFS root.
 - Under the domain-based DFS root, create a link that points to the stand-alone DFS namespace.
- To more easily delegate administration. If multiple groups within an organization want to manage their own namespaces, they can do so and still present a single cascaded DFS namespace to their users.

When linking to other namespaces, you must follow these guidelines to make certain that clients can be redirected properly if a target is unavailable:

- If you plan to specify a domain-based DFS namespace as a link target (either the root or a link within that namespace), you cannot specify alternate link targets. (Windows Server 2003 enforces this restriction.)
- If you plan to specify a stand-alone DFS namespace as a link target (either the root or a link within that namespace), you can specify alternate link targets to other stand-alone DFS paths. Do not specify domain-based DFS roots or shared folders as alternate targets.

Important: The DFS tools do not prohibit you from specifying domain-based DFS roots or shared folders as alternate targets. Therefore, follow these guidelines carefully.

When linking to other namespaces, review the following restrictions:

- A DFS path can consist of no more than eight hops through other DFS namespaces.
- Clients running Windows 98 might not correctly access links pointing to other DFS namespaces. Windows 98-based clients can only access the following types of links to other namespaces:

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- A link in a stand-alone DFS namespace that points to a stand-alone DFS root or link.
- A link in a domain-based DFS namespace that points to a stand-alone DFS root. This technique works only if the client has the latest Active Directory client installed, as described in Knowledge Base article 323466, "Availability of the Directory Services Client Update for Windows 95 and Windows 98."

Q. How can I estimate the size of each root and link in the DFS Active Directory object?

A. Each element in the namespace (root name, link name, target path, and comments) takes up space in the DFS Active Directory object. The amount of space can vary depending on the number of characters used in each element. The following formula assumes that each element is 10 characters:

- Root: Approximately 300 bytes
- Each root target: Approximately 150 bytes.
- Each link in the root: Approximately 320 bytes.
- Each link target: Approximately 120 bytes.

For example, if you create a root (300 bytes) with 3 root targets (150 bytes × 3) and then add 100 links (100 × 320 bytes) with each link having 3 link targets (100 × 120 bytes × 3), the DFS Active Directory object will be approximately 300 + (150 × 3) + (100 × 320) + (100 × 120 × 3) = 67 kilobytes (KB) in size.

Q. Can I create a DFS link to a printer?

A. No. This is not supported.

DFS Root Servers

Q. If I use multiple root targets in a domain-based DFS namespace, do I need to enable replication on the root?

A. No. DFS takes care of creating the necessary folder structures on each root target. In fact, we recommend against enabling replication on the root, although this step is sometimes done so that data stored in multiple root folders stays synchronized. Instead, it is better to store data in link targets and enable replication on links for the following reasons.

- When you enable replication on the root, morphed folders can occur under the DFS root folder. Morphed folders occur when two or more identically named folders on different servers are added to the replica tree. FRS identifies the conflict during replication, and the receiving member protects the original copy of the folder and renames (morphs) the later inbound copy of the folder. The morphed folder names have a suffix of "_NTFRS_XXXXXXX" where "XXXXXXX" represents eight random hexadecimal digits.

Morphed folders occur in replicated roots for the following reason: When you create a link in the namespace, DFS creates a link folder under each root folder on every root server. For

Distributed File System Frequently Asked Questions (Microsoft Corporation)

example, if you add 1,000 links to a namespace, DFS creates a link folder under the DFS root folder for each of those 1,000 links on every root server. When you enable FRS replication on the root, FRS attempts to replicate its local copy of the folder structure to every root server. Because each root server has a local copy of the same folder structure as the incoming changes, FRS identifies the duplicate folder names and renames the folders that were most recently created. FRS then replicates all morphed folders to all root targets in the replica set.

- When adding a new root target to an FRS replicated root, you cannot replicate the contents of individual folders in the root based on business priority. Instead, the entire contents of the root are replicated to the new root target. However, if you enable replication only on individual links, you are creating multiple replica sets, which allows you to enable replication on the most important links first, and then enable replication on the links in the namespace as desired.
- You cannot take individual root targets offline. For example, if you are adding a new root target, users who are referred to the new member might see incomplete data until replication is complete. However, if you enable replication on individual links, you can take a new link target offline while the initial replication takes place or whenever you want to restrict access to a particular link target.

