VFM (Virtual File Manager) v6.0

Create and Manage Namespaces

May 29, 2007

Publication Number: 215-03204_A0

Copyright © 2007 Brocade Communications Systems, Inc. All Rights Reserved.

Copyright © 2007 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this book covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owners.

Software derived from copyrighted material of Brocade Communications Systems, Inc. is subject to the following license and disclaimer:

Network Appliance and Brocade reserve the right to change any products described herein at any time, and without notice. Network Appliance and Brocade assume no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance and Brocade. The use and purchase of this product do not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance or Brocade.

This product includes software developed by the Apache Software Foundation.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

Brocade®, Tapestry™ StorageX®, and associated logos are registered trademarks or trademarks of Brocade Communications Systems, Inc. Other product and company names are trademarks of their respective owners.

Brocade Communications Systems, Inc, 1745 Technology Drive, San Jose, CA 95110 (www.brocade.com).

NetApp® and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, the European Union, and Japan. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. SnapMirror is a registered trademark of Network Appliance, Inc. in the United States.

VFM® and the VFM logo are registered trademarks of Network Appliance, Inc.

Preface

What the guide covers

This document describes how you can use Network Appliance® VFM® technology to simplify file management and increase data availability while reducing storage costs. It describes how to create and manage a Microsoft® Distributed File System (DFS) global namespace. It begins with instructions about how to create DFS roots and links and how to quickly populate the namespace with namespace creation and permission based policies. It provides instructions about how you can make the namespace highly available and how to automatically back up your namespace by creating namespace availability and namespace backup policies, respectively. The document also explains how to create multiprotocol namespaces for CIFS and NFS clients and how to virtualize users' home directories.

The guide is divided into the following sections:

- **Chapter 1 Introduction** an overview of this guide.
- **Chapter 2 Create Namespaces** explains how to create and manage a DFS namespace.
- **Chapter 3 Populate the Namespace Automatically** explains how to use VFM to easily populate and maintain a logical namespace.
- **Chapter 4 Populate the Namespace Based on Permissions** explains how to use VFM to easily populate the namespace based on group permissions of shares.
- **Chapter 5 Make the Namespace Highly Available** explains how to synchronize the logical structure of DFS roots to make the namespace highly available.
- **Chapter 6 Create Multiprotocol Namespaces** explains how to create and manage multiprotocol namespaces for CIFS and NFS clients.
- **Chapter 7 Virtualize User Home Directories** explains how to virtualize users' home directories.
- **Chapter 8 Back up the Namespace** explains how to automatically back up your namespace.
- **Appendix** provides a list and description of the VFM guides.
- **Glossary** provides definitions of terms used in this guide.

Audience

This guide is for network administrators who are familiar with Windows NT®, Windows® 2000, Windows Server® 2003, and DFS. It does not cover basic system or network administration topics.

Typographic conventions

- **Bold** text - Items on a dialog box or page on the VFM console that you are instructed to click.
- *`code_text_in_italics`* – Variable; replace with actual value.

Using the online help

- Certain icons appear to the left of a topic title to indicate that the information provided applies only to a specific operating system, type of DFS root, or data transfer protocol.

Icon	Description
Win2K	Indicates that the information applies only to DFS roots on Windows 2000 or Windows Server 2003, Enterprise Edition.
domain root	Indicates that the information applies only to domain-based roots.
W2K3	Indicates that the information applies only to DFS roots on Windows Server 2003.

- Definitions of new terms are available wherever they appear in help topics. The first time a new term appears in a help topic, it appears as a green hyperlink.
- Context help contains detailed information about a dialog box or view, and might include links to related topics. Press **F1** or click ? Help.

Support

Contact NetApp technical support, 24 x 7.

Support is either through the web at http://now.netapp.com or by phone. For details, see http://www.netapp.com/support.

Support phone numbers:

- 888 4-NETAPP (US and Canada)
- (1-888-463-8277)
- (408) 822-4700
- 800-44-NETAPP (EMEA/Europe)
- 800-800-0800 (Asia/Pacific)

Note: To get your product build number and license information, click **About VFM** on the Help menu.

Enter new license key

Enter a new license key for the VFM client and server components when you want to extend the VFM evaluation period or when you purchase additional licenses from VFM.

1. Contact NetApp to request a new license key.
2. On the **Help** menu, click **About VFM**.
3. Click **Edit Serial Numbers**.
4. In the License Type list, click the appropriate item.
5. If you selected "Evaluation" as the license type, type the new activation key.

6. If you selected "Full" as the license type, select a product number from the Product list and type the new activation key.
7. Click **OK**.

Note: After you change the activation key, you must restart the VFM client.

Table of Contents

PREFACE ..... **I**

CHAPTER 1 INTRODUCTION **1**

Checklist *1*

CHAPTER 2 CREATE NAMESPACES **3**

The Logical View tree *3*
Basic DFS requirements *3*
Recommended size limits *4*
Additional resources *4*
POPULATING THE NAMESPACE 4
CREATE AND MANAGE ROOTS 5
Create a stand-alone DFS root *7*
Create a domain-based DFS root *8*
Create a consolidation DFS root *9*
How consolidation DFS roots work *14*
Display an existing DFS root *18*
Monitor DFS root status *18*
Set permissions on a domain-based DFS root *18*
Modify properties of a DFS root *18*
View attributes of a DFS root *19*
Back up a DFS root *19*
Refresh a DFS root *20*
Check status of a DFS root *20*
Remove a DFS root from display *20*
Delete a DFS root *20*
Create a root replica *21*
View the replicas of a root *21*
View contents of a root replica *22*
Compare contents of a root target *22*
Delete a root replica *22*
CREATE AND MANAGE LINKS 23
Add a DFS link *23*
Add multiple links *26*
Create new shared folders to link *28*
Expand a link *28*
Add a logical folder to the namespace *29*
Rename a DFS link or folder *30*
Monitor DFS links *30*
View attributes of a DFS link *30*
Modify properties of a DFS link *31*
Refresh a DFS link *31*
Check the status of a DFS link *31*
Delete a DFS link *32*
Manage link targets *32*
MONITOR STATUS 38
Modify status monitoring properties *38*

CHAPTER 3 POPULATE THE NAMESPACE AUTOMATICALLY **41**

CONFIGURE A NAMESPACE CREATION POLICY 41
UPDATE THE SCHEDULE 43
ADD OR REMOVE SERVERS OR DOMAINS 43
ADD ITEMS TO AN EXCLUSION LIST 44

CHANGE THE SEARCH TYPE 44
CHANGE THE SEARCH STRING OF A POLICY 45
CHANGE HOW THE LINKS ARE ARRANGED 45
SCAN FOR ITEMS IMMEDIATELY 45
REVIEW THE LIST OF NEW RESOURCES BEFORE ADDING LINKS 46
DELETE A NAMESPACE CREATION POLICY 46

CHAPTER 4 POPULATE THE NAMESPACE BASED ON PERMISSIONS 47

CONFIGURE A PERMISSION BASED NAMESPACE POLICY 47
UPDATE THE SEARCH CRITERIA 49
To change security groups 49
To change search type or search string 49
OTHER OPTIONS 50
DELETE A PERMISSION BASED NAMESPACE POLICY 50

CHAPTER 5 MAKE THE NAMESPACE HIGHLY AVAILABLE 51

Create a namespace availability policy checklist 51
NAMESPACE CONFIGURATION OPTIONS 51
MAKE DFS ROOTS HIGHLY AVAILABLE 53
CREATE A WIDELINK NAMESPACE 53
To create a widelink namespace 54
NAMESPACE SYNCHRONIZATION OPTIONS 54
SCHEDULE SYNCHRONIZATION 55
START SYNCHRONIZATION IMMEDIATELY 55
ADD ADDITIONAL ROOTS OR SHARES TO A POLICY 56
Drag a root or CIFS share to a policy 56
Add a root or share to a policy 56
REMOVE ROOTS AND WIDELINK NAMESPACES 56
CHANGE THE MASTER ROOT OF A POLICY 57
DELETE A NAMESPACE AVAILABILITY POLICY 57

CHAPTER 6 CREATE MULTIPROTOCOL NAMESPACES 59

Create a multiprotocol namespace policy checklist 59
CREATE A MULTIPROTOCOL NAMESPACE POLICY 59
HOST A UNIX NAMESPACE ON A FILER 60
CONFIGURE UNIX CLIENTS TO ACCESS THE NAMESPACE 61
SELECT DEFAULT UNIX SETTINGS 61
ADD A SYNC POINT 62
SCHEDULE SYNCHRONIZATION 63
RUN CUSTOMIZED COMMANDS DURING SYNCHRONIZATION 63
UPDATE A MULTIPROTOCOL NAMESPACE POLICY 64
START NAMESPACE SYNCHRONIZATION IMMEDIATELY 64
DELETE A SYNC POINT 64
DELETE A MULTIPROTOCOL NAMESPACE POLICY 65

CHAPTER 7 VIRTUALIZE USER HOME DIRECTORIES 67

CREATE A HOME FOLDER POLICY 67
ADD A LINK TO A USER HOME FOLDER 68
Assumption 68
To add a link to a user home folder 68
To add a common link to multiple home folders 68
ADD NEW USERS TO A POLICY 68
VIEW PROPERTIES OF A HOME FOLDER POLICY 69
REFRESH A HOME FOLDER POLICY 69
RESOLVE DISCREPANCIES 69
Discrepancies that VFM resolves 69

To resolve a discrepancy *69*
REMOVE A USER FROM A HOME FOLDER POLICY 70
MOVE A USER 70
LOCATE A USER IN THE NAMESPACE 70
LOCATE A DFS ROOT IN THE NAMESPACE 70
DELETE A HOME FOLDER POLICY 71

CHAPTER 8 BACK UP THE NAMESPACE 73

Backup *73*
Restore *73*
Namespace backup policy checklist *73*
CREATE A NAMESPACE BACKUP POLICY 74
SCHEDULE BACKUPS 74
BROWSE CONTENTS OF A BACKUP 75
REMOVE A ROOT FROM A NAMESPACE BACKUP POLICY 75
DELETE A NAMESPACE BACKUP POLICY 75
RESTORE A DFS ROOT 76

APPENDIX 77

GLOSSARY 79

INDEX 83

Chapter 1 Introduction

This guide explains how to create and manage a logical namespace. It begins with instructions about how to create DFS roots and links and how to quickly populate the namespace with namespace creation and permission based policies. It provides instructions about how you can make the namespace highly available and how to automatically back up your namespace by creating namespace availability and namespace backup policies respectively. The section also explains how to create multiprotocol namespaces for CIFS and NFS clients and how to manage the life cycle of user home directories.

Checklist

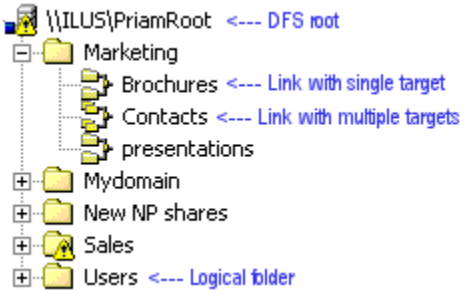
- For basic requirements and general information about DFS and instructions about how to create namespaces, see “Create namespaces.”
- For instructions about how to automatically populate your namespace, see "Populate the namespace automatically.”
- For instructions about how to automatically populate your namespace based on group permissions you specify in a policy selection criteria, see “Populate the namespace based on permissions.”
- For instructions about how to keep aligned the logical structure of two or more DFS roots or a DFS root and widelink namespaces, see "Make the namespace highly available.”
- For instructions about how to create and manage namespaces for CIFS and NFS clients, see “Create multiprotocol namespaces.”
- For instructions about how to manage the life cycle of user home directories, see “Manage user home directories."
- For instructions about how to back up the logical structure of a namespace, see “Back up the namespace.”

Chapter 2 Create Namespaces

This section explains how to create and manage a DFS namespace. The section is arranged according to the elements that make up a namespace, such as roots, links, and link targets. Status monitoring is also covered in this section.

The Logical View tree

The Logical View tree shows the roots, links, and logical folders in your namespace. You manage your namespace from this tree.



Basic DFS requirements

- You can create DFS roots on Windows 2000 and Windows Server 2003 servers. Domain-based roots replicated through Microsoft File Replication Service (FRS) must be created on partitions formatted with Windows 2000 or Windows Server 2003 NTFS on servers that are part of a Windows 2000 or Windows Server 2003 Active Directory™ Domain.
- You can add a DFS link under the DFS root to reference any root, shared folder, or subfolder of a shared folder.
- Linking from one DFS link to another DFS link is possible only if the second link is in a separate namespace. For example, you cannot have \\Server\DFS_root\DFS_link1\DFS_link2 unless DFS_link2 lies under another DFS root.
- You can replicate each DFS root (domain-based only) and shared folder (domain-based and stand-alone) to eliminate single points of failure.
- Administering a stand-alone DFS root requires Local Administrator privileges on the server hosting the root.
- Administering a domain-based DFS root requires Domain Administrator privileges for the domain hosting the root and Local Administrator privileges on each of the servers hosting root targets.
- A consolidation DFS root is a special stand-alone DFS root.

Recommended size limits

Item	Maximum number
Characters per file path	DFS has no inherent limitation on the number of characters in any item of the namespace. Microsoft Win32 APIs have a MAX PATH limitation of 260 characters and applications exceeding this limit fail attempting to access UNCs or directory paths.
Replica members in a domain-based set	See article Q232613 in the Microsoft Windows knowledge base.
DFS roots per server	One root for Windows 2000 servers. Multiple roots for a server running Windows Server 2003 Enterprise Edition. Other DFS-compatible systems might support additional roots per server.
DFS roots per domain	See article Q232613 in the Microsoft Windows knowledge base.
DFS links or shared folders in a DFS root	See article Q232613 in the Microsoft Windows knowledge base.

Additional resources

To read more about DFS, see the following list of recommended web sites.

- **DFS documentation about Windows Server 2003**
  - http://www.microsoft.com/windowsserver2003/community/centers/fileservices/dfsfaq.mspx?pf=true
- **DFS documentation about Windows 2000**
  - http://www.microsoft.com/WINDOWS2000/techinfo/administration/fileandprint/dfsbp.asp

Populating the namespace

There are several ways to populate the namespace. Select a method that best meets your needs.

- "Add a link dialog box" enables you to add one link at a time.
- Drag UNC paths from Windows Explorer to a root in the Logical View.
- "Add multiple links dialog box" enables you to add multiple links and folders at a time. Use this method when you know where items are located on your network and most of the DFS shares that you want to link are located on a few machines. A wizard steps you through the process. You can drag items from Windows Explorer to a folder.

- Namespace Creation Policy wizard enables you to add multiple links and folders at a time. Use this method when you want to add links to multiple shares that are supported by different machines and when you want to keep the logical namespace aligned with subsequent changes in the underlying physical resources.
- Permission Based Namespace wizard enables you to add multiple links and folder at a time like the Namespace Creation Policy wizard. Use this method when you want to populate the namespace based on security permissions of shares.

Create and manage roots

The first step in creating a namespace is to create roots. The root is the top of the logical hierarchy. It can be domain-based or stand-alone. You can create domain-based DFS roots, stand-alone DFS roots, and a special stand-alone root named consolidation DFS root. This section explains how to create and manage these roots.

Note: Windows Server 2003, Enterprise Edition, can host multiple DFS roots. To manage this configuration, VFM must be installed on Windows XP Professional or on Windows Server 2003.

The following table compares the features of each root.

Domain-based DFS root	Stand-alone DFS root	Consolidation DFS root
Microsoft Active Directory must be configured before you can create the root.	Does not use Microsoft Active Directory.	Does not use Microsoft Active Directory.
Must be hosted on a domain member server or domain controller.	Can be hosted on three types of Windows 2000 servers: a stand-alone server, a member server, or a domain controller.	• A special type of stand-alone root that must be hosted on a member server and not a domain controller. • Must be hosted on Windows Server 2003. It is recommended that you host the root on Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition.
Can have multiple root targets.	Can only have one root target.	Can only have one root target.
Can be the target of a link.	Can be the target of a link.	• Cannot be the target of a link. • Does not support link names with "\" characters (for example,

Domain-based DFS root	Stand-alone DFS root	Consolidation DFS root
		abc\def).
Shared folders can be hosted on any type of Microsoft server, or any other server software for which a Windows NT-based client is available. This includes any version of Windows NT Server or Windows NT Workstation, NetWare®, Windows 95, Windows 98, Windows 2000, Windows Server 2003, Windows for Workgroups, LAN Manager, or NFS. **Notes:** Only Windows 2000 and Windows Server 2003 clients support access to domain-based DFS roots in Microsoft Active Directory. You must update Windows NT 4.0, Windows 95, and Windows 98 clients with appropriate service packs before they can connect to domain-based roots. Windows 95 and Windows 98 clients can only negotiate referrals for Server Message Block (SMB) shares. All other targets appear as empty directories.	Shared folders can be hosted on any type of Microsoft server, or any other server software for which a Windows NT-based client is available. This includes any version of Windows NT Server or Windows NT Workstation, NetWare, Windows 95, Windows 98, Windows 2000, Windows Server 2003, Windows for Workgroups, LAN Manager, or NFS. **Notes:** Windows 95 and Windows 98 clients can only negotiate referrals for SMB shares. All other targets appear as empty directories.	
Supports multiple target links.	Supports multiple target links.	
Can make use of FRS replication.	FRS replication not available.	FRS replication not available.

Create a stand-alone DFS root

A Stand-alone DFS root has its configuration information stored locally on the host server. The root has a single root target. When the root target is unavailable, the data referenced by links under the root is inaccessible.

Note: For instructions about how to make a stand-alone DFS root highly available, see Make DFS roots highly available."

Prerequisites

- Microsoft DFS server software (Distributed File System Service `dfssvc.exe`) must be running on the server that hosts the DFS root.
- You must have administrator permissions for the server where you create the DFS root.
- Windows 2000 servers can host only one DFS root.
- VFM creates roots on Windows 2000 and Windows Server 2003 servers.
- Windows Server 2003, Enterprise Edition, can host multiple DFS roots. To manage this configuration, VFM must be installed on Windows XP Professional or on Windows Server 2003.

To create a stand-alone DFS root

1. Perform one of the following actions:
   - Right-click Logical View and click **Add a new DFS root**.
   - Click **Create DFS root**.
   - On the **Tools** menu, click **Add a new DFS root**.
2. Click **Next**.
3. In the **Server name** field, type the name of the server where you want to create the DFS root, or click **Browse** to select an available server.
4. Click **Next**.
5. Select **Create a Stand-alone DFS root** and click **Next**.
6. Select an existing shared folder or create a new shared folder.
   - If you clicked **Use an existing shared folder**, type the path and name of the shared folder or select an available shared folder.
   - If you clicked **Create a new shared folder**, type the path and name of the shared folder in the appropriate fields.

   The name of the DFS root is the same as the shared folder you selected.
7. Click **Next**.
8. In the **Comment** field, optionally type a word or phrase.
9. In the **Clients cache this referral for** field, optionally change the duration (in seconds) that the root is cached on a DFS client, then click **Next**.
10. Verify the information then click **Finish**. The new DFS root appears in the Logical View tree.

Create a domain-based DFS root

A domain-based DFS root has its configuration information stored in Active Directory. The root can have multiple root targets or replicas, which offers fault tolerance and load sharing at the root level.

Prerequisites

- Microsoft DFS server software (Distributed File System Service `dfssvc.exe`) must be running on the server that hosts the DFS root.
- Microsoft Active Directory must already be operational.
- The account used for VFM must have administrator permissions for both the domain and the server where you create the DFS root.
- When creating domain-based roots, it is strongly recommended that you run VFM on a system that is a member of the domain that hosts the root. Name resolution problems and permission problems often manifest themselves in scenarios where the administrative machine resides in an NT4 domain and is attempting to create a domain-based root in a separate Active Directory domain.
- Windows 2000 servers can host one only DFS root.
- Windows Server 2003, Enterprise Edition, can host multiple DFS roots. To manage this configuration, VFM must be installed on Windows XP Professional or on Windows Server 2003.

To create a domain-based DFS root

1. Perform one of the following actions:
    - Right-click Logical View and click **Add a new DFS root**.
    - Click **Create DFS root**.
    - On the **Tools** menu, click **Add a new DFS root**.
2. Click **Next**.
3. In the **Server name** field, type the name of the server where you want to create the DFS root or click **Browse** to select an available server.
4. Click **Next**.
5. Select **Create a domain-based DFS root** and click **Next**.
6. Select an existing shared folder or create a new shared folder.
    - Best practices dictate that the share name used should match the name of the root that is being created.
    - If you clicked **Use an existing shared folder**, type the path and name of the shared folder or select an available shared folder.
    - If you clicked **Create a new shared folder**, type the path and name of the shared folder in the appropriate fields.
7. Click **Next**.
8. In the **DFS root name** field, optionally type a name for the root (follow the file naming conventions for the operating system of the server).
9. Optionally type a word or phrase in the **Comment** field.
10. In the **Clients cache this referral for** field, optionally change the duration (in seconds)

that the root is cached on a DFS client then click **Next**.

11. Verify the information.
12. Click **Finish**. The new DFS root appears in the DFS Tree window.

Create a consolidation DFS root

Consolidation DFS roots are special stand-alone roots that enable you to move files referenced in UNC paths embedded in links, in line-of-business applications, and in other places without affecting users. The consolidation root redirects the user from the old location referenced by the UNC path to the new location. For an illustration about how consolidation roots work, see "How consolidation DFS roots work."

Prerequisites

- Microsoft DFS server software (Distributed File System Service `dfssvc.exe`) must be running on the server that hosts the DFS root.
- You must install a software update that enables you to host a consolidation root on the server you select. Contact Microsoft for the software update. After you apply the software update, you must restart the Distributed File System service. For more information about consolidation roots, see Microsoft Knowledge Base Article 829885.
- Before you configure the consolidation root, you must rename the server to be consolidated. See "How consolidation DFS roots work" for clarification.
- The consolidation roots must be installed on Windows Server 2003. It is recommended that you host the root on Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition.
- The consolidation root must be hosted on a member server and not a domain controller because the server consolidation logic is disabled if the root is hosted on a domain controller.
- The NETBIOS name of the server that hosts the consolidation root must be the same as the host name part of its fully qualified domain name (FQDN).
- The consolidation of UNC paths from two servers that have the same host name is not supported. For example, you cannot consolidate two servers that are named *server1.npd.com* and *server1.<subdomain>.npd.com*.
- The account used for VFM must have administrator permissions for the server where you create the DFS root.
- Windows Server 2003, Enterprise Edition, can host multiple DFS roots. To manage this configuration, VFM must be installed on Windows XP Professional or on Windows Server 2003.

To create a consolidation DFS root

Notes:

- To clarify the instructions about how to configure a consolidation DFS root, the following terms are used:
  - The server that hosts the consolidation DFS root is named *ConsolidationServer*.
  - The server to be consolidated is named *Server1*. *Server1* is renamed to *OldServer1* before the consolidation DFS root is created.
  - Data is migrated from *OldServer1* to *ConsolidationServer*.

1. Perform one of the following actions:
   - Right-click Logical View and click **Add a new DFS root**.
   - Click **Create DFS root**.
   - On the **Tools** menu, click **Add a new DFS root**.
2. Click **Next**.
3. In the **Server name** field, type the name of the Windows Server 2003 server that will host the DFS root or click **Browse** to select an available server. For example, you would type *ConsolidationServer*.
4. Click **Next**.
5. Select **Create a DFS Consolidation root** and click **Next.**
6. In the **Server name** field, type the original name of the CIFS server that you want to consolidate. For example, you would type *Server1*.
7. In the **Local Path of New Share** field, type the path of the share on the server hosting the root that will contain the root configuration information.
8. Click **Next**. VFM uses the name of the server you want to consolidate as the name of the share of the consolidation root. The share name is preceded by a hash (#) character. For example, *\\ConsolidationServer\#Server1* would be the name of the consolidation DFS root.
9. Optionally, type a word or phrase that best describes the root in the **Comment** field.
10. Optionally, change the duration (in seconds) that the root is cached on a DFS client and then click **Next**.
11. Click **Finish**. The root appears in the Logical View tree.

12. After you create the root, you must perform the following actions:

Action		Description
1	Make sure that **Automatically update DHCP client information in DNS** is selected on the DHCP server.	• If you use a Microsoft Windows 2000 DHCP server, make sure that the **Automatically update DHCP client information in DNS** check box is selected only at the server level and not selected at the DHCP scope level. • If you use a Microsoft Windows 2003 DHCP server, make sure that the **Enable DNS dynamic updates according to the settings below** check box is selected only at the server level and not selected at the DHCP scope level. • To clear the DHCP scope level, perform the following actions: 1. On the DHCP server, click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DHCP**. 2. Expand the DHCP server name, right-click the first Scope on the list, and click **Properties**. 3. Click the **DNS** tab. 4. For a Microsoft Windows 2000 DHCP server, clear the **Automatically update DHCP client information in DNS** check box. For a Microsoft Windows 2003 DHCP server, clear the **Enable DNS dynamic updates according to the settings below** check box. 5. Repeat Steps 2 through 4 for each DHCP scope.
2	On the Windows Internet Name Service (WINS) server, verify that static WINS entries do not exist for the server to be consolidated. For example, you would make sure that WINS entries do not exist for *Server1*. If WINS entries exist, delete them. For more information	

Action		Description
	about how to delete static WINS entries, contact Microsoft.	
3	From a command-line prompt on the server hosting the consolidation DFS root, type the following command: `ipconfig /registerdns`	
4	Restart the Server service on the server hosting the consolidation DFS root. If you stop and restart the Server service instead of restarting it, you must start the DFS service and Computer Browser service. Whenever you stop the Server service, the DFS and Computer Browser services are also stopped.	

Optionally, log a system event every time that the DFS root consolidation server successfully resolves a referral. The log enables you to see which clients are accessing the consolidated data through the old server name.

1. Locate then click the following registry key:

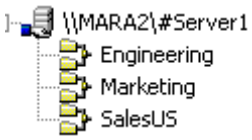
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dfs\Parameters\Replicated`

2. On the **Edit** menu, point to **New**, and click **DWORD Value**.
3. Type **LogServerConsolidation** and press ENTER.
4. In the **Value data** box, type **1** and click **OK**. This will log the logical path and the client's IP address to the system event log as event ID: 14318. Allocate sufficient space to the system log. Microsoft recommends that you set the system event log to at least 64 megabytes. Make sure to set the system event log to overwrite events as needed.

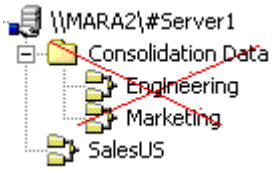
- To configure a consolidation DFS root in a cluster server environment, see the Microsoft Knowledge Base Article 829885.
- After you create the consolidation DFS root, migrate the data to the new location by creating a migration policy and create links under the consolidation root that target shares in the new location that will be redirected. For example, a link under the consolidation root *\\ConsolidationServer\#Server1* would target the location of a share on *ConsolidationServer*. For instructions about how to configure a migration policy and add links to the consolidation root, see "Create a migration policy" and "Add multiple links."

- Links in a consolidation root cannot be referenced under a logical folder. Links must always be directly under the consolidation root. If you try to access a link under a logical folder, you get the error "No network provider accepted the given path."

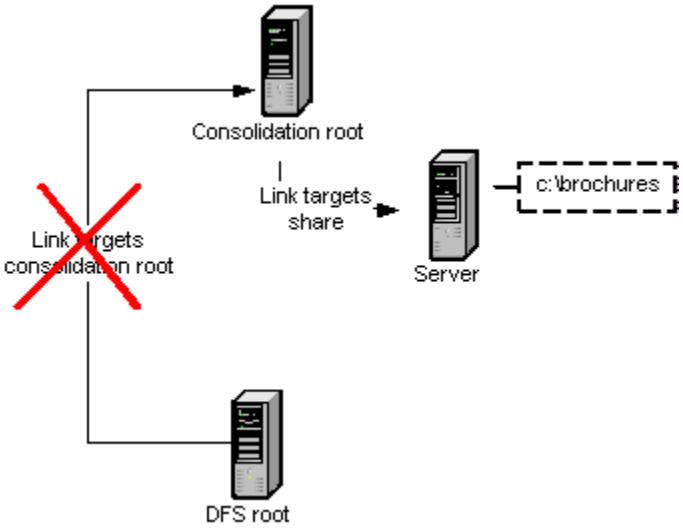
Correct configuration of a consolidation root. Links are listed directly under the root.



Incorrect configuration of a consolidation root. The targets of links "Engineering" and "Marketing" cannot be accessed because they are configured under the logical folder "Consolidation Data."



- The target of a link of a consolidation root <u>must</u> be a share. A consolidation root cannot be the target of a link of a DFS root. See the following illustration.

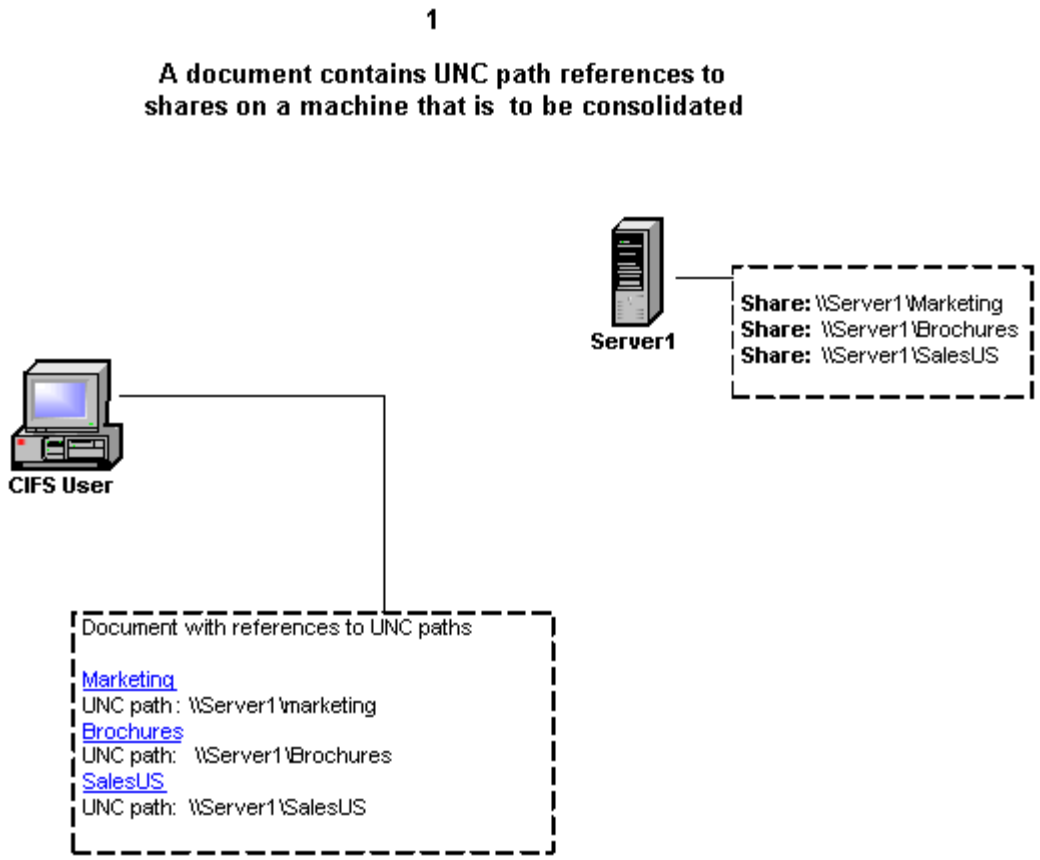


How consolidation DFS roots work

The following diagrams illustrate how consolidation DFS roots enable you to migrate data without affecting UNC path references embedded in user documents.

When to use a consolidation root

You might want to configure a consolidation root when you need to move data from a server that contains files that are referenced in users' documents. When the files are moved to the new location, all UNC path references to the files on the old server must be updated to point to the new location. A consolidation root enables you to move the referenced files without having to update UNC path references.

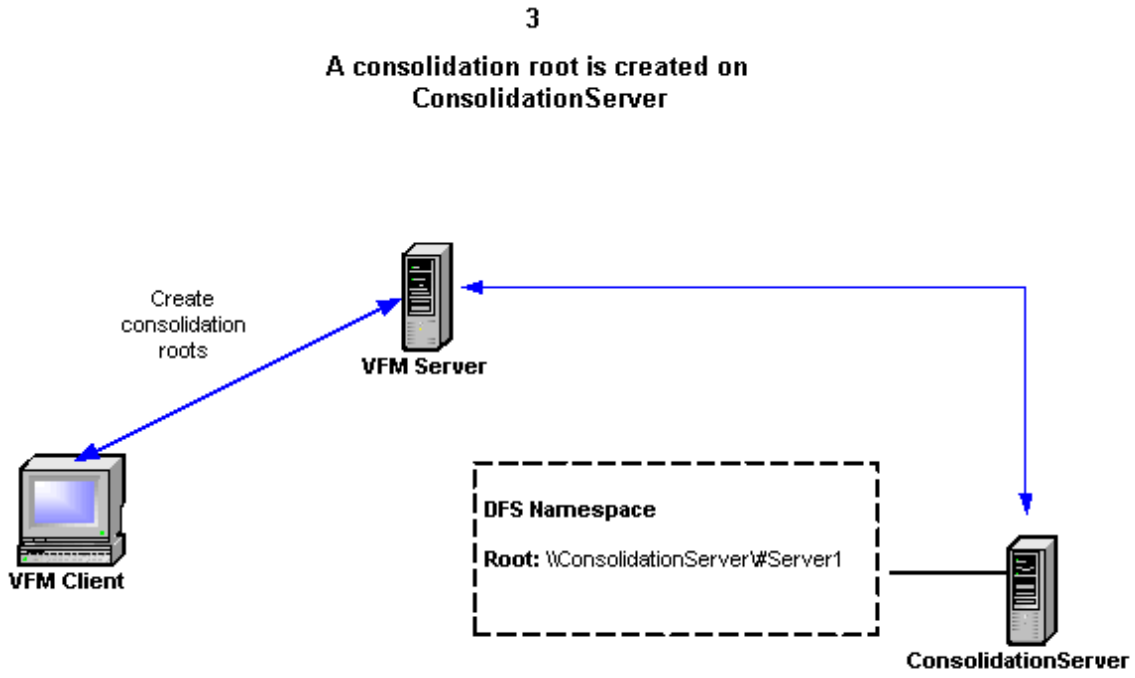


Rename the server you want to consolidate

Before you configure a consolidation root, rename the server you want to consolidate.