Q. What DFS structures are stored locally on root servers?

A. Stand-alone and domain-based DFS root servers store DFS-related information in the registry. All root servers also store a copy of the namespace structure on a local volume on the server in DFS root folders and link folders as follows.

Root Folders

When you create a DFS root, you specify a shared folder to use as the root folder. The root folder is accessible on the local server, although we recommend that you keep the root folder as uncluttered as possible. For example, you might place in the root folder a single file such as a readme file, which describes the contents and purpose of the namespace.

Link Folders

When you add links to the root, DFS creates special folders under each root folder. These folders, called link folders, are actually reparse points, and they display the following error message if you try to access them on the local server:

```
E:\RootName\LinkName is not accessible. The network location cannot be reached.
```

Users who access the link folders from across the network are redirected to the appropriate link target.

If you include subfolders in your link names, such as Groups\Marketing, DFS creates the required subfolders that contain the link folder. For example, when you browse the namespace structure under E:\RootName on the local server, you can open the subfolder E:\RootName\Groups, but you cannot open the link folder E:\RootName\Groups\Marketing.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

Q. What are the hardware requirements for root servers?

A. When evaluating the hardware specifications of the servers that host DFS roots, note that clients access the root server to get referrals, and then the clients cache the referrals locally. Therefore, root servers do not typically experience high CPU usage. However, as the size of the namespace grows, the DFS service uses more memory, so consider using more than the minimum recommended RAM for servers that host large DFS namespaces and for servers that host multiple DFS namespaces.

Q. What are the factors to consider when hosting DFS roots on domain controllers?

A. When deciding whether to host a DFS root on a domain controller, consider the following factors:

- Only members of the Domain Admins group can manage a DFS namespace hosted on a domain controller.
- If you plan to use a domain controller to host a DFS root, the server hardware must be sized to handle the additional load. As described in the previous question, root servers that host large or multiple namespaces require additional memory.

Q. How do I decommission a root server that hosts a domain-based DFS root?

A. Use the following procedure to decommission a root server:

1. Remove the root server from the DFS namespace by using one of the following methods:
 - In the Distributed File System snap-in, right-click the root target you want to remove, and then click Remove Target.
 - Using the version of Dfsutil.exe included in the Windows Server 2003 Support Tools, run the following command, where RootTargetServer refers to the root server to be decommissioned:

```
Dfsutil /UnmapFtRoot /Root:<DFSName> /Server:RootTargetServer /Share:<Share>
```
2. On the decommissioned root target, remove DFS information from the registry by using the following Dfsutil.exe command:

```
Dfsutil /Clean /Server:RootTargetServer /Share:<RootName>
```
3. On the decommissioned root target, at the command prompt, type net stop dfs & net start dfs.

After you remove a root target, DFS stops giving referrals to the decommissioned server within 15 minutes of the update to the DFS Active Directory object on the local domain controller from the PDC emulator master. (This update can take time depending on Active Directory replication schedules.)

Q. How can I create multiple domain-based namespaces on a server running Windows Server 2003

Distributed File System Frequently Asked Questions (Microsoft Corporation)

Standard Edition?

- A. To create multiple domain-based namespaces on a server running Windows Server 2003 Standard Edition, install the hotfix described in article 903651 in the Microsoft Knowledge Base on the Microsoft Web site.

Managing DFS

Q. Can I disable the Distributed File System service on domain controllers?

A. No, this service is required to provide domain-based namespace referrals and SYSVOL referrals.

Q. What are best practices for setting permissions in namespaces?

A. Follow these guidelines:

- Use NTFS permissions to secure DFS targets. If you are using File Replication Service (FRS) to replicate DFS link targets, any NTFS permission changes you make on one member of the replica set replicate to other members. If you are not using FRS for automatic replication, you must set the NTFS permissions on targets and manually propagate any changes that occur. It is also important to set shared folder permissions identically on each target of a particular root or link. Otherwise, user access might be inconsistent depending on which target the client is referred to. Note that FRS does not replicate shared folder permissions, so you must apply or update them manually to each target.
- Set NTFS and shared folder permissions for root targets identically on all root servers. This is especially important to remember to do when you add new root targets to an existing namespace.
- When setting NTFS permissions, always use the path of the physical folder instead of navigating through the DFS namespace to set permissions. This is especially important when you have multiple link targets for a given link. Setting permissions on a folder by using its DFS path can cause the folder to inherit permissions from its parent folder in the namespace. In addition, if there are multiple link targets, only one of them gets its permissions updated when you use the DFS path.

Q. What permissions are required to manage a namespace? How can I delegate authority to manage a DFS namespace?

A. The following table describes the permissions required to administer DFS namespaces.
Permissions or Group Memberships Required to Administer DFS Namespaces

Task	Permissions or Group Membership Required
Creating or removing a domain-based DFS root on a member server	One of the following: <ul style="list-style-type: none">• Membership in the Domain Admins group• Full Control permission on the DFS-Configuration container in Active

Distributed File System Frequently Asked Questions (Microsoft Corporation)

	Directory and membership in the local Administrators group on the root server
Adding or removing a root target from an existing domain-based DFS root on a member server	One of the following: <ul style="list-style-type: none"> • Membership in the Domain Admins group • Full Control permission on the DFS-Configuration container in Active Directory and membership in the local Administrators group on the root server
Creating or deleting a stand-alone DFS root on a member server	Membership in the local Administrators group on the root server
Adding a link to a domain-based DFS namespace or adding a target to an existing link on a member server	Membership in the local Administrators group on each of the root target servers.*
Removing a link from a domain-based DFS namespace or removing a target from an existing link on a member server	Membership in the local Administrators group on each of the root target servers.*
Changing root-related or link-related information, such as comments, referral status, and cache limits on a member server	Membership in the local Administrators group on each of the root target server.*
Using the following parameters in Dfsutil.exe, a Windows Support Tool: /RenameFtRoot /UnmapFtRoot /Insite /SiteCosting /RootScalability /UpdateWin2kStaticSiteTable /PurgeWin2kStaticSiteTable	One of the following: <ul style="list-style-type: none"> • Membership in the Domain Admins group. • Full Control permission on the DFS-Configuration container in Active Directory and membership in the local Administrators group on the root server.
Enabling replication on links in a domain-based DFS namespace	Membership in the Domain Admins group
Performing any of the tasks in this table on a domain controller	Membership in the Domain Admins group

*To ensure that the administrator can reliably administer the namespace, we recommend that the administrator be a member of the local Administrators group on each root server. If a DFS administration tool sends a request to a root server on which the administrator is not a member of the local Administrators group, the request will fail. If the administrator is a member of the local Administrators group on some but not all root servers, the administrator's ability to administer the namespace will be inconsistent.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

The procedures below can be used to allow members of the local Administrators group on each root server to create and manage domain-based DFS namespaces.

To grant a selected user the ability to create new DFS namespaces as well as administer existing ones, do the following:

1. Verify that the user is a member of the local Administrators group on all root servers for namespaces that the user will administer, or add the user if necessary.
2. In the Active Directory Users and Computers snap-in, on the View menu, click Advanced Features.
3. In the console tree, double-click the System folder to expand it.
4. Click the DFS-Configuration folder. Any existing root objects appear in the details pane.
5. Right-click DFS-Configuration, and then click Properties.
6. On the Security tab, click Add.
7. Type the name of the user who will administer all domain-based DFS namespaces, and then click OK.
8. Select the Full Control permission, and then click OK.

To allow a user to administer only within a single DFS namespace, do the following:

1. Verify that the user is a member of the local Administrators group on all root servers for the namespace that the user will administer, or add the user if necessary.
2. In the Active Directory Users and Computers snap-in, on the View menu, click Advanced Features.
3. In the console tree, double-click the System folder to expand it.
4. Click the DFS-Configuration folder. Any existing root objects appear in the details pane.
5. Right-click the root object that you want to allow the user to administer, and then click Properties.
6. On the Security tab, click Add.
7. Type the name of the user, and then click OK.
8. Verify that the user is granted the Full Control permission, and then click OK.

Q. What tools do I use to manage DFS namespaces?

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

- A. Three tools are used for managing DFS namespaces: the Distributed File System snap-in, dfscmd.exe, and dfsutil.exe.