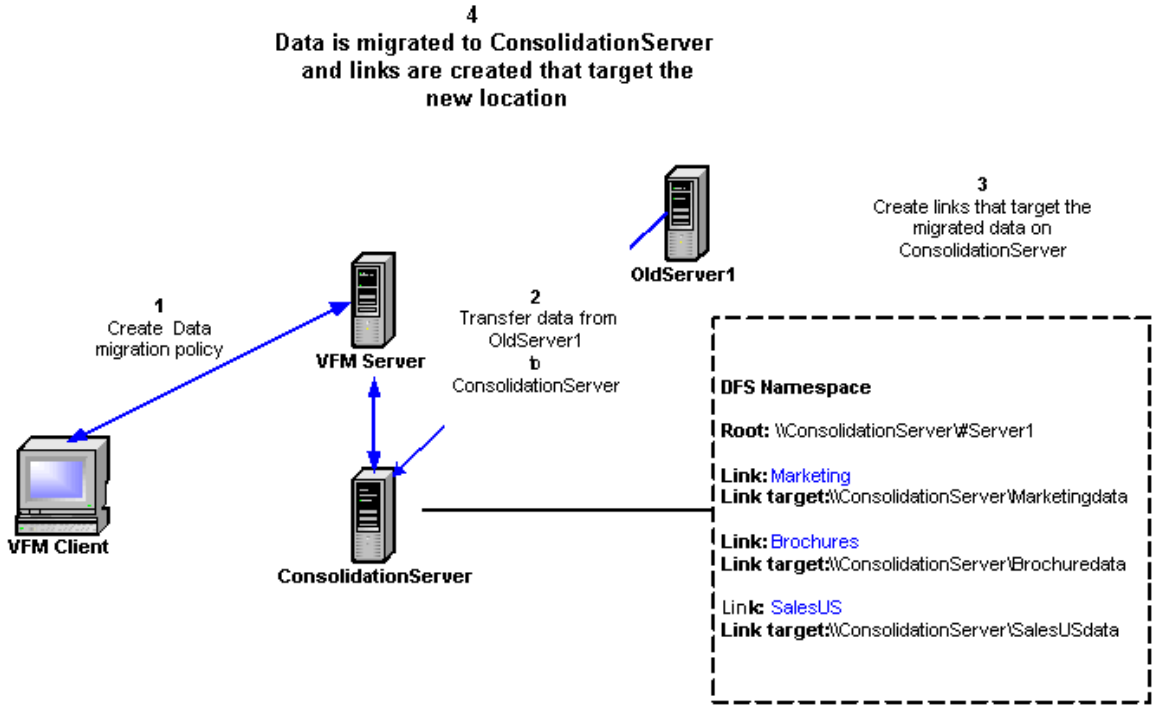
Create a consolidation DFS root

VFM provides a wizard that steps you through the process of creating a consolidation root. There are other steps you must perform when configuring a consolidation root. For example, you must install a Microsoft software update on the machine that will host the root. See "Create a consolidation root" for detailed instructions.



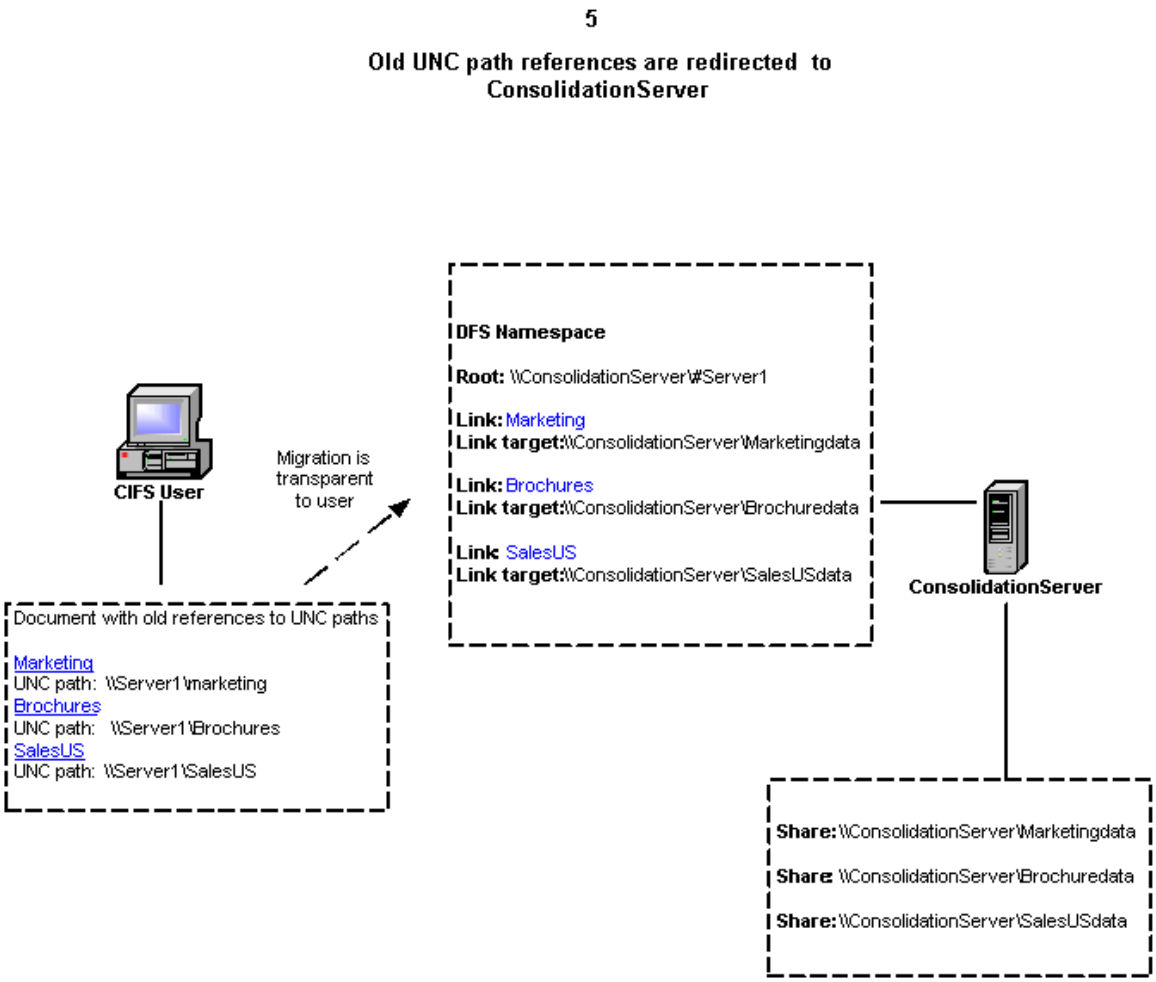
Move the data from old server location to the new location

Create a migration policy to move the data to the new location and create links to shares in the new location.



Old UNC path references are redirected

The old UNC path references to shares in the old server are redirected to the new location of the shares.



Display an existing DFS root

Display DFS roots that already exist on your network.

1. Perform one of the following actions:
    - Right-click Logical View and click **Display an existing DFS root**.
    - Click **Display an existing DFS root** on the toolbar.
    - On the **Tools** menu, click **Display an existing DFS root**.
2. Perform one of the following actions:
    - Type the name of the DFS root, its host server, or the domain.
    - Select the domain that contains the DFS root, and select the root. If a server is configured so that it does not appear in a browser, it does not appear in this list. You can still display the server in the Logical View tree by typing the name of the root or server in the **DFS Root**, **Host Server**, or **Domain** field.
3. Click **OK**.

Note: To view all the roots in the namespace, click Logical View.

Monitor DFS root status

By default, DFS roots and links are monitored. You can turn off status monitoring for a root.

1. Perform one of the following actions:
    - Click the root. On the **Properties** tab that appears in the right pane, click Edit.
    - Right-click the root and click **Properties**.
2. Click the Status Monitoring tab, and clear the Monitor status every check box.

Set permissions on a domain-based DFS root

Set or change permissions for a domain-based DFS root.

1. Right-click the root and click **Properties**.
2. Click the **Security** tab.

Modify properties of a DFS root

Edit the properties of a root displayed in the Logical View tree.

1. Perform one of the following actions:
    - Click the DFS root to display the **Properties** tab in the right pane, and click Edit.
    - Right-click the DFS root and click **Properties**.
2. Update the information and click OK.

View attributes of a DFS root

Click a root to display the following tabs in the right pane.

- **Properties** - Shows the characteristics or parameters of the selected root and enables you to edit certain fields. Right-click an item to display a context menu.
- **Status** - Shows information for any monitored item (for example, root, link, and target). By default, roots and links are monitored. You can choose to enable monitoring of targets. Right-click a root and click **Properties**, and click the **Status Monitoring** tab.
- **Replication Tasks** - Shows information about replication operations for items forming part of the root.
- **Explorer** - Shows the namespace, as a user browsing with Windows Explorer would see it. Right-click a root share, a single target link, or replicated link to display a context menu.
- **Dependencies** - Shows the underlying resources, such as systems, shares, and disks, forming part of the root. Right-click an item to display a context menu.
- **Events** - Shows the history of events for the item selected.
- **Reports** - Shows a list of reports generated that reference the root.

Back up a DFS root

You can manually back up the logical structure of a root.

1. Perform one of the following actions:
   - Right-click a root and click **Backup**.
   - Right-click Logical View and click **Backup**.
   - On the **Tools** menu, click **Manual backup**.
2. Select the DFS roots you want to back up.
3. Accept the default name for the backup file or type a new name.
4. Click **Backup**.
5. Click **OK**. The backup file is saved on the VFM server.

Notes:

- To check whether the backup operation is complete, click the **Events** tab for each root that was backed up.
- You can set up a policy to automatically back up selected DFS roots. On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, then click **Backup Policy**.

Refresh a DFS root

Update the contents of a root in the Logical View tree.

Perform one of the following actions:

- Select the root and press **F5**.
- Select the root and click **Refresh** on the main toolbar.
- Right-click the root and click **Refresh**.
- Select the root and click **Refresh** on the **View** menu.

Fresh information is gathered from the network for all the items that make up the DFS root.

Notes:

- Gathering fresh information for the entire DFS root takes extra time if the DFS root is large.
- To refresh all the items in the namespace, click **Refresh All** on the **View** menu.

Check status of a DFS root

If needed, you can manually check the status of a DFS root to ensure that the root is still valid.

Right-click the DFS root and click **Check status**.

Note: To remove the status display from a root, right-click the root and click **Clear status**.

Remove a DFS root from display

When the Logical View Logical View displays too many roots to manage effectively, or you complete the management of a root, you can remove the root from appearing in the VFM console. This does not delete the root from the server.

Right-click the root and click **Remove from display**.

Delete a DFS root

When you delete a root, it is removed from the server. The configuration files are removed, but files that were referenced by the root are not deleted. When you delete a root, the clients can no longer browse it using the namespace.

1. Right-click the root and click **Delete**.
2. Click **Yes**.

Create a root replica

Specify additional servers to host copies of the logical structure of a namespace to provide fault tolerance and load balancing. Only domain-based DFS roots can contain more than one root target.

1. Perform one of the following actions:
   - Right-click the root and click **Add replica**.
   - Click Logical View to display a Properties tab. Right-click a root and click **Add replica**.
2. Type the name of the server that will host the root target, or click **Browse** to find the server.
3. Click **Next**.
4. Perform one of the following actions:
   - Select **Use an existing share** and select a shared folder from the list.
   - Select **Create a new share** and type a local path and the name for the shared folder. The application creates the shared folder on the server specified.
5. Click **Finish**. The root is now represented in the Logical View as root with multiple targets .

Notes:

- You can create only one DFS root on Windows 2000 servers. Windows Server 2003, Enterprise Edition, can host multiple DFS roots.
- When creating or selecting a share, best practices dictate that the share name match the name of the root.
- To provide fault tolerance and load balancing of stand-alone roots, create a namespace availability policy.

View the replicas of a root

Display a list of root targets for a domain-based DFS root.

1. Click the DFS root in the Logical View tree.
2. Click the **Properties** tab that appears in the right pane. The targets of the root appear under **Replicas**.

Notes:

- Right-click a root target to display a context menu.
- Double-click a root target to display where it is physically located on your network. The Physical View tree expands to display the machine where the target resides.

View contents of a root replica

View the contents of domain-based root targets. To browse the contents of a root target, you must make it the active target.

1. In the Logical View tree, select a domain-based root target.
2. Click the **Explorer** tab in the right pane.
3. Right-click a domain-based root target, point to **Target,** and click the target you want to activate. The contents of the replica appear in the right window.

Notes:

- You can also view the contents of a link, share, or folder. In the Logical View tree or Physical View tree, right-click an item, point to **External Tools**, and click **Explorer**.
- Changing the active target only changes the target the VFM console machine is viewing. It does not change what other users of the namespace see.

Compare contents of a root target

Compare the contents of a domain-based root target.

1. Click a root under the Logical View to display its properties in the right pane.
2. Under **Replicas**, select the targets that you want to compare.
3. Right-click, point to **Reports**, point to **Physical**, and click **File Differences**. The first target on the list that you selected appears in the **Compare** field.
4. Click **Next**.
5. Type a name for the report and the location at which you want to save it.
6. Click **Finish**.

Note: You can also compare contents of shares in the Physical View. Right-click a share, point to **Reports,** and click **File Differences**.

Delete a root replica

You can delete a domain-based DFS root replica and not delete the root as long as the domain-based root contains more than one root replica. If all root replicas are deleted, the root is deleted.

1. Select a root in the Logical View. A **Properties** tab appears in the right pane.
2. Under **Replicas**, right-click a shared folder and click **Delete**.
3. Click **Yes**.

Create and manage links

The next step in creating a namespace is to create links. Links form a connection to one or more shared folders, other links, or to another root. This section provides instructions about how to create and manage links and link targets.

Note: The Namespace Creation Policy and Permission Based Policy wizards enable you to add multiple links and folders at a time. Use these methods when you want to add links to multiple shares that are supported by different machines and when you want to keep the logical namespace aligned with subsequent changes in the underlying physical resources.

Add a DFS link

Add links to the namespace using any one of the following operations.

- Drag a share from Windows Explorer to a DFS root in the Logical View tree
- Drag an item from the Physical View tree to a DFS root in the Logical View tree
- Use the Add link dialog box to perform the following tasks:
    - To make a shared folder or subfolder the target of a link
    - To add a link to a folder in the namespace
    - To add a link to multiple folders in the namespace
    - To add a link to multiple roots

A link can appear below a root or links can be grouped into folders. The target of a DFS link must be one of the following types:

- 1 to N shared folders
- 1 to N stand-alone DFS paths
- Only 1 domain-based DFS path

Configuring other combinations of link targets might prevent link target failover from functioning correctly.

To drag a share from Windows Explorer to a DFS root in the Logical View tree

Drag a network share (UNC path) from Windows Explorer to a DFS root in the Logical View tree.

Notes:

- You cannot drag local folders (for example, c:\<*path*>) to a DFS root from Windows Explorer.
- If you want to drag shares from your local system into the DFS namespace, browse Windows Explorer to your local host through the Network Neighborhood so that Explorer displays a UNC path name to your local share before performing the drag-and-drop operation.

To drag an item from the Physical View tree to the Logical View tree

Drag a shared folder from the Physical View tree to a DFS root in the Logical View tree.