Distributed File System Snap-in

The Distributed File System snap-in is available in Windows Server 2003 in the Administrative Tools folder. This snap-in provides a graphical user interface for configuring namespaces and is the only tool available for enabling FRS replication in DFS namespaces.

The Distributed File System snap-in is also part of the Windows Server 2003 Administration Tools Pack; you can install this pack on computers running Windows XP Service Pack 1 (SP1) or later and create FRS schedules and topologies on remote servers running Windows 2000 and Windows Server 2003. For more information, see Administering Windows Server-based Computers Using Windows XP Professional-based Clients.

Dfscmd.exe

The Dfscmd.exe command-line tool is available in Windows Server 2003. Use Dfscmd.exe for basic DFS tasks, such as creating links, adding and removing link targets, and viewing the namespace. For more information about Dfscmd.exe, in Help and Support Center for Windows Server 2003 click Tools, and then click Command-line reference A-Z.

Dfsutil.exe

The Dfsutil.exe command-line tool is a Windows Support Tool. You can install Dfsutil.exe from the \Support\Tools folder on the Windows Server 2003 operating system CD. Dfsutil.exe provides extensive features for configuring and managing DFS, including those that are not available in the Distributed File System snap-in, such as root scalability mode and least expensive target selection (site-costing).

For more information about Dfsutil.exe, in Help and Support Center for Windows Server 2003, click Tools, and then click Windows Support Tools.

- Q. How do I back up and restore a DFS namespace or move a DFS namespace from one server to another?
- A. You can use Dfsutil.exe to export the namespace from the source server, and then optionally restore the namespace to a destination server.

In the following example, an administrator wants to migrate the following namespaces on different servers to a single server running Windows Server 2003 Enterprise Edition:

- \\NT4SVR\Marketing (a stand-alone DFS root on a server running Windows NT Server 4.0)
- \\W2KSVR\Public (a stand-alone DFS root on a server running Windows 2000 Server)

First, the administrator creates the following stand-alone DFS roots on the server running Windows Server 2003 Enterprise Edition:

- \\2003SVR\Marketing
- \\2003SVR\Public

Next, the administrator installs Windows Support Tools from the Windows Server 2003 operating system CD, and then uses the Dfsutil.exe tool to run the following commands:

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- Dfsutil /Root:\\NT4SVR\Marketing /export:Nt4.txt
- Dfsutil /Root:\\W2KSVR\Public /export:w2k.txt

Finally, the administrator runs the following commands to import the namespaces onto the server running Windows Server 2003 Enterprise Edition:

- Dfsutil /Root:\\2003SVR\Marketing /import:Nt4.txt /set
- Dfsutil /Root:\\2003SVR\Public /import:w2k.txt /set

Q. How do I delete a link folder?

A. If you used a DFS tool to delete a link, yet the link folder still remains, you cannot delete it using traditional methods (such as by using Windows Explorer) because a reparse point is set on the folder. Morphed link folders that are created when File Replication service (FRS) is enabled on the root also have reparse points. To delete the reparse point from a particular link folder, use the following command to view all link folders on a volume:

```
dfsutil /viewdfsdirs:driveletter: /verbose
```

Identify the link folder whose reparse point you want to remove and then use the following command:

```
fsutil reparsepoint delete linkfolderpath
```

After you delete the reparse point, you can delete the link folder.

Q. Can I use DFS to selectively hide folders from users who are not authorized to access the folders?

A. No, DFS does not support this functionality.

Q. Can I use DFS with Offline Files and redirected My Documents folders?

A. Using DFS, roaming profiles, Offline Files, redirected My Documents, and FRS is supported in the following scenarios (see below for the corresponding number references):

Microsoft Supported DFS, Offline Files, and FRS Deployments					
Scenario	Client Operating System	DFS Only	DFS and Offline Files	DFS and FRS	DFS, Offline Folders, and FRS
Roaming Profiles	Windows NT 4.0	N/A(1)	N/A(2)	N/A(1)	N/A(2)
Roaming Profiles	Windows 2000	Yes(3)	No(4,8)	No(5)	No(4,5,8)
Roaming	Windows	Yes(3)	No(8)	No(5)	No(5,8)

Distributed File System Frequently Asked Questions (Microsoft Corporation)

Profiles	Server 2003				
Roaming Profiles	Windows XP	Yes(3)	No(8)	No(5)	No(5,8)
Redirected My Documents	Windows NT 4.0	Yes	N/A(2)	No(6)	N/A(2)
Redirected My Documents	Windows 2000	Yes	No(8)	Not recommended(7)	No(8)
Redirected My Documents	Windows Server 2003	Yes	Yes(9)	Not recommended(7)	Not recommended(7,9)
Redirected My Documents	Windows XP	Yes	Yes(9)	Not recommended(7)	Not recommended(7,9)
Collaboration Shared Folder	Windows NT 4.0	Yes	N/A(2)	Depends(10)	N/A(2)
Collaboration Shared Folder	Windows 2000	Yes	No(8)	Depends(10)	No(8)
Collaboration Shared Folder	Windows Server 2003	Yes	Yes(9)	Depends(10)	Yes(9,10)
Collaboration Shared Folder	Windows XP	Yes	Yes(9)	Depends(10)	Yes(9,10)
Publishing Shared Folders	Windows NT 4.0	Yes	N/A(2)	Yes	N/A(2)
Publishing Shared Folder	Windows 2000	Yes	No(8)	Yes	No(8)
Publishing Shared Folder	Windows Server 2003	Yes	Yes(9)	Yes	Yes(9)
Publishing Shared Folder	Windows XP	Yes	Yes(9)	Yes	Yes(9)

1. Windows NT 4.0 profiles are stored in the user's MyDocuments directory.
2. The Offline Files feature is not available in Windows NT 4.0.
3. If the DFS root is a stand-alone root in a remote site, or a domain-based root with no local targets, the profile might fail to load. To work around this issue, disable slow link detection or install a redundant root target at each client site. For more information, see Knowledge Base article 830856, A roaming profile is not loaded from a DFS share.
4. Roaming profiles should not be enabled for Offline Files. For more information, see Knowledge Base article 287566, The Cache Option for Offline Files Must Be Disabled on

Distributed File System Frequently Asked Questions (Microsoft Corporation)

Roaming User Profile Shares.

5. Roaming profiles that are replicated via FRS to multiple link targets might lead to data loss (due to FRS conflict resolution) if a user logs in to multiple workstations, makes changes to the same file on different targets, and then logs off both workstations.
6. Windows NT 4.0 profiles are stored in the user's MyDocuments directory. This is equivalent to issue 5.
7. If there is replication latency between link targets, the users' data might be out-of-date on the other link target, causing users to be confused if they ever fail over to another link target.
8. Enabling Offline Files on DFS link targets is only supported on client computers running Windows XP and Windows Server 2003. For more information, see Knowledge Base article 262845, Support for DFS-Based Shares for Offline Files.
9. Administrators must not enable Offline Files on a path with the same first component as a path used for roaming profiles. For example, if roaming profiles are stored on a domain root named \\Domain\Roam, Offline Files should not be enabled for a DFS root named \\Domain\Project. Similarly, if roaming profiles are stored on a stand-alone root or regular shared folder, such as \\Server\Roam, Offline Files should not be enabled for a path such as \\Server\Other.

Offline Files treats the first component of the path name as if it were a server and caches everything under that "server." In the \\Domain\Roam and \\Domain\Project example above, enabling Offline Files for \\Domain\Project would result in the roaming profiles being cached by Offline Files as well.

10. FRS does not provide distributed file locking. Depending on the update patterns of users, the lack of distributed locking might cause one user's update to override another user's update. If the collaboration is such that end users are not writing to the same files simultaneously, this most likely would not be an issue.

Q. What tools should I use to manage DFS when I have root servers that run Windows 2000 Server and Windows Server 2003?

A. Use the Distributed File System snap-in available in Windows Server 2003. This version of the Distributed File System snap-in is also part of the Windows Server 2003 Administration Tools Pack; you can install this pack on computers running Windows XP with Service Pack 1 (SP1) or later. For more information, see Knowledge Base article Administering Windows 2000-Based and Windows Server 2003-Based Computers Using Windows XP Professional-Based Clients.