To make a shared folder or subfolder the target of a link

1. Perform one of the following actions:
   - Select a root in the Logical View tree and click **Add link**.
   - Right-click a DFS root in the Logical View tree and click **Add link**.
   - Right-click a DFS root on the Properties tab of Logical View and click **Add link**.
   - Select a DFS root in the Logical View tree and click **Add link** on the **Tools** menu.
   - Drag a network share (UNC path) to the Logical View.
2. Under **Users connect to**, type the name of the link.
3. Click **Add**.
4. Under **Send the user to one of these shared folders or directories**, perform one of the following actions:
   - Type the name of a folder.
   - Click **Browse** to find a share or subfolder in your network or the Physical View tree.
   - Drag a network share and drop it into the **Send the user to one of these shared** folders or directories field.
5. Click OK.
6. In the Comment field, optionally type a word or phrase that describes the link.
7. In Clients cache this link for, type how long (in seconds) a reference to the link is cached on the DFS client.
8. Click OK. The DFS link appears under the root selected.

To add a link to a folder

Group links in logical folders. Create a folder on a DFS root server and add links to it.

1. Perform one of the following actions:
   - Select a root in the Logical View tree and click **Add link**.
   - Right-click a DFS root in the Logical View tree and click **Add link**.
   - Right-click a DFS root on the Properties tab of Logical View and click **Add link**.
   - Select a root in the Logical View tree and click **Add link** on the **Tools** menu.
2. Under **Users connect to**, type a name for the folder and the name of the link; for example: *foldername\linkname* or *folder1\folder2\linkname.*
3. Click **Add**.

4. Under **Send the user to one of these shared folders or directories**, type the name of a folder, or click **Browse** to find a share or subfolder in your network or the Physical View tree.
5. Click **OK**.
6. In **Comment**, type a word or phrase that describes the link.
7. In Clients cache this link for, type how long (in seconds) a reference to the link is cached on the DFS client.
8. Click OK. The folder appears under the DFS root selected.

To add a link to multiple folders

Add the same link to multiple folders in the Logical View.

1. Select a folder with subfolders to display a Properties tab in the right pane.
2. On the **Properties** tab, right-click the selected subfolders and click **Add links**.
3. Under **Users connect to**, type the name of the link.
4. Click **Add**.
5. Under **Send the user to one of these shared folders or directories**, perform one of the following actions:
   - Type the name of a share.
   - Click **Browse** to find a share or subfolder in your network or the Physical View tree.
   - Drag a network share to **Send the user to one of these shared folders or directories**.
6. Click OK.
7. In Comment, type a word or phrase that describes the link.
8. In Clients cache this link for, type how long (in seconds) a reference to the DFS link is cached on the DFS client.
9. Click OK. The link appears under the folders selected.

To add a link to multiple roots

Add the same link to multiple roots in your namespace.

1. Select **Logical View** Logical View to display a **Properties** tab in the right pane.
2. On the **Properties** tab, right-click the selected roots and click **Add links**.
3. Under **Users connect to**, type the name of the link.
4. Click **Add**.
5. Under **Send the user to one of these shared folders or directories**, perform one of the following actions:
   - Type the name of a share.
   - Click **Browse** to find a share or subfolder in your network or the Physical View tree.

6. Drag a network share to **Send the user to one of these shared folders or** directories.
7. Click OK.
8. In Comment, type a word or phrase that describes the link.
9. In Clients cache this link for, type how long (in seconds) a reference to the link is cached on the DFS client.
10. Click OK. The link appears under the roots selected.

Notes:

- To display hidden shared folders, select the **Show hidden shares** check box.
- By default, only server machines are displayed. To also display workstations, select **Show workstation computers**.
- The following reserved device names cannot be used as the name of a link: CON, PRN, AUX, CLOCK$, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.

Add multiple links

You can visualize the namespace you are designing and see the namespace as you build it. The Logical View tree is updated as you add a link or logical folder.

Note: Device names cannot be used as the name of a link. For more information, see "Add a DFS link."

To add multiple links

Add multiple links to the DFS root selected or to an existing folder in the namespace.

1. Perform one of the following actions:
   - Right-click a DFS root in the Logical View and click **Add multiple links**.
   - Right-click a DFS root on the Properties tab of Logical View and click **Add multiple links**.
   - Select the root and click **Add multiple links** on the **Tools** menu.
2. To add links, perform one of the following actions:
   - Drag network shares (UNC paths) from Windows Explorer to the tree view in the Add Multiple Links dialog box.
   - Select the DFS root or a folder and click **Add Links**.
   - Right-click the DFS root or folder and click **Add links**.

   A dialog box appears, enabling you to browse your network or Physical View tree.

3. Expand the tree you want to search and select an item or items.

Notes:

- To display hidden shared folders, select the **Show hidden shares** check box.
- By default, only displays server machines are displayed. To also display workstations, select **Show workstation computers**.
- To view a context menu, right-click a shared folder.

4. Click **OK**. The links you created appear in bold print in the namespace tree.
5. Repeat Steps 2 through 4 to create additional links.
6. Click a link to display its properties.
7. Optionally update the link properties
   - **Name -** Type a new name for the link.
   - **Send the user to this shared folder or directory -** Change the target of the link. Type the address of a new target or click **Browse** to locate another target.
   - **Comment -** Add an optional description of the link.
   - **Clients cache this link for -** Set the duration (in seconds) the target of the link is cached on a DFS client.
8. Click **OK** to apply the changes to the namespace. A status window displays the changes being made.
9. Click **Done**.

To add multiple links to a folder

Create folders to group links in a common directory in the Logical View. You can also create a folder when you add a link in the "Add a link" dialog box.

1. Select the DFS root or a folder in the namespace of the Add Multiple Links dialog box.
2. Click **New Folder**.
3. Type a name for the folder and press **Enter**.
4. Perform one of the following actions to add links to the folder:
   - Select the folder and click **Add Links**.
   - Right-click the folder and click **Add Links**.
   - Drag network shares from Windows Explorer.
   - Cut and paste mapped network drives or items with valid UNC paths to the folder from Windows Explorer.

Notes:

- You cannot drag or paste local folders from Windows Explorer.
- If you want to drag shares from your local system into the DFS namespace, browse Windows Explorer to your local host through the Network Neighborhood so that Explorer displays a UNC path name to your local share before performing the drag-and-drop operation.

To move a link or folder to a new location

After a link or folder is added to the namespace of the Add Multiple Links dialog box, you can move the item to a new location in the tree.

Perform one of the following actions:

- Drag the link or folder to a new location on the tree.
- Right-click the link or folder you want to move and click **Cut**. Right-click the link or folder where you want to move the item and click **Paste**.

Create new shared folders to link

Select the machine or machines where you want to create shares and add the shares to a new or existing link.

1. Perform one of the following actions:
    - On the **Tools** menu, click **Create shares**.
    - Right-click a link in the Logical View and click **Create shares**.
    - Right-click a machine in the Physical View tree and click **Create shares**.
2. Click **Next**.
3. Select **Regular Share** and click **Next**.
4. Type the information requested and click **Next**.
5. Select the machine or machines where you want to create the folder and click **Next**.
6. Select an option and click **Next**.
7. Perform one of the following actions:
    - If the path of the link appears, click **Next**.
    - If the path of the link does not appear, type the path or click **Browse** to locate the link in the namespace, and click **Next**.
8. Click **Finish**. The share is created on the machines and added to the link.

Expand a link

Replace a link targeting a share with links targeting the subdirectories contained in the original share. When the share contains data in its root, you can migrate the data and create a link to target the data. This enables you to access the data through the namespace.

Expand a link option enables you to perform the following:

- Move data in subdirectories to a different machine to load balance.
- Make the data in subdirectories available from different locations in the namespace.

Note: When expanding namespaces, the DFS limitations on numbers of links contained in a root need to be considered. For more information, see " Basic DFS requirements and limitations."

1. Right-click a link whose target contains subdirectories and click **Expand**.
2. If the same link appears in other locations of the namespace, a list of identical links appears. You can expand all, none, or some of the identical links. After you make your choice, click **OK**.

3. The subdirectories are identified and the actions that will be performed is explained. Click **Yes**.
4. Click **Done**. The original link is deleted, a logical folder with the same name as the original link is created, and new links are added to the logical folder that target the subdirectories.
5. If the original target contains data along with subfolders, you have the option to migrate the data to another location to make the data accessible through the namespace. To migrate the data, click **Yes** when the dialog box appears.
6. Perform one of the following actions:
   - Select an existing migration policy and continue with Step 10
   - Click **New Policy** to create a new migration policy and continue with Step 7.
7. Type the name for the policy.
8. Click **OK**.
9. Select the new policy.
10. Click **Next**. The original and destination paths appear.
11. Click **Next**.

    Click **Finish**. A link targeting the data appears under the same folder as the links targeting the subdirectories. The link name ends with `_data`.

Add a logical folder to the namespace

You can create folders in your namespace. The folders appear alphabetically in the Logical View tree. You can add links to the folders and move the folders and their links to another folder or DFS root.

1. Perform one of the following actions:
   - Right-click a DFS root or folder in the Logical View and click **Add folder**.
   - Select a DFS root to display a Properties tab in the right pane. Right-click anywhere on the page and click **Add folder**.
2. Type a name for the folder and click **OK**.

Notes:

- The permissions on a DFS root share controls whether you can create logical folders in the namespace. Windows Server 2003 defaults share permissions to read-only and Windows 2000 Server defaults share permissions to allow everyone full access.
- A folder and its links can be moved to another folder or DFS root. Drag the folder to its new location.
- Dragging a folder moves only its logical structure but does not move data physically resident in the folder on the DFS root server. Best practices dictate that data should not reside physically on the DFS root server because this can increase the load on the server by forcing it to serve files as well as the logical namespace. If you have data in folders in your DFS namespace, use the VFM migration features to move it to the new location where you transferred the folder.
- To create a subfolder, right-click the newly created folder and click **Add folder**.
- To add links to the folder, right-click the folder and click **Add link** or **Add multiple links**. You can also drag links to the folder.

Rename a DFS link or folder

To change the name of a link or folder in the Logical View tree perform one of the following actions:

- Click a link or logical folder slowly to display a text box and type a new name.
- Right-click the link or folder and click **Properties**, type a new name, and click **OK**.
- Click the link to display a **Properties** tab in the right pane and click Edit. Type a new name and click **OK**.

Notes:

- If the namespace contains links that are identical to the link you renamed, you are given the option of renaming all the identical links in one easy step.
- Device names cannot be used as the name of a link. See "Add a DFS link" for detailed information.

Monitor DFS links

To get status monitoring information about links, you must go through the DFS root that contains the links. If status monitoring is turned on for a DFS root, you can also turn on status monitoring for its links.

1. Perform one of the following actions:
   - Right-click the root that contains the links you want to monitor and click **Properties**.
   - Click the root to display the **Properties** tab in the right pane and click Edit.
2. Click the **Status Monitoring** tab and select **Monitor links every**.
3. Enter how often (in minutes) you want to check the status of each link when it is online.
4. Enter how often (in minutes) you want to check the status of each link when it is offline.

View attributes of a DFS link

Select a DFS link to display the following tabs in the right pane.

- **Properties -** Shows the characteristics or parameters of the selected link and enables you to edit certain fields. Right-click an item to display a context menu.
- **Status -** Shows information about the link. This tab also shows information about targets when target monitoring is turned on. By default, roots and links are monitored. To enable monitoring of targets, edit the properties of the DFS root to which the link belongs.
- **Replication Tasks -** Shows information about link target replication operations.
- **Explorer -** Shows the namespace as a user browsing with Windows Explorer would see it. Right-click a root share, a single target link or a replicated link to view a context menu.
- **Dependencies -** Shows the underlying resources, such as systems, shares, and disks that form part of the link. Right-click an item on the tab to display a context menu.
- **Events -** Shows the history of events for the item selected.
- **Reports -** Shows a list of reports generated that reference the link and the targets of the link.

Modify properties of a DFS link

Edit the properties of a DFS link in the Logical View tree.

1. Perform one of the following actions:
   - On the **Properties** tab of a link, click Edit.
   - Right-click the DFS link and click **Properties**.
2. Update the information and click **OK**. If the namespace contains links that are identical to the link you modified, you have the option of updating all the identical links in one easy step.

Notes:

- When you browse for a folder, you have the option of creating, renaming, deleting, and sharing new folders, and removing a share.
- Right-click a shared folder to view a context menu.
- Double-click a shared folder and right-click a folder or anywhere in the window to view a context menu.
- When the cache period elapses, the DFS client must access the root share to update the shared folder information. Entering a lower value increases associated network traffic. A higher value reduces associated network traffic at the possible expense of updated share information.
- If the cache time-out value is set too high, client computers might not pick up changes to DFS referrals unless they are restarted (see Microsoft Knowledge base article Q222604).

Refresh a DFS link

Update the contents of a DFS link in the Logical View tree. Fresh information is gathered from the network for all the targets of the DFS link.

Perform one of the following actions:

- Select the link and press **F5**.
- Select the link and click **Refresh** on the main toolbar.
- Right-click the link and click **Refresh**.
- Select the link and click **Refresh** on the **View** menu.

Note: To refresh all the items in the namespace, click **Refresh All** on the **View** menu.

Check the status of a DFS link

If needed, you can manually check the status of a DFS link to ensure that it is still valid.

Right-click the DFS link and click **Check status**.

Notes:

- To remove the status display from a link, right-click the link, and click **Clear status**.
- If VFM is actively monitoring the status of a link or its targets, clearing status only takes effect after VFM finishes checking status for the link.

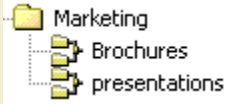
Delete a DFS link

When you delete a DFS link, the DFS logical structure is removed but the targets of the DFS link are not deleted.

1. Perform one of the following actions:
    - Select the DFS link and click **Delete** on the main toolbar.
    - Right-click the link and click **Delete**.
    - To delete all the links under a logical folder, right-click a logical folder and click **Delete**.
2. Click **Yes**.

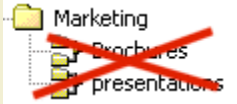
Notes:

- Links contained in any of the Admin policies must be removed from the policy before they can be deleted from the root.
- When you want to delete all the links under a logical folder, it is more efficient to delete the logical folder than it is to select all the links under the logical folder and delete the links.
- When a root runs on Microsoft Windows Server 2003 and you delete all the links under a logical folder, the logical folder is also removed. In Windows 2000, logical folders are not removed. This is a Microsoft Windows behavior. The following example illustrates this behavior.
    - The logical folder *Marketing* contains two links.



    - DFS root on Windows Server 2003. When links *Brochures* and *presentations* are deleted, the logical folder *Marketing* is also deleted.

    - DFS root on Window 2000. When links *Brochures* and *presentations* are deleted, the logical folder *Marketing* is is not deleted.



Manage link targets

- A link can have as targets:
    - 1 to N shared folders
    - 1 to N stand-alone DFS paths
    - Only 1 domain-based DFS path.
- When a link has two or more targets, the roots or shared folders that are the targets of the link provide alternate paths for the link.

View the target of a link

To display the target or targets (replicas) of a link:

1. Click the link in the Logical View tree.
2. On the **Properties** tab, scroll to **Targets**.

Notes:

- Right-click a target to display a context menu.
- Double-click a target to display where it is physically located on your network. The Physical View tree expands to display the machine where the target resides.
- Targets that are members of a client disaster recovery policy have radio buttons instead of check boxes next to them because only one target can be online. Replication status information appears to the right of each target in addition to the storage status information available for all targets.

Add targets to a link

Add multiple copies of a shared folder to a link. This provides fault tolerance and load balancing to control network traffic at the share level.

- There are two ways that you can add link targets.
  - Quickly add multiple targets at one time. Use this method when the path pattern of the target you want to rebase is the same as the path pattern of the target you want to add to the link. For example, you can rebase the link target `\\secure.npb.com\engineering` with `\\saturn.ppn.com\engineering` but you cannot rebase the link target `\\secure.npb.com\engineering` with `\\saturn.ppn.com\dept\engineering` because they do not have the same path pattern.
  - Add target paths and update how long a reference to the link is cached on the client. Use this method when the path pattern of the existing link target is different from the path pattern of the target you want to add to the link. For example, you have an existing link target `\\secure.npb.com\engineering` and you want to add another link target `\\saturn.ppn.com\dept\engineering`.
- The target of a link must be one of the following types:
  - 1 to N shared folders
  - 1 to N stand-alone DFS paths
  - Only 1 domain-based DFS path

Note: Configuring other combinations of link targets might prevent link target failover from functioning correctly.

To quickly add multiple link targets

1. Right-click a link and click **Clone**.
2. Perform one of the following actions:
   - When the link contains multiple targets, select the target that you want to rebase and click **Next**.
   - When the link contains one target, continue with Step 3.
3. Select which part of the UNC path of the link target you want to rebase.
4. Perform one of the following actions:
   - Type the name of a machine or multiple machines that you want the link to target. Separate machine names with a semicolon (;). Machine names can be written in any of the following formats:

Format	Example
machine name	secure;saturn
UNC path	\\secure.npb.com;\\saturn.ppn.com
Path	secure.npb.com;\\saturn

   - Click **Browse** to find a machine in your network.
5. Click **Next**. VFM shows the target you want to rebase and the new link targets that will be created.
6. Click **Finish**.

To add a link target

1. Right-click a link and click **Add replica**.
2. Click in **Send the user to one of these share folders or directories** and perform one of the following actions:
   - Type the path of a folder and continue with Step 6.
   - Click **Browse** to find a folder on the network and continue with Step 3.
3. Expand the tree for the domain or click the domain.
4. Double-click a machine to display a list of shared folders.
5. Click OK.
6. To add another target, click Add and repeat Step 2.
7. Click **OK**.

Notes:

- The contents of the targets of a link are synchronized when the link is a member of a disaster recovery or replication policy.
- For links that are not members of a disaster recovery or replication policy, you must either rely on other mechanisms when possible or manually ensure that the contents of the links targets stay synchronized.

Change storage status of a link target

- A link target on DFS roots hosted on Windows 2000 or Windows Server 2003 can be taken offline. The action does not remove the target from the link. The target is temporarily unavailable to DFS clients (not included in referrals to the DFS client).
- Links with multiple targets that are members of disaster recovery policies can only have one target online. Targets of those links appear in VFM with radio buttons.
- Referrals for the link do not contain information about the offline target, although clients already accessing the target continue to do so until they request a fresh referral.

To take a link target offline

1. Click the link that references the shared folder to display the **Properties** tab in the right pane.
2. Under **Targets** on the **Properties** tab, perform one of the following actions:
    - Clear the check box next to a target.
    - Select a radio button next to a target to take the online target offline. Targets that are members of a client disaster recovery policy have radio buttons instead of check boxes because only one target can be online. When you select a target, you perform a manual failover. The selected target becomes the active target.
    - Right-click the folder and click **Toggle Storage Offline/Online**.

Note: The offline status indicator appears on the folder.

To put a link target online

1. Click the link that references the shared folder. A **Properties** tab appears in the right pane.
2. Under **Targets** on the **Properties** tab, perform one of the following actions:
    - Select the check box or radio button next to a target. Targets that are members of a client disaster recovery policy have radio buttons instead of check boxes because only one target can be online. When you select a target, you perform a manual failover. The selected target becomes the active target.
    - Right-click the offline folder and click **Toggle Storage Offline/Online**.

To change the storage status of all or selected targets

Quickly change the storage status of all or selected targets in a folder or root.

1. Click a root or folder in the Logical View tree to display the **Properties** tab in the right pane.
2. Under **Links**, select the links of the targets you want to change.
3. Right-click and click **Toggle all targets online** or **Toggle all targets offline**.

Monitor link targets

If status monitoring is turned on for links, you can turn on status monitoring for the targets of the links. Monitoring link targets provides additional information about the "health" of your namespace configuration by checking whether the targets of links are available.

1. Perform one of the following actions:
    - Right-click the root and click **Properties**

- Click the root to display the **Properties** tab and click Edit.

3. Click the Status Monitoring tab and select Monitor targets every.
4. Enter how often (in minutes) you want to check the status of each target when it is online.
5. Enter how often (in minutes) you want to check the status of each target when it is offline.

Check status of a link target

If needed, you can manually check the status of a link target to ensure that it is still valid.

1. In the Logical View tree, click the link that references the shared folder to display the **Properties** tab in the right pane.
2. Under **Targets** on the **Properties** tab, right-click the target and click **Check status**.

Note: To remove the status display from a link target, right-click the target and click **Clear status**.

View size of data in the namespace

View the size and amount of space used by data in the namespace.

Perform one of the following actions:

- Right-click a root, link, or logical folder in the Logical View and click **Properties**.
- Right-click a share or directory in the Physical View and click **Properties**.

The size of the information contained in that portion of the logical namespace displays, along with the number of files, folders, and links when it is applicable.

Refresh a shared folder

You can update the information about a shared folder.

Notes:

- To refresh the information about all the items in both the Logical View and Physical View, click **Refresh all** on the **View** menu.
- To refresh the information about all the items in the logical or physical views, right-click Logical View or Physical View in the tree and click **Refresh**.

Perform one of the following actions:

- Right-click a shared folder and click **Refresh**.
- Select a shared folder and press **F5**.
- Select a shared folder and click **Refresh** on the main toolbar.
- Select a shared folder and click **Refresh** on the **View** menu.

View targets replicated with FRS

Check the File Replication Service (FRS) status of the targets of a domain-based DFS root.

1. Click the root or link to display the **Properties** tab in the right pane.
2. VFM returns one of the following values for **FRS Replication**:
    - **Unknown** - Status monitoring is not turned on for the root or VFM has not checked status.

- **On** - All the targets for the root have FRS replication turned on.
- **Off** - FRS replication is not turned on for the root.
- **Partial** - Only some of the targets of the root have FRS replication turned on. (DFS roots or DFS links only)

Note: VFM replication does not rely on FRS.

View contents of a link target

View the contents of DFS link replicas. To browse the contents of a replica, you must make it the active target.

1. In the Logical View tree, click a DFS link with replicas.
2. Click the **Explorer** tab in the right pane.
3. Right-click a DFS link replica, point to **Target,** and click the replica you want to activate. The contents of the replica appear in the right window.

Notes:

- You can also view the contents of a link, share, or folder. In the Logical View tree or Physical View tree, right-click an item, point to **External Tools**, and click **Explorer**.
- Changing the active target only changes the target the VFM console machine is viewing. It does not change what other users of the namespace see.

Compare contents of link targets

Compare the contents of the targets of a link .

1. Click a link under the Logical View to display its properties in the right pane.
2. Under **Targets**, select the targets you want to compare.
3. Right-click, point to **Reports**, point to **Physical**, and click **File Differences**. The first target on the list that you selected appears in the **Compare** field.
4. Click **Next**.
5. Type a name for the report and the location where you want to save it.
6. Click **Finish**.

Note: You can also compare contents of shares in the Physical View. Right-click a share, point to **Reports**, and click **File Differences**.

Delete a link target

When a link contains multiple targets, you can delete a target without deleting the link from the namespace. The target is only removed from the logical structure or namespace. The target is not deleted from the machine where it resides.

1. In the Logical View tree, click the link that references the shared folder to display the **Properties** tab in the right pane. Under **Targets** on the **Properties** tab, right-click the target and click **Delete**.
2. Click **Yes**.

Monitor status

Monitoring the status of roots, links and targets

- The status of roots and links are monitored.
- You can control whether and how frequently the status of items in the namespace are checked.
- Monitoring the status of link targets is optional.
- When links and shares are monitored, the status report for a root includes information about all the items that make up the root. For example, a root with unavailable targets has a status report that includes a list of the targets and their status.
- Links in a client disaster recovery policy show "unknown" status until monitoring has run at least once for the policy. Monitoring is necessary to perform failover of links that participate in disaster recovery policies.
- On the **Status** tab of a root, right-click an item to view menu options.
- Monitoring resources generates network traffic between the VFM components and the resources being monitored. Slower polling rates generate less traffic but provide less timely notification of problems in the monitored namespace.

Monitoring status of data replication

- When you use VFM replication in a replication policy, replication status monitoring is available to the policy and its targets.
- Place the cursor over an item to quickly display information about the item.
- If status monitoring is turned on for the links and folders contained in a replication policy, status indicators are displayed for the items on the **Replication** tab that appears in the right pane when you select a policy.

Modify status monitoring properties

When you create a namespace, the status of the root and links contained in the root are monitored. You can control whether and how frequently the namespace is monitored. You can also select Link targets for monitoring.

1. Right-click a root and click **Properties**.
2. Click the **Status Monitoring** tab.
3. Perform one of the following actions:
    - To turn off monitoring the root, clear the **Monitor status every** check box.
    - To change how often the root is monitored, click the arrows to change **minutes when online** and **minutes when offline**.
4. Select the **Monitor links every** check box to monitor the status of every link in the namespace. Click the arrows to change **minutes when online** and **minutes when offline**.
5. Select the **Monitor targets every** check box to monitor the status of every target in the namespace. Click the arrows to change **minutes when online** and **minutes when offline**.

Notes:

- You can also update status monitoring by clicking a root to display the **Properties** tab in the right pane.
- Monitoring resources generates network traffic between the VFM components and the resources being monitored. Slower polling rates generate less traffic but provide less timely notification of problems in the monitored namespace.

Chapter 3 Populate the Namespace Automatically

Namespace creation policies enable you to easily populate and maintain a namespace. You can use namespace creation features interactively to perform the initial population of your namespace. After the namespace is in place, the policies can automatically run on a scheduled basis to scan for changes in the physical resources supporting the namespace. You can configure policies to report changes or to update the namespace automatically to reflect the changes detected by the policy.

This section provides instructions about how to configure and manage namespace creation policies. Before you create your first policy, see "Namespace creation policy planning considerations."

Configure a namespace creation policy

Configure a namespace creation policy to automatically populate the logical namespace and to keep the logical namespace aligned with subsequent changes in the underlying storage resources.

1. Perform one of the following actions:
   - On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, and click **Creation Policy**.
   - Right-click the **Namespace Policies** folder in Admin View, point to **New**, and click **Creation Policy**.
   - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Creation Policy**.
2. Click **Next**.
3. Type a word or phrase that best describes this policy in the **Name** field (optional).
4. Clear **Automatically modify namespace after scanning** if you do not want to automatically create links for items that match the search criteria. After the policy runs, the items are listed under "New Resources" on the Properties tab that appears in the right pane when the policy is selected. You can create links for the items you want to include in the namespace.
5. Select one of the following:
   - **Search for items not already targeted from this policy's folder** when you do not want to target shares, subfolders, NetApp filer volumes, or qtrees that are already targeted by links in the folder. This is the default.
   - **Search for items not already targeted from this root** when you do not want to target shares, subfolders, NetApp filer volumes, or qtrees that are already targeted by links in the DFS root.
6. Select **Remove links whose shares or folders no longer exist** when you want to remove links targeting shares or subdirectories when a scan detects that the items no longer exist.
7. Select **Remove links from the entire root** when the links created by the policy are listed under a folder and you want to scan the entire root and remove links targeting the shares

or subdirectories that no longer exist.

8. From the **Use the Monitor on** list, optionally select the machine where another monitoring agent is located.
9. Select whether you want to limit the number of links that are added every time the policy runs. Accept the limit specified or change the limit. When this option is cleared, adds links are added for all the candidates found. Microsoft recommends limits to the number of links that are added to a DFS root. See the overview for DFS for detailed information about recommended size limits.
10. Click **Next**.
11. Select an existing DFS root or click **New** to create a new DFS root to contain the links, and click **Next**.
12. Group the links in a folder or add them under the root. Perform any of the following actions:
    - In the **Name** field, type a different name for the folder.
    - Click **New Folder** to create a new folder or subfolder.
    - Click **Delete** to remove the selected folder.
    - Click the root to add the links under the root.
13. Click **Next**.
14. Select the domain or domains that you want to search or select devices, and click **Next**.
15. Type a word or pattern in the **Search String** field. You can use DOS wild-card characters (* or ?) in the search string. You can use the asterisk (*) as a substitute for zero or more characters in a name and the question mark (?) as a substitute for a single character in a name. You can combine search strings by separating them with semi-colons; for example, entering mkt*;sales* finds all shares on the selected domains or servers whose names begin with either mkt or sales.
16. Select a search type.
17. If you selected "Search shares matching the search string for folders matching the following path," type a folder search string.

    Note: To search for folders, the VFM account must have "Read" and "List Folder Contents" permissions for the shares and subdirectories that match the search criteria.
18. (Optional) Select **Allow Partial Matches** if you want to search for partial matches.
19. (Optional) Select **Linked through target share if the target folder is also shared** when you want to create links that directly target shared subdirectories that match the folder search string.
20. (Optional) Search for hidden and administrative shares.
21. Click **Next**. A list of items that match your search string appears.
22. Clear the check box of items that you do not want to add, and click **Next**.
23. Select a template to arrange how links appear in the namespace. You can preview the namespace.
24. Click **Next**.
25. Rearrange the links, if desired. You can move a link or folder, add a folder, add more links, remove a link or folder from the namespace, and update the properties of a link.
26. Click **Next**.

25. Select **Use Schedule**.
26. Select how frequently you want to scan for items and click **Next**.
27. Click **Finish**. The new policy appears under the Creation Policies folder.

Notes:

- If you uninstall a monitoring agent, ensure that namespace creation policies that formerly used the uninstalled agent are reassigned to a currently available agent. Right-click a namespace creation policy and click **Properties**. On the General, tab, select a monitoring agent from the "Use this Monitor on" list.
- The Namespace Creation wizard creates links that reference volumes or qtrees regardless of their share status. Links that reference volumes or qtrees that cannot be accessed because they are not shared appear as broken links in the namespace.
- Permission based namespace policies enable you to populate the namespace based on share security permissions. For instruction about how to create a permission based namespace policy, see "Configure a permission based namespace policy."

Update the schedule

Make changes to the schedule of a namespace creation policy.

1. Perform one of the following actions:
   - Right-click a namespace creation policy and click **Properties**.
   - Select a namespace creation policy to show a Properties tab in the right pane, and click Edit **Edit**.
2. Click **Schedule**.
3. Perform any of the following actions:
   - Click **Add** and configure a new schedule.
   - Select an existing schedule from the list and update it.
   - Select **Use alternate schedule when the policy fails** to attempt to run the policy at a stated frequency until the policy runs successfully.
4. Click **OK**.

Add or remove servers or domains

Add or remove servers and domains that a namespace creation policy scans.

1. Perform one of the following actions:
   - Right-click a namespace creation policy and click **Properties**.
   - Select a namespace creation policy to show a Properties tab in the right pane and click Edit
2. Click **Domains**.

3. Perform any of the following:
    - Click **Add** to browse for domains and servers to include in the policy.
    - To remove a server or domain from the policy, select it and click **Remove**. If a server being removed from the policy has shares being referenced by links, you have the option of removing the links from the namespace.
4. Click **OK**.

Add items to an exclusion list

Maintain an exclusion list of resources you do not want to reference from the namespace. The items on the exclusion list are ignored when a search is performed for resources to add to the namespace.

1. Perform one of the following actions:
    - Right-click a namespace creation policy and click Properties.
    - Select a namespace creation policy to show a Properties tab in the right pane and click Edit.
2. Click **Target Search Ignore List**.
3. Click **Add** and select items to include in the list.
4. Click **OK**.

Note: When you create a new policy using the Namespace Creation wizard and you clear items from the search results list, the cleared items are added to the Ignore List of the policy.

Change the search type

Select a different item to search to update the namespace. You can search for shares, subfolders, NetApp filer volumes, or qtrees. The next time the policy runs, it scans for the new items.

1. Perform one of the following actions:
    - Right-click the namespace creation policy and click **Properties**.
    - Select a namespace creation policy to show a Properties tab in the right pane and click Edit.
2. Click **Target Search**.
3. In the Search Type list, select a different item to search.
4. Optionally update the search string.
5. If you selected "Search Folders" as the search type, type a folder search string. The policy searches for subdirectories matching the folder search string of shares matching the string in the **Search string** field.
    - If you want to search for partial matches, select **Allow Partial Matches**.
    - If you want to create links that directly target shared subdirectories found, select **Linked through target share if the target folder is also shared**..
6. Click **OK**.

Change the search string of a policy

Change the search criteria for a namespace creation policy.

1. Perform one of the following actions:
   - Right-click a namespace creation policy and click **Properties**.
   - Select a namespace creation policy to show a **Properties** tab in the right pane and click Edit.
2. Click **Target Search**.
3. In the **Search string** field, type a new word or pattern to match shares, volumes, or qtrees.
4. Optionally update the folder search string if "Search Folders" is the search type.
5. Click **OK**.

Change how the links are arranged

Change how new links are arranged in the namespace. Select a different template for a namespace creation policy. The next time the policy runs, the new links are arranged according to the new template. Existing links are not affected.

1. Perform one of the following actions:
   - Right-click the namespace creation policy and click **Properties**.
   - Select a namespace creation policy to show a Properties tab in the right pane and click Edit.
2. Click **Target Search**.
3. Select a new template from the Hierarchy Template list. A graphic view of how new links will be arranged in the namespace appears in the lower part of the dialog box.
4. Click **OK**.

Scan for items immediately

You can bypass the namespace creation policy schedule and manually start the scanning process any time you want.

1. Perform one of the following actions:
   - Right-click a namespace creation policy and click **Start Scanning Now**.
   - Select a namespace creation policy to show a Properties tab in the right pane, right-click anywhere on the tab, and click **Start Scanning Now**.
2. Click **Scan**. If items that match the search criteria are found, they appear under the DFS root that contains the links.
3. Perform one of the following actions:
   - Click **Create** to add the links that reference the items to the namespace.
   - Click **Cancel** if you do not want to add the links or if you want to have the option of selecting which links in the list you want to add to the namespace.