Use the version of Dfsutil.exe that shipped in Windows Server 2003 Support Tools for command-line administration of Windows Server 2003 DFS. Use the version of Dfsutil.exe that shipped in the Windows 2000 Resource Kit for command-line administration of Windows 2000 DFS.

Q. What are the issues to consider when I use multiple servers running Windows 2000 Server and Windows Server 2003 to host a domain-based DFS root?

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- A. DFS handles site information in each of these operating systems differently. Windows Server 2003 family operating systems do not store site information in the DFS Active Directory object; instead, root servers running Windows Server 2003 obtain site information directly from Active Directory.

By contrast, if you have root servers running Windows 2000 Server, those servers try to obtain site information from the DFS Active Directory object. Unless you use the version of Dfsutil.exe included in the Windows Server 2003 Support Tools to manually update the site information in the DFS Active Directory object, the root servers running Windows 2000 Server might provide referrals (based on old site information) that lead to a target outside of the client's site.

The following table describes how DFS root servers handle site information.

How Root Servers Handle Site Information		
Site Aspect	Windows 2000 Server	Windows Server 2003
Where DFS stores and retrieves site information for root and link targets	DFS stores a copy of site information for root and link targets in the DFS object in Active Directory.	DFS uses IP addresses of root and link targets to obtain site information directly from Active Directory. By default, DFS does not store site information in the Active Directory object.
Characteristic of site information	Static	Dynamic
Method for updating site information after moving a link target to a different site	Remove the link target from the namespace, and then add it back.	By default, site information is updated automatically every 25 hours.
How root servers use site information for referrals	Root servers running Windows 2000 Server use the link target's site information only if the link target was created by using a DFS tool in Windows 2000 Server. If the link target was created by using a DFS tool in Windows Server 2003, no site information is stored. As a result, a referral from a Windows 2000 root server could lead to a target outside of the client's site.	Root servers running Windows Server 2003 ignore any site information in the Active Directory object. Instead, they use site information directly from Active Directory.

We recommend running Windows Server 2003 on every root server for a number of reasons:

- Site information is always up-to-date, because DFS obtains site information directly from Active Directory instead of storing a copy of site information in the DFS Active Directory object.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- The DFS Active Directory object can hold additional root and link targets, because it does not contain site information.

If you want referrals from root servers running Windows 2000 Server to be ordered according to site information, you can use the /UpdateWin2kStaticSiteTable parameter in the Windows Server 2003 version of Dfsutil.exe to update the static site information for all root and link targets in the DFS Active Directory object. If you plan to use this parameter, review the following information:

- Using this parameter increases the size of the DFS Active Directory object, possibly making it exceed the 5-MB recommended size limit.
- You need to run this parameter each time one or more of the following tasks is performed:
 - A new root target, new link, or a new link target for an existing link is added to the namespace.
 - A link target server is moved from one site to another.
 - Site information of root targets or link targets is changed in Active Directory.

When all root servers are running Windows Server 2003, you can use the /PurgeWin2kStaticSiteTable parameter in Dfsutil.exe to remove site information from the DFS Active Directory object, providing you with additional space for creating root and link targets.

- Q. Is it a best practice to configure one-way File Replication Service (FRS) replication between DFS link targets?
- A. Yes, FRS does support one-way replication between link targets. However, you must be aware of the following caveats for using one-way replication:
- To keep the content on all link targets consistent, you must ensure that no changes occur on any servers without outbound FRS connections, because those changes will not be replicated to other servers. In addition, FRS will not update the modified files with changes made on other servers. For example, if Server1 has no outbound connections, and someone changes File1.doc on Server1, the updated version of File1.doc is never replicated to another server. If someone later makes a change to File1.doc on Server2, those changes will not be applied to File1.doc on Server1. To prevent this occurrence, we recommend that you set up share permissions to prevent users from making changes and advise administrators who log on locally to the server to avoid making changes to the files.
 - Servers without outbound connections will still create change orders in their outbound logs for changes they receive. These change orders and their associated staging files will be kept for seven days by default. You can adjust this duration by modifying the "Outlog Change History In Minutes" registry entry. To do this, see the Microsoft Knowledge Base article 221111, Description of FRS entries in the registry.
 - When setting up one-way replication, use the following best practices:
 - Make sure you select the desired initial master in the Configure Replication wizard. The initial master's files will be replicated to the other members.