4. To review the list of new items, select the policy to show the Properties tab on the right pane. Under New Resources, right-click an item and perform one of the following actions:
    - Click **Add as Link** to create a link and add it to the namespace.
    - Click **Ignore** if you do not want to reference the item from the namespace. The item is added to the policy Ignore list. The next time the policy is scanned, these items do not show up as new resources.

Review the list of new resources before adding links

You can set up a namespace creation policy so that you can always review scanning results and determine which items you want to reference from the namespace.

1. Perform one of the following actions:
    - If you are creating a new namespace creation policy, clear **Create links after scanning**.
    - If you want to change an existing policy, right-click the policy and click **Properties**. On the General tab, clear **Create links after scanning**.
2. When items are scanned, search results are listed under **New Resources** on the Properties tab of the policy. To display the Properties tab, select the policy and the tab appears on the right pane.
    - To reference an item from the namespace, right-click the item and click **Add as Link**.
    - If you do not want to reference an item in the namespace and you do not want to show the item again after the next scan, click **Ignore**. The item is added to the Ignore list for the policy. To view the list, right-click the policy, click **Properties**, then click **Ignore List**.

Delete a namespace creation policy

To delete a namespace creation policy, perform one of the following actions:

- Right-click the policy and click **Delete**.
- Select the policy and press the **Delete** key.
- Select the policy to show a Properties tab in the right pane. Right-click anywhere on the page and click **Delete**.

Chapter 4 Populate the Namespace based on Permissions

Permission based namespace policies enable you to populate a logical namespace based on the group permissions of shared folders and their subdirectories. Like namespace creation policies, permission based namespace policies enable you to easily populate and maintain a logical namespace. You can use these policies, like namespace creation policies, to perform the initial population of your namespace. After the namespace is in place, the policies can automatically run on a scheduled basis to scan for changes.

This section provides instructions about how to configure and manage permission based namespace policies.

Note: The VFM account must have permission to read the security descriptor of the shares and underlying folders you want the policy to scan.

Configure a permission based namespace policy

Configure a permission based namespace policy to automatically populate the logical namespace and to keep the logical namespace aligned with subsequent changes in the security permissions of underlying storage resources. Permission based namespace policies enable you to group shares in the namespace based on security permissions. The VFM account must have permission to read the security descriptor of the shares and underlying folders you want the permission based namespace policy to scan.

1. Perform one of the following actions:
    - On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, and click **Permission Based Policy**.
    - Right-click the **Namespace Policies** folder in Admin View, point to **New**, and click **Permission Based Policy**.
    - Right-click the **Permission Based Policies** folder and click **New Permission Based Policy**.
    - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Permission Based Policy**.
2. Click **Next**.
3. Type a word or phrase that best describes this policy in the **Name** field.
4. Clear **Automatically modify namespace after scanning** if you do not want to automatically create links for items that match the search criteria. After the policy runs, the items are listed under "New Resources" on the Properties tab that appears in the right pane when the policy is selected. You can create links for the items you want to include in the namespace.
5. Select one of the following:
    - **Search for items not already targeted from this policy's folder** when you do not want to target shares and subfolders that are already targeted by links in the folder. This is the default.
    - **Search for items not already targeted from this root** when you do not want to target shares and subfolders that are already targeted by links in the DFS root.

6. Select **Remove links whose shares no longer exist** when you want to remove links targeting shares when a scan detects that the shares no longer exist.
7. Select **Remove links from the entire root** when you want to scan the entire root and remove links targeting shares that no longer exist.
8. From the **Use the Monitor on** list, optionally select the machine where another monitoring agent is located.
9. Select whether you want to limit the number of links that are added every time the policy runs. Accept the limit specified or change the limit. When this option is cleared, links are added for all the candidates found. Microsoft recommends limits to the number of links that are added to a DFS root. For information about recommended size limits, see the overview for DFS .
10. Click **Next**.
11. Select an existing DFS root or click **New** to create a new DFS root to contain the links, and click **Next**.
12. Group the links in a folder or add them under the root. Perform any of the following actions:
    - In the **Name** field, type a different name for the folder.
    - Click **New Folder** to create a new folder or subfolder.
    - Click **Delete** to remove the selected folder.
    - Click the root to add the links under the root.
13. Click **Next**.
14. Select the domain or domains that you want to search or select devices, and click **Next**.
15. Click **Add** to browse for security groups that have access to resources on the domain or servers you selected.
16. Type a word or pattern in the **Search String** field. You can use DOS wild-card characters (* or ?) in the search string. You can use the asterisk (*) as a substitute for zero or more characters in a name and the question mark (?) as a substitute for a single character in a name. You can combine search strings by separating them with semi-colons; for example, entering mkt*;sales* finds all shares on the selected domains or servers whose names begin with either mkt or sales.
17. Select a search type.
18. If you selected "Search shares matching the search string for folders matching the following path", type a folder search string.

    Note: To search for folders, the VFM account must have "Read" and "List Folder Contents" permissions for the shares and subdirectories that match the search criteria.
19. (Optional) select **Allow Partial Matches** if you want to search for partial matches. For an explanation about how partial matches works, see the "Notes" in the namespace creation topic "Change the search type."
20. (Optional) select to search hidden and administrative shares.
21. Click **Next**. A list of items that match your search criteria appears.
22. Clear the check box of items that you do not want to add, and click **Next**.
23. Select a template to arrange how links appear in the namespace. You to preview the namespace.

Note: If you selected domains to search for resources and the domains contain groups with the same name (for example, domain1\sales and domain2\sales), make sure that you select a template that sorts by domain, such as Domain-Group Name-Machine-Shares, Machines-Domain-Group Name-Shares, or Domain-Group Name-Shares. You cannot create links with the same name under the root or a logical folder of the namespace.

24. Click **Next**.
25. Optionally rearrange the links. You can move a link or folder, add a folder, add more links, remove a link or folder from the namespace and update the properties of a link.
26. Click **Next**.
27. Select **Use Schedule**.
28. Select how frequently you want to scan for items and click **Next**.
29. Click **Finish**. The new policy appears under the Permission Based Policies folder.

Notes:

- If you uninstall a monitoring agent, ensure that the permission based policies that formerly used the uninstalled agent are reassigned to a currently available agent. Right-click a permission based policy and click **Properties**. On the General tab, select a monitoring agent from the "Use this Monitor on" list.
- Namespace creation policies enable you to populate the namespace with links that reference shares, volumes, and qtrees. For instructions about how to create namespace creation policies, see "Configure a namespace creation policy."

Update the search criteria

Update the search criteria.

To change security groups

1. Perform one of the following actions:
   - Right-click the permission based namespace policy and click **Properties**.
   - Select a permission based namespace policy to show a Properties tab in the right pane and click Edit.
2. Click **Groups**.
3. Perform one of the following actions:
   - Click **Add** to include additional groups
   - Select a group and click **Remove** to delete the item from the list.
4. Click **OK**.

To change search type or search string

See the following namespace creation policy topics:

- Change the search type
- Change the search string of a policy

Other options

To update the permission based namespace policy, see the following namespace creation policy topics:

- Update the schedule
- Add or remove servers or domains
- Add items to an exclusion list
- Change how the links are arranged
- Scan for items immediately
- Review the list of new resources before adding links

Delete a permission based namespace policy

To delete a permission based namespace policy, perform one of the following actions:

- Right-click the policy and click **Delete**.
- Select the policy and press the **Delete** key.
- Select the policy to show a Properties tab in the right pane. Right-click anywhere on the page and click **Delete**.

Chapter 5 Make the Namespace Highly Available

Namespace availability policies enable you to keep the logical structure of two or more DFS roots and/or a DFS root and widelink namespaces aligned.

- By synchronizing roots, you can load balance the work on your DFS root server across multiple identical instances of the root. This also provides fault tolerance because the namespace is available from more than one server.
- By synchronizing a DFS root and a widelink namespace, your CIFS clients can access the namespace hosted on a filer.
- A namespace availability policy provides flexibility in configuring your namespace to make it highly available. See "Namespace configuration options."

This section provides instructions about how to create and manage policies to synchronize the logical structure of DFS roots and widelink namespaces to make them highly available. Before you create your first policy, see "Namespace availability planning considerations."

Note: You can create disaster recovery policies to make data highly available.

Create a namespace availability policy checklist

To create your first policy, follow the basic steps listed below:

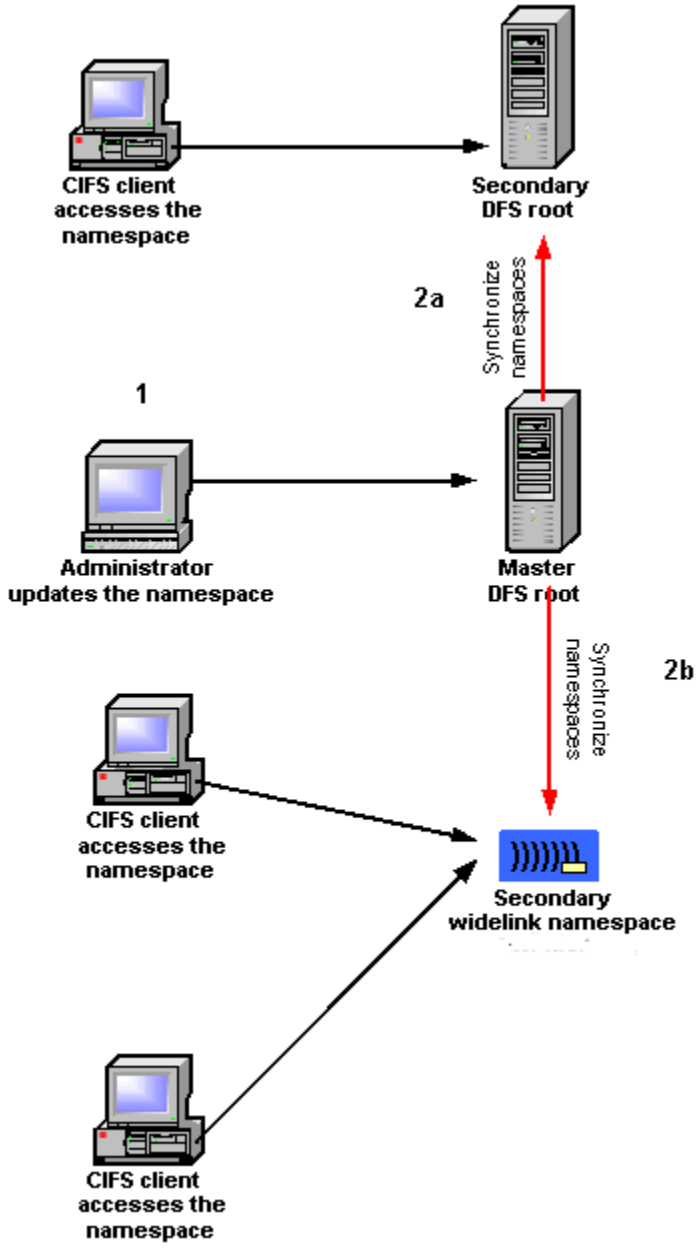
1. Make DFS roots highly available or create a widelink namespace.
2. Schedule synchronization.

Namespace configuration options

You have the flexibility of configuring your namespace in several ways to make it highly available.

- You can host the namespace on a filer.
    - You configure a namespace availability policy with a master DFS root and at least one secondary CIFS share on a NetApp filer where you will host a widelink namespace.
    - The logical structure of the DFS root is synchronized with the widelink namespace.
    - Your CIFS clients access the namespace on the filers.
- You can host the namespace on a filer and Windows systems or only Windows systems. See the illustration below.
    - You configure a namespace availability policy with a master DFS root and at least one secondary CIFS share on a filer and/or secondary DFS root on a Windows system.
    - The logical structure of the master DFS root is synchronized with the secondary root and widelink namespace hosted on the secondary share.
    - Your CIFS clients access the namespace on a filer and/or Windows system.

30BNamespace configuration options



Note: Namespace availability policies do not support creating widelink namespaces on shares hosted on vFilers.

Make DFS roots highly available

Namespace availability policies enable you to synchronize the logical structure of two or more DFS roots

1. Perform one of the following actions:
   - On the **Tools menu**, click **New Policy**, point to **Namespace Policy**, then click **Availability Policy**.
   - Right-click the **Namespace Policies** folder in the Admin View, point to **New**, and then click **Availability Policy**.
   - Right-click the **Availability Policies** folder and click **New Availability Policy**.
   - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Availability Policy**.
2. Type a word or phrase that best describes this policy in the **Name** field.
3. Click **Add** and type the path of a root or click ... **Browse** to locate a root in your network.
4. Repeat Step 3 to add more roots. The policy must have at least two roots.
5. Select the master root. Secondary roots mirror the logical structure of the master root.
6. Select **Synchronize after scanning**.
7. Click **OK**.

Notes:

- Roots containing links participating in disaster recovery policies can also be members of namespace availability policies.
- In this configuration, as with disaster recovery policies containing links hosted on replicated domain-based roots, it is recommended that you configure the disaster recovery policies for manual fail over rather than for automatic fail over if the links target read/write data rather than read-only data.

Create a widelink namespace

Namespace availability policies enable you to create widelink namespaces on NetApp filers and synchronize the logical structure of a master DFS root with the widelink namespace. This enables CIFS clients to access the namespace directly through a filer instead of a Windows server.

Notes:

- The filer where you want to create a widelink namespace must be running Data ONTAP 6.4 or later.
- Namespace availability policies do not support creating widelink namespaces on shares hosted on vFilers.

To create a widelink namespace

1. Perform one of the following actions:
   - On the **Tools menu**, click **New Policy**, point to **Namespace Policy**, then click **Availability Policy**.
   - Right-click the **Namespace Policies** folder in the Admin View, point to **New**, and then click **Availability Policy**.
   - Right-click the **Availability Policies** folder and click **New Availability Policy**.
   - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Availability Policy**.
2. Type a word or phrase that best describes this policy in the **Name** field (optional).
3. Click **Add** in the **Synchronize the following roots** field and type the path of the root, or click ... **Browse** to locate a root in your network.
4. Click **Add** in the **Synchronize the following NetApp filer shares** field and type the path of the share, or click ... **Browse** to locate the share in your network.
5. Select **Synchronize after scanning**.
6. Click **OK**. When the policy runs, a widelink namespace hosted on the CIFS share specified in the policy is created and the logical structure of the master DFS root is synchronized with the widelink namespace.

Note: For performance reasons and to avoid possible conflict with widelinks that might already exist under an existing share, it is recommended that you create and share a directory for hosting a widelink namespace instead of using an existing share. the contents of a share assigned to host a widelink namespace is scanned and all widelinks found on the share are managed.

Namespace synchronization options

You can choose whether the logical structure of the roots and widelink namespaces should be automatically synchronized each time a namespace availability policy runs, or whether to be informed when the logical structure of the roots and widelink namespaces are not the same.

- **To automatically synchronize at specified times**

  Make sure that the "Synchronize after scanning" properties option is selected for a policy then schedule synchronization.
- **To scan the roots for differences at specified times**

  Make sure that the "Synchronize after scanning" properties option is cleared for a policy and that you scheduled synchronization. The roots and widelink namespaces are scanned according to the schedule and you are provided the scanning results, but the logical structure of the roots and widelink namespaces is not modified.
- **To manually synchronize root structures**

  Use the "Start synchronization now" option to manually initiate the synchronization of the logical structure of the roots and widelink namespace in the policy. If you did not select the "Synchronize after scanning" properties option, you can synchronize after scanning is complete. Manually initiated scans or synchronizations are performed directly by the VFM server rather than by a monitoring agent to which the policy is assigned. This is because of the additional status information and user interaction provided by manually initiated scans.

Schedule synchronization

To make sure that changes made to the logical structure of the master root are synchronized with the secondary root and/or secondary widelink namespace, schedule how frequently you want to synchronize the logical structure.

1. Perform one of the following actions:
   - Right-click the namespace availability policy and click **Properties**.
   - Select a namespace availability policy and click Edit on the **Properties** tab that appears in the right pane.
2. Click **Schedule Monitoring**.
3. Click **New** to configure a new schedule.
4. Optionally, select **Use alternate schedule when the policy fails** and type a frequency, in minutes, to run the schedule any time replication fails.
5. Click **OK**.

Start synchronization immediately

You can bypass the synchronization schedule and manually start the synchronization process any time you want.

Manually initiated scans or synchronizations are performed directly by the VFM server rather than by a monitoring agent to which the policy is assigned. This is because of the additional status information and user interaction provided by manually initiated scans.

1. Perform one of the following actions:
   - Right-click a namespace availability policy and click **Start Synchronization Now**.
   - Click a namespace availability policy to show a Properties tab in the right pane. Right-click anywhere on the Properties tab and click **Start Synchronization Now**.
   - Click the **Availability Policies** folder to show a list of policies in the right pane. Right-click a policy and click **Start Synchronization Now**.

   The synchronization operation scans the logical structure of the roots and widelink namespaces in the policy and, if differences are detected between the master and secondary roots and widelink namespaces, changes are applied to the secondary roots and widelink namespaces to align their structure with that of the master root.
2. Expand the tree to view scanning results. If an error message appears, correct the problem before synchronizing. If no error messages appear, click Synchronize.

Notes:

- This menu item is disabled if a synchronization operation is in progress.
- To view detailed information about the synchronization operation, click the policy to show an Events tab in the right pane. Double-click the "Synchronization completed successfully..." event and expand the tree under Details.

Add additional roots or shares to a policy

A namespace availability policy must contain at least two DFS roots or a root and a widelink namespace. A policy can contain an unlimited number of roots and widelink namespaces.

Drag a root or CIFS share to a policy

You can add DFS roots and CIFS shares that will host widelink namespaces.

- Drag a root from the Logical View or right pane to a namespace availability policy.
- Drag a CIFS share on a filer from the Physical View tree or right pane to a namespace availability policy. The filer hosting the share must be running Data ONTAP 6.4 or later.

Add a root or share to a policy

1. Perform one of the following actions:
    - Right-click the namespace availability policy and click **Properties**.
2. Select a namespace availability policy and click Edit on the **Properties** tab that appears in the right pane.
3. Click General.
4. Click Add and type the path of a root, or click ... Browse to locate a root in your network.
5. Click Add in the Synchronize the following NetApp filer shares field and type the path of a CIFS share, or click ... Browse to locate a CIFS share on a filer in your network.
6. Repeat Steps 3 and 4 to add more roots and shares.
7. Click OK.

Note: When you add a CIFS share to a namespace availability policy, the filer is added to the All Resources and NetApp Filer Resources folders in the Physical View.

Remove roots and widelink namespaces

If you no longer want a DFS root or widelink namespace to participate in a namespace availability policy, perform one of the following actions:

- Right-click a root in the Logical View tree and click **Remove from Namespace Availability Policy**.
- Select a namespace availability policy to display a Properties tab in the right pane. Right-click a root or widelink namespace on the Properties tab and click **Remove from Namespace Availability Policy**.
- Double-click a namespace availability policy, right-click a root or widelink namespace under the policy, and click **Remove from Namespace Availability Policy**.

Change the master root of a policy

To designate the master root for a synchronization policy, perform one of the following actions:

- Select a namespace availability policy to display a **Properties** tab in the right pane. On the Properties tab, select a root.
- Right-click a namespace availability policy and click **Properties**. On the General dialog box, select a root.

Delete a namespace availability policy

When you delete a namespace availability policy, namespace synchronization is no longer available. DFS roots and widelink namespaces that were members of the policy can still be accessed.

1. Perform one of the following actions:
    - Right-click a namespace availability policy and click **Delete**.
    - Select the **Availabilities Policies** folder to display a Properties tab in the right pane. Right-click a policy and click **Delete**.
2. Click **Yes**.

Chapter 6 Create Multiprotocol Namespaces

Create a common namespace for UNIX and Windows users to provide access to files stored on NetApp filers. This presents a unified view of files to users. A multiprotocol namespace policy enables you to build namespaces for NFS clients to mirror the namespace presented to CIFS clients and to build namespaces for CIFS clients to mirror the namespace presented to NFS clients. You can automatically synchronize the namespaces. Before you create your first policy, see "Multiprotocol namespace planning considerations."

Create a multiprotocol namespace policy checklist

To create your first policy, follow the basic steps listed below:

1. Create a multiprotocol namespace policy.
2. Host a UNIX namespace on a filer.
3. Configure UNIX clients to access the namespace.
4. Select default UNIX settings.
5. Add a sync point.
6. Schedule synchronization

Create a multiprotocol namespace policy

Create a multiprotocol namespace for CIFS and NFS clients. You can automatically synchronize the namespaces.

1. Perform one of the following actions:
    - On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, and click **Multiprotocol Policy**.
    - Right-click the **Namespace Policies** folder in Admin View, point to **New**, and click **Multiprotocol Policy**.
    - Right-click the **Multiprotocol Policies** folder and click **New Multiprotocol Policy**.
    - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Multiprotocol Policy**.
2. In the **Name** field, type a word or phrase that best describes this policy. The name appears under the Multiprotocol Policies folder and on the Properties tab of items that are members of the policy.
3. Type the name of a DFS root that contains links that target data on NetApp filers, or click **Browse** to locate a root in your namespace.
4. Perform one of the following actions:
    - If synchronization is from a UNIX namespace to a DFS namespace, type a CIFS UNC path name for the directory that contains the automount files describing the UNIX namespace.
    - If synchronization is from a DFS namespace to a UNIX namespace, type a CIFS UNC path name for the directory that will contain files created by VFM to configure the UNIX namespace.
    - Click **Browse** to locate the directory.

Notes:

- The CIFS UNC path name you type in the **UNIX Files Location** text box must be accessible to the VFM server.
- The multiprotocol namespace enables users to access directories hosted on NetApp filers that are accessible through both NFS exports and CIFS shares.

5. From the **Use the Monitor on** list, optionally select the machine where another monitoring agent is located.
6. (Optional) Click **Select default share security** to select default share access permissions for all shares referenced by links contained the DFS namespace.
   - Click **Add** to select the users and groups to whom you want to assign permissions.
   - Select the permissions you want to allow each user or group.
   - Click **OK**.
7. Click **OK**.

Notes:

- Direct and indirect automount maps are supported. Auto_master files are not supported.
- The DFS and UNIX namespaces in a multiprotocol namespace policy must reference data on NetApp filers.
- VFM does not support the Solaris-specific automount options, such as running executables and evaluating environment variables when determining the actual export to mount.

Host a UNIX namespace on a filer

Automatically copy the contents of the export files it creates to the */etc/exports* file and to run the command `exportfs -a` to make the new exports visible to NFS clients.

1. Perform one of the following actions:
   - Right-click a multiprotocol policy and click **Properties**.
   - Select a multiprotocol policy to show a Properties tab in the right pane and click .
2. Click **Scripts**.
3. Select **Automatically apply exports**.
4. Click OK.

Configure UNIX clients to access the namespace

You can automatically copy automount files to NIS.

1. Perform one of the following actions:
   - Right-click a multiprotocol policy and click **Properties**.
   - Select a multiprotocol policy to show a Properties tab in the right pane and click Edit.
2. Click **Scripts**.
3. Select **Push automount files to NIS**.
4. Type the name of an NIS client machine.
5. Type the name of a directory on the NIS machine where the automount files are temporarily copied.
6. Type the path on the NIS machine where the `make` program is located.
7. Click **OK**.

Important:

Before you run the multiprotocol namespace policy, you must add the NIS server to the Physical View. See "Add a machine to the physical view" for instructions.

Note: NFS clients that are making use of the automount files must have the directory that is specified in the automount files.

Select default UNIX settings

Set options to control NFS client access to the data.

1. Perform one of the following actions:
   - Right-click a multiprotocol namespace policy and click **Properties**.
   - Select the Multiprotocol Namespace Policies folder to display a Properties tab in the right pane, then click Edit.
2. Click **Default UNIX Settings**. Select how you want to set up access restrictions. You can select from several export settings options.

To...	Then do this...
Allow only specific client machines access to the data	1. Select **Restricted Access**. 2. In the **Allow Access** field, type the names of the machines, subnets, or netgroups that are allowed access.
Allow read-only access to the data to all machines	Select **Read-Only**.

To...	Then do this...
Allow read-write access to specific client machines and read-only to all other machines	3. Select **Read-Only**. 4. In the **Allow Write Access** field, type the name of the client machines, subnets, or netgroups that are allowed read-write access.
Prevent root access to the data	Select **No Root Access**.
Allow root access to the data to all clients	Select **All Root Access**.
Allow root access to the data to only specific machines	5. Select **No Root Access**. 6. In the **Always allow Root Access** field, type the name of the client machines, subnets, or netgroups that always are allowed root access.

3. (Optional) Change how entries specified by the automount map are mounted. The following list specifies the VFM default mount options:
   - Mount resources read-write.
   - Allow set user ID execution.
   - Soft mount, return an error if the server does not respond.
   - Do not allow keyboard interrupts of a process waiting on a hard mount.
4. Click **OK**.

Add a sync point

Add synchronization points between the master and secondary multiprotocol namespaces. The secondary namespace is updated when the logical structure of the master namespace changes.

1. Perform one of the following actions:
   - Right-click a multiprotocol namespace policy and click **Properties**.
   - Select a multiprotocol namespace policy to show a **Properties** tab in the right pane and click Edit.
2. In the **General** dialog box, click **New**.
3. Type a word or phrase that describes the data synchronized between the DFS and UNIX namespaces.
4. Indicates the direction of the synchronization of the logical structure of the namespace.
   - If DFS is selected, whenever the links in the DFS Logical Folder change, the automount file and corresponding export files are updated.
   - If UNIX is selected, whenever the contents of the automount file changes, the links in the DFS Logical Folder are updated.

5. Type the name of the DFS namespace folder that contains links targeting data on NetApp filers or click **Browse** to select the folder contained in the DFS root you specified in the **DFS Root** field.
6. In the **Automount File** field, perform one of the following actions:
   - If DFS is the master, type a name for the automount file that will be create.
   - If UNIX is the master, type the name of an automount file or click **Browse** to select the file in the directory you specified in the **UNIX Files Location** field.
7. Click **OK**. The new sync point appears in the **Sync Points** list.
8. Repeat Steps 2 through 7 to create additional synchronization points.
9. Click **OK**.

Note: The DFS and UNIX namespaces in a multiprotocol namespace policy must reference data on NetApp filers.

Schedule synchronization

To make sure that changes made to the logical structure of the sync points are synchronized from the master namespace, schedule how frequently you want to synchronize the logical structure.

1. Perform one of the following actions:
   - Right-click the multiprotocol policy and click **Properties**.
   - Select a multiprotocol policy and click Edit on the **Properties** tab that appears in the right pane.
2. Click **Schedule**.
3. Click **Add** and configure the schedule.
4. Click **OK**.

Run customized commands during synchronization

Specify batch files to run before and after namespace synchronization.

1. Perform one of the following actions:
   - Right-click a multiprotocol namespace policy and click **Properties**.
   - Select a multiprotocol namespace policy to show a Properties tab in the right pane and click Edit.
2. Click **Scripts**.
3. Select **Run Batch File Before Sync** and type the path where the script file is located, or click **Browse** to locate the file in your network.
4. Select **Run Batch File After Sync** and type the path where the script file is located, or click **Browse** to locate the file in your network.
5. Click **OK**.

Notes:

- For detailed information about configuring batch files to run in VFM storage policies, see "Running batch files."
- For more information about the example scripts provided by VFM, see "Batch files."

Update a multiprotocol namespace policy

Make changes to a multiprotocol namespace policy.

1. Perform one of the following actions:
    - Right-click a multiprotocol namespace policy and click **Properties**.
    - Select the Multiprotocol Namespace Policies folder to display a Properties tab in the right pane, then click **Edit**.
2. Change the appropriate information.
3. Click **OK**.

Start namespace synchronization immediately

You can bypass the synchronization schedule and manually start the namespace synchronization process any time you want.

1. Perform one of the following actions:
    - Right-click a multiprotocol namespace policy and click **Start policy now**.
    - Select the Multiprotocol Policies folder to show a Properties tab in the right pane. Right-click a policy and click **Start policy now**.
2. Click **Done**.

Delete a sync point

When you delete a sync point from a multiprotocol namespace policy, synchronization between the master and secondary resources is canceled. UNIX and DFS clients continue to access their respective namespaces as they are currently configured.

1. Perform one of the following actions:
    - Right-click the policy and click **Properties**.
    - Select the policy to show a Properties tab in the right pane and click .
2. Click **General**.
3. Select the sync point you want to delete and click **Remove**.
4. Click **OK**.

Delete a multiprotocol namespace policy

When you delete a multiprotocol namespace policy, both DFS and UNIX clients can still access their respective namespaces as they are currently configured. Namespace synchronization is no longer available.

1. Perform one of the following actions:
    - Right-click a multiprotocol namespace policy and click **Delete**.
    - Select the **Multiprotocol Policies** folder to display a Properties tab in the right pane. Right-click the policy and click **Delete**.
2. Click **Yes**.

Chapter 7 Virtualize User Home Directories

The VFM Home Folder Policy Creation wizard guides you through the steps to creating a home folder policy.

Create a home folder policy

When users access their home directories from the namespace, you can load balance and migrate user data without affecting users. VFM enables you to group users in home folders to accommodate users from different domains and to place home directories at different points in the namespace. You can also organize users' home directories as subfolders to facilitate the creation of personal namespaces for users.

Before you begin, review DFS size limitations on the number of links contained in a DFS root.

1. Perform one of the following actions:
    - On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, and click **Home Folder Policy**.
    - Right-click the **Namespace Policies** folder in the Admin View, point to **New**, and then click **Home Folder Policy**.
    - Right-click the **Home Folder Policies** folder and click **New Home Folder Policy**.
    - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Home Folder Policy**.
2. Click **Next**.
3. Type a word or phrase that best describes this policy in the **Name** field. The name appears under Home Folder Policies and on the Properties tab of items that are members of the policy.
4. In the **Domain** field, type the name of the domain that contains the home directories, or click **Browse** to select a domain.
5. In the **DFS Root** field, type the name of the root that you want to add users' home directories, or click **Browse** to select a root.
6. In the **Link Template** fields, optionally type the name of folders where you want to group the home directories, and/or type the common name for the link that targets the users' home directory. If you select not to group users in folders, the users appear alphabetically by name in the Logical View under the DFS root selected. See "Organizing user home directories in the namespace" for examples of the different ways you can organize the user home folders.
7. Click **Next**.
8. Select the users you want to add to the namespace.
9. Select **Show users without a home folder** if you want to add users who do not have a home directory.
10. Click **Next**.
12. Click **Finish**.

Add a link to a user home folder

Customize user access to data.

Assumption

The home folder policy that contains the users was created to show user home directories in subfolders.

To add a link to a user home folder

1. Right-click a user home folder and click **Add link**.
2. Type the name you want to give the link in the **User connect to** field.
3. Click **Add** and type the name of a shared folder or directory, or click **Browse** to display a list of domains from which you can select a share or subfolder.
4. Click **OK**. The new data is accessed as a subfolder on the user's home folder.

To add a common link to multiple home folders

This organization can be useful, for example, when you need to give a set of users access to a directory containing information about a project on which they are collaborating.

1. Select the root that contains the user home folders to display a Properties tab in the right pane.
2. Select the user home folders listed under **Links**.
3. Right-click and click **Add link**.
4. Type the name you want to give the link in the **User connect to** field.
5. Click **Add** and type the name of a shared folder or directory, or click **Browse** to display a list of domains from which you can select a share or subfolder.
6. Click **OK**. The new data is accessed as a subfolder on the selected users' home folders.

Note: You can update identical links in one easy step. When you rename, add, remove targets, or change the timeout of a link that appears in several places in the namespace, a list of the identical links displays and you can update all the links simultaneously.

Add new users to a policy

Add new users to an existing home folder policy. If the users have home directories, they are added automatically to the namespace.

1. Perform one of the following actions:
   - Right-click the home folder policy to which you want to add users and click **Add Users**.
   - Right-click anywhere on the **Properties** tab of a home folder policy and click **Add Users**.
2. Select the users you want to add.
3. Select **Show users without a home folder** if you want to add users who do not have a home directory.

4. Click **Next**.
5. Click **Finish**.

View properties of a home folder policy

View the properties of a home folder policy.

1. Open **Home Folder Management** in the Admin View.
2. Perform one of the following actions:
    - Click a home folder policy. A Properties tab appears in the right pane. The list of users also appears in this tab.
    - Right-click a home folder policy and click **Properties**.

Refresh a home folder policy

Update the information for users in a home folder policy to reflect changes made in the domain.

Perform one of the following actions:

- Under the **Home Folder Policies** folder, right-click the home folder policy you want to update and click **Refresh**.
- Right-click anywhere on the Properties tab of the home folder policy and click **Refresh**.

Note: Refreshing the policy reevaluates how users named in the policy access their home folder but does not make any changes to the user accounts or to the links in the namespace.

Resolve discrepancies

Update user information and apply the rules you set for a home folder policy.

Discrepancies that VFM resolves

- **Users on the list with home directories but without a DFS link -** VFM adds links for the users to the namespace.
- **Users who were deleted from the domain -** VFM removes the users from the namespace but keeps their name on the list.
- **Users originally added to the list that did not have home directories -** VFM checks the domain, updates information for each user, and applies rules.