Distributed File System Frequently Asked Questions (Microsoft Corporation)

- Create a two-way replication topology first, and then remove connections as needed to set up one-way replication between two members.
- Make inbound-only replica link targets read-only and warn administrators about modifying content in inbound-only link targets. Do not provide links to read/write shares to clients.
- Configure outlog retention on inbound-only servers.

Q. Can DFS and FRS be used in collaboration scenarios where multiple users might change files at the same time?

A. This is not advised because FRS does not provide distributed file locking. Depending on the update patterns of users, the lack of distributed locking might cause one user's update to override another user's update. If the collaboration is such that end users are not writing to the same files simultaneously, this most likely would not be an issue.

Q. Can I use access-based enumeration (ABE) in a DFS environment?

A. Yes, for instructions, see article 907458 in the Microsoft Knowledge Base. For more information about access-based enumeration, see Windows Server 2003 Access-based Enumeration and Windows Server 2003 Access-based Enumeration Tools.

Q.

A.

Domain and Forest Issues

Q. Can I host a domain-based DFS namespace in multiple domains?

A. No. All root targets for a given domain-based DFS root must be in the same domain.

Q. How does DFS work across domains and forests?

A. DFS clients periodically discover new domains in the local forest and in trusted forests. This discovery process, which occurs every 15 minutes by default, runs against a domain controller from the domain that hosts the client's computer account. To avoid real-time queries to domain controllers in the domain, the referrals received during the discovery process are stored in a special table, called the domain cache or SPC cache. As a result of this process, clients can more quickly distinguish queries for fully qualified domain names from fully qualified computer names.

To determine the domains and forests in which a client can access domain-based namespaces, you can view the domain cache on a client computer by using the Dfsutil.exe command-line tool with the /spcinfo parameter. The following text illustrates the output displayed when you use this command.

```
[*][dc-01.contoso.com]
[*][CONTOSO]
[*][contoso.com]
[+][contoso.com]
```

Distributed File System Frequently Asked Questions (Microsoft Corporation)

```
[-dc-02.contoso.com]
[+dc-01.contoso.com]
[-dc-04.contoso.com]
[-dc-03.contoso.com]
[-][AFRICA]
[-][EUROPE]
[+][CONTOSO]
[-DC-02]
[+DC-01]
[-DC-03]
[-DC-04]
[-][europe.contoso.com]
[-][africa.contoso.com]
```

The preceding sample output can be interpreted as follows:

- Entries preceded by [*] are provided by the Workstation service.
- The [+] next to the domain controller named DC-01 under [contoso.com] and [CONTOSO] indicates that it is the active domain controller for that domain. The client will contact this domain controller as needed to obtain domain name referrals, domain controller referrals, and domain-based root referrals.
- The client has already contacted DC-01 to receive domain name referrals for Contoso.com, Europe.Contoso.com, and Africa.Contoso.com.
- The client has already contacted DC-01 to receive domain controller referrals for the Contoso.com domain.

If an organization has a large number of trusted domains and forests, it is possible that clients will not be able to access all domain-based namespaces within the trusted domains and forests. This limitation can occur when the list of trusted domains and forests is too large to fit in the client's buffer. By default, DFS clients send a 4-KB (2,048 Unicode character) buffer to a domain controller when requesting domain name referrals. If the list of domains is too large to fit into the 4-KB buffer, DFS clients automatically increase their buffer size to accept the list of domains, up to a maximum of 56 KB.

If the list of domains exceeds 56 KB, DFS puts as many domains in the buffer as it can until the buffer reaches 56 KB. DFS then writes an entry with the ID 14536 in the system event log of the domain controller that provided the domain referral. When populating the buffer, DFS gives preference to local and explicitly trusted domains by filling the buffer with their names first. Consequently, by creating explicit trust relationships with domains that host important DFS namespaces, you can minimize the possibility that those domain names might be dropped from the list that is returned to the client.

When populating the cache, DFS gives preference to local and explicitly trusted domains by filling the cache with their names first. Consequently, by creating explicit trust relationships with domains that host important DFS namespaces, you can minimize the possibility that those domain names might be dropped from the list that is returned to the client.