To resolve a discrepancy

Perform one of the following actions:

- Right-click anywhere on the **Properties** tab of a home folder policy and click **Apply Rules**.
- Right-click a home folder policy and click **Apply Rules**.

Remove a user from a home folder policy

When you remove a user from a home folder policy, the user is only removed from the policy and the namespace. The user's data is not removed from the domain. The home directory setting in the user’s profile is updated so that the user can access his home directory share.

1. Open **Home Folder Management** in the Admin View.
2. Perform one of the following actions:
    - Click a home folder policy. Under **Users** on the **Properties** tab that appears in the right pane, right-click a user and click **Remove**.
    - Right-click a home folder policy and click **Remove Users**. Select the users you want to remove. Click **Next** and click **Finish**.

Move a user

Move a user's share to another location and make this move transparent to the user. Before you move a user's share, review "Data migration considerations" and "Preparing for data migration."

1. Select a home folder policy to display the **Properties** tab in the right pane.
2. Under **Users**, right-click the user you want to move and click **Data migration**.
3. Use the Data Migration wizard to move the user's data and retarget the link.

Locate a user in the namespace

Find where a user is located in the namespace.

1. Click the home folder policy that contains the user. A **Properties** tab appears in the right pane.
2. Find the user in the list and click the link under **DFS Link**.

Locate a DFS root in the namespace

Find where the DFS root of a home folder policy is located in the namespace.

1. Click the home folder policy that contains the user. A **Properties** tab appears in the right pane.
2. Click the link next to **Base DFS Path**.

Note: You can also locate a DFS root in the namespace by clicking Logical View. A Properties tab appears in the right pane that shows a list of all the roots in the namespace. Double-click the root you want to locate.

Delete a home folder policy

When you delete a home folder policy, all the user links are deleted from the namespace. VFM changes the users' account information so that their home folders point directly to the targets that used to be pointed by links.

1. Right-click the policy you want to delete and click **Delete**.
2. Click **Yes**.

Chapter 8 Back Up the Namespace

Create a namespace backup policy to back up the logical structure of DFS roots so that you can restore a root to a known state in the event that it is deleted or changes to the root need to be rolled back.

Backup

- Only the links of the DFS roots selected are backed up. Data referenced by links in the namespace and empty logical folders are not backed up.
- Permissions on logical folders are not backed up.
- The backup operation records the configuration data that was gathered about the namespace.
- If you have cascaded roots, you must back up each root separately.

Restore

- Recreates the links contained in a backed-up DFS root onto a DFS root.
- Restores selected items in a backup file.
- You might encounter errors if you attempt to restore a backup configuration to a different type of root than it was originally created on. This can occur if you attempt to restore the backup set for a Windows 2000 DFS root to an NT4 DFS root. You can skip the problem steps in the confirmation dialog boxes and restore those aspects of the backup that apply to NT4 DFS roots.

Note: When you export your VFM configuration, all your DFS root backups are included with the export data. This enables you to restore a root that might no longer be available after you import the VFM configuration.

Namespace backup policy checklist

To create your first policy, follow the basic steps listed below:

1. Create a namespace backup policy.
2. Schedule backups.

Create a namespace backup policy

Back up automatically the logical structure of your namespace so that you can quickly restore it if it becomes necessary.

1. Perform one of the following actions:
   - On the **Tools** menu, click **New Policy**, point to **Namespace Policy**, and click **Backup Policy**.
   - Right-click the Namespace Policy folder in the Admin View, point to **New**, then click **Backup Policy**.
   - Right-click Admin View, click **New**, point to **Namespace Policy**, and click **Backup Policy**.
   - Select the Namespace Policies folder to show a Properties tab in the right pane. Right-click the Backup Policies folder and click **New Backup Policy**.
2. Type a word or phrase that best describes this policy in the **Name** field.
3. Click **Add** and type the path of a root, or click ... **Browse** to locate a root in your namespace.
4. Repeat Step 3 to add more roots.
5. Click **OK**.

Notes:

- When the DFS root you are backing up and the VFM server are hosted on machines running Windows Server 2003 release 2 or later, the attributes of the root are backed up.

  DFS root attributes restored:
  - Link target failover priority
  - Link target costing
  - DFS root permission settings
  - Ability to enable or disable root scalability mode
  - Ability to configure site costing
- You can also manually back up a root. On the **Tools** menu, click **Manual backup**.

Schedule backups

Schedule how frequently you want to back up the roots participating in a policy.

1. Perform one of the following actions:
   - Right-click a namespace backup policy and click **Properties**.
   - Select a namespace backup policy to show a Properties tab in the right pane and click Edit.
2. Click **Schedule**.
3. Select **Use Schedule**.
4. Type the time and date you want to begin making backups

5. Select how frequently you want to make backups, and type how many backups to keep.
6. Click **OK**.

Note: If you enable multiple schedules (for example, hourly, nightly, and weekly backups) and backups initiate at the same time, only the longer period backup is initiated. For example, if you schedule hourly and nightly backups that initiate at the same time, only the nightly backup is initiated. Multiple simultaneous backups are not initiated to avoid duplicate network traffic and the maintenance on duplicate backups.

Browse contents of a backup

Quickly view the contents of a backup.

1. On the **Tools** menu, click **Browse Backups**. A list of backup policies appears.
2. Double-click the policy that contains the backup file. Daily, Hourly, and Weekly folders appear.
3. Double-click the folder that contains the backup file. A list of backup files appears.
4. Double-click the backup file you want to view. A tree that looks like the Logical View appears on the left pane.
5. Click an item in the tree to view its properties on the right-pane.
6. When you finish browsing, click **OK**.

Remove a root from a namespace backup policy

Remove a DFS root from selected namespace backup policies.

1. Right-click the root and click **Remove from Namespace Backup Policy**.
2. Select the policies from which you want to remove the root.
3. Click **OK**.

Note: If the root is the only root participating in a policy, the root is not removed from the policy. If you no longer want the policy to back up the root, delete the policy.

Delete a namespace backup policy

When you delete a namespace backup policy, all the backup files associated with the policy are deleted.

1. Perform one of the following actions:
   - Right-click a namespace backup policy and click **Delete**.
   - Select the Backup Polices folder to show a Properties tab in the right pane. Right-click the policy you want to delete, and click **Delete**.
   - Select a namespace backup policy to show a Properties tab in the right pane. Right-click anywhere on the page, and click **Delete**.
2. Click **Yes**.

Note: If you want to delete a root and retain the namespace backups for the root, perform the actions listed below. To help clarify the instructions, *TempRoot* is the name of a root you add

temporarily to the policy. *DeleteRoot* is the root you want to delete, and *NewRoot* is the root that you use to restore the contents of *DeleteRoot*.

1. Add *TempRoot* to the namespace backup policy that contains the root you want to delete.
2. Remove *DeleteRoot* from the policy, and delete the root.
3. Add *NewRoot* to the policy.
4. Restore the contents of *DeleteRoot* to *NewRoot*.
5. Remove *TempRoot* from the namespace backup policy.

Restore a DFS root

Restore the logical structure of a DFS root that you previously backed up. The DFS links of the root are restored.

1. Perform one of the following actions:
   - On the **Tools** menu, click **Restore from backup**.
   - Right-click Logical View and click **Restore**.
   - Right-click a DFS root and click **Restore**.
2. Click **Next**. A list of all the roots in your namespace appears.
3. Select the root to which you will restore the links from a backup file.
4. Click **Next**.
5. Type the path of a backup file, or click **Browse** to find the location of the file.
6. Click **Next**. If the backup file contains the logical structure of more than one root, a list of the roots appears. Select the root you want to restore.
7. Click **Next**. The target DFS root is compared with the backup root and shows the links that are different and the action that will be taken for each link.
8. Clear the links that you do not want to restore.
9. (Optional) Click **View Backup** for a detailed view of each item in the backup root.
10. (Optional) Select **Remove existing links** to remove links in the target root that are not in the backup root.
11. (Optional) Select **Restore DFS Root Properties** to restore the attributes of roots. The roots and the VFM server must be hosted on machines running Windows Server 2003 release 2 or later.

    DFS root attributes restored:
    - Link target failover priority
    - Link target costing
    - DFS root permission settings
    - Ability to enable or disable root scalability mode
    - Ability to configure site costing
12. Click **Next**. A window displays the name of the backup file, the name of the DFS root you selected from your backup file, and the name of the DFS root you selected as the target of the restore process.
13. Click **Finish**.

Appendix

No.	Title	File name	Contents
1.	*Advanced Configuration and Techniques*	VFMAdvConfig.pdf	• Explains how to use VFM to configure security permissions • Explains how to manage replication and monitoring agents • Explains how to run batch files in policies and reports • Explains how to make the VFM server highly available
2.	*Create and Manage Namespaces*	VFMNamespace.pdf	Explains how to create a DFS namespace (roots, links, and link targets), how to quickly populate the namespace, make the namespace highly available, create multiprotocol namespaces, virtualize user home directories, and back up the namespace.
3.	*Getting Started*	VFMGettingStarted.pdf	A tutorial to get you started using VFM. It explains how to install VFM and steps you through the process of creating a logical namespace, making the namespace highly available, making data highly available, transferring CIFS and NFS data, creating multiprotocol namespaces, virtualizing user home directories, and backing up data and the namespace.
4.	*Make Data Highly Available*	VFMMakeDataAvailable.pdf	Explains how to make data highly available by creating client, filer, and server disaster recovery policies
5.	*Manage Physical Resources*	VFMPhysicalResources.pdf	Explains how to use VFM to Work with NetApp filers, set replication properties, and work with Windows and UNIX machines
6.	*Manage Snapshots on Filers*	VFMSnapshots.pdf	Explains how to use VFM to manage snapshots on NetApp filers using snapshot access and snapshot scheduling policies

No.	Title	File name	Contents
7.	*Optimize Storage*	VFMOptimizeStorage.pdf	• Explains how to create and manage archival migration policies to optimize storage. • Explains how to load balance Windows servers by creating storage load balancing policies
8.	*Reports*	VFMReports.pdf	Explains how to create and publish reports
9.	*Transfer Data*	VFMTransferData.pdf	• Explains how to transfer CIFS and NFS data by creating migration and replication policies • Explains how to transfer data between NetApp filers by creating SnapMirror policies
10.	*Troubleshooting*	VFMTroubleshooting.pdf	• Includes diagnostic information, such as troubleshooting, event IDs, migration, replication, and status indicators • Provides examples of file exclusions and inclusions

Glossary

A

ACE: Access Control Entry, an entry in an Access Control List.

ACL: Access Control List, a list associated with a file that contains information about which users or groups have permission to access or modify the file.

C

CIFS: Common Internet File System. A file-sharing protocol based on the Microsoft Server Message Block (SMB). It enables you to share file systems over the Internet and Intranet. The CIFS protocol is used primarily for file sharing by Windows platforms.

Client: The user interface component of the application.

Consolidation DFS root: A special stand-alone DFS root that has its configuration information stored locally on a member server. The root must be hosted on Windows Server 2003.

D

Dependencies: The servers, drives, and shared folders that together contain the data published through the DFS namespace

DFS: Microsoft Distributed File System consists of software residing on network servers and clients that transparently links shared folders on different file servers into a single namespace for improved load balancing and data availability. NOTE: This should not be confused with Transarc's DFS product, which is a separate distributed file system product that is not interoperable with the Microsoft product.

DFS link: Located under the namespace root. Forms a connection to one or more shared folders, links or to another root.

DFS namespace: The logical view of shared file resources seen by users.

DFS path: A UNC path starting at a DFS root.

DFS root: The share at the top of the namespace topology. The starting point for the links and shared folders that make up the namespace.

DFS topology: Overall logical hierarchy of a namespace, including elements such as roots, links, shared folders, and replica sets.

DFS tree: The consolidated DFS view provided by the application, which includes the Admin View, Logical View, Physical View, and Reports.

Domain-based DFS root: A DFS root that has its configuration information stored in Active Directory. The root can have multiple root targets, which offers fault tolerance and load sharing at the root level.

E

Export: SEE NFS export

F

Fault-tolerant DFS: SEE Domain-based DFS root

FQDN: Fully-qualified Domain Name. A host, domain name, and a top-level domain. For example, www.brocade.com is a fully-qualified domain name where www is the host, .brocade is the second-level domain, and .com is the top-level domain.

FRS: Microsoft File Replication Service.

G

GID: Group Identification Number. A unique number assigned to identify a group of users in UNIX environments.

K

Key-pair: Consists of a public key and a corresponding private key. It is safe to distribute a public key, but a private key must be kept secret.

L

Link target: A DFS link can have as targets: 1 to N shared folders, OR 1 to N stand-alone DFS paths, OR only 1 domain-based DFS path.

M

Migration candidates: Items that match migration criteria in an archival migration policy. You can select which items you want to migrate. Items not selected for migration are automatically added to the exclusion list of the archival migration policy.

Migration task: Identifies the source and destination.

Monitoring agent: The component that can be installed to evaluate storage policies from a different machine than the one where the application server is installed.

N

NFS: Network File System developed by Sun Microsystems. A file-sharing protocol that enables you to share file systems over the Internet and Intranet. NFS is used with both UNIX and non-UNIX computers.

NFS export: A directory that is published for access by NFS clients. The export specifies a directory to be exported and which machines have access to the directory. NFS exports are similar to CIFS shares in that they provide access to directories.

P

Pool: A group of storage locations.

Primary server: An active application server or monitoring agent.

Primary target: In a disaster recovery policy, this is the active target to which users are referred by the DFS root.

Q

qtree: A special directory of the root of a volume that behaves like a virtual subvolume with special attributes.

Quiesce: Wait for all existing transfers to both volumes and qtrees to complete and then block any further updates.

R

RAID: Redundant Array of Independent Disks enables file access even when a disk in a RAID group is damaged.

Rebase: To change the destination path proposed by the application to the actual path to where the data is to be migrated.

References: The DFS link targeting the selected physical item. For example, when you click a server under the Physical View tree, properties and associated DFS links appear.

Replica: A DFS root or DFS shared folder that provides an alternate path for a DFS link. NOTE: In Windows NT 4 terminology, this is referred to as an alternate volume.

Replica set: Two or more DFS roots or DFS shared folders that provide alternate paths for a DFS link.

Replication agent: The component deployed by the application server or monitoring agent during the configuration of storage policies that transfer CIFS and NFS data, or when you run a file differencing report.

Report schedule group: Enables you to set a schedule to automatically gather information. A report schedule group can be configured to start during off hours to offload network and computing resources during business hours. You can produce multiple reports from the data gathered without generating additional network traffic.

Report source group: Specifies the location where you want to gather information. It is assigned to a report schedule group. A report source group also enables you to specify batch files to run before and/or after the information is gathered.

Report type: Determines what information is gathered. Report types are assigned to report source groups.

S

Secondary target: SEE Standby target.

Server: The component that responds to requests from the client component, monitors the DFS namespace, and processes storage policies.

Shared folder: File or folder in the DFS namespace that can be accessed by users who have proper permissions. NOTE: In Windows NT 4, this is referred to as a DFS volume, leaf, or branch.

SID: Security identifier that uniquely identifies a Windows user or group.

Stand-alone DFS root: A DFS root that has its configuration information stored locally on the host server. The root has a single root target. When the root target is unavailable, the data referenced by links under the root is inaccessible.

Standby target: A target in a disaster recovery policy that is offline. During a failover, a standby target can become the active target.

Storage location: A combination of a server UNC path and the local path pointing to a directory in the file system. For example, \\rama:c:\ is a storage location representing the C drive on machine "rama" and \\secure.npb.com:/vol/vol0/myqtree is a storage location representing the qtree "myqtree" on volume vol0 on secure.npb.com.

T

Target: LINK TARGET: A shared folder, a DFS link, or a DFS root that is referenced by a DFS link. ROOT TARGET: A shared folder that is referenced by a DFS root. SEE ALSO Link target.

Trustee: The user account, group, or logon session to which an Access Control Entry (ACE) applies.

U

UID: User Identification Number. A unique number assigned to identify a user in UNIX environments.

UNIX file permissions: Control access to files and directories. Permissions can be applied to the owner of a file, a group, or everyone on the UNIX network.

W

Widelink namespace: A logical namespace hosted on a NetApp filer CIFS share that provides the benefits of a namespace without requiring additional Windows servers.

Index

.NET 7, 8
/etc/exports file 60
Access restrictions 61
Active Directory 4, 8
Add a DFS link 23
Add a folder 23, 29
Add a link 4
Add folder 26
Add link targets 33
Add links to users' home directories 67, 68
Add multiple links 4, 26, 41
Add new home directories 68
Add new users to a home folder policy 68
Align namespace 41
Anonymous