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

Important: To make sure that clients can access link targets in other trusted domains or trusted forests, you must use DNS names for all link targets and configure DFS to use fully qualified domain names in referrals. For more information, see [How to Configure DFS to Use Fully Qualified Domain Names in Referrals](#).

Q. Can I enable FRS replication on a DFS link whose targets are in different domains?

A. Yes, if you are a member of the Enterprise Admins group, you can configure FRS replication on a DFS link whose targets are in different domains in the same forest. If you are not a member of the Enterprise Admins group, permissions must be configured as follows:

- You must have Read and Create All Child Objects permissions for the computer object of each computer that will be part of the replica set.
- You must be a member of the local Administrators group on each computer that will be part of the replica set.
- You must have Read and Create All Child Objects permissions for the File Replication Service container and all its child objects. Although the File Replication Service container can exist in every domain, you must add these permissions to the File Replication Service container that is in the domain where the domain-based root is configured.

If any of these permissions are not configured correctly, you will get an Access Denied message when you try to enable replication by using the Configure Replication Wizard in the Distributed File System snap-in.

For more information, see article 296183, [Overview of Active Directory Objects That Are Used by FRS](#).

DFS Availability

Q. How do I ensure the availability of a DFS namespace?

A. The answer depends on type of namespace: stand-alone or domain-based.

For stand-alone DFS namespaces, you ensure the availability of a stand-alone DFS root by creating it on the cluster storage of a clustered file server by using the Cluster Administrator snap-in.

For domain-based DFS namespaces, you ensure the availability of domain-based DFS roots by creating multiple root targets on nonclustered file servers or on the local storage of the nodes of server clusters. (Domain-based DFS roots cannot be created on cluster storage.) All root targets must belong to the same domain. To create root targets, use the Distributed File System snap-in or the Dfsutil.exe command-line tool.

To ensure the availability of domain-based DFS roots, you must have at least two domain controllers and two root targets within the domain that is hosting the root. If you have only one domain controller and it becomes unavailable, the namespace is inaccessible. Similarly, if you have only a single root target, and the server hosting the root target is unavailable, the namespace is also unavailable.

Q. How do I increase the availability of data in link targets?

Distributed File System Frequently Asked Questions

(Microsoft Corporation)

A. There are two ways to increase the availability of data in link targets:

- Create a single link that points to a link target on a clustered file server.
- Create multiple link targets and replicate content among them.

You can create link targets that point to clustered file servers in both types of namespaces. However, if you want to replicate content among multiple link targets, the type of namespace determines your replication options.

Using Replication in Stand-alone DFS Namespaces

In a stand-alone DFS namespace, you can replicate the files by copying them manually, using scripts, using Robocopy.exe, which is available in the Microsoft Windows Server 2003 Deployment Kit, or by using other replication tools. The Distributed File System snap-in does not provide a user interface for configuring FRS replication in stand-alone DFS namespaces. To configure replication manually, consult the documentation supplied with your replication tools.

Using Replication in Domain-based DFS Namespaces

The Distributed File System snap-in in Windows Server 2003 provides a user interface for creating the FRS topology and schedule on servers running Windows Server 2003. Using FRS in a domain-based DFS namespace is optional; you can also replicate files by copying them manually or by using non-Microsoft replication tools.

Q. What happens when a root target or link target fails or is taken offline?

A. If a DFS client attempts to access a previously used target, and that target is unavailable, the DFS client works down through its referral list for the next available target. This process is often referred to as link target or root target failover. If the client reaches the end of the referral list (that is, there are no available targets), the DFS client fails the request.

Because stand-alone DFS namespaces can have only one root target, no failover occurs if the stand-alone root server is not available; in that case, clients cannot access the namespace.

For link target failover to work correctly, each link can have targets that correspond to only one of the following locations:

- One or more shared folders.
- One or more stand-alone DFS paths anywhere in the stand-alone DFS namespace, including the root.
- A single domain-based DFS path anywhere in the domain-based DFS namespace, including the root.

For root target failover to work correctly, clients must access a domain-based DFS namespace by using the format \\DomainName\RootName, not \\RootServerName\RootName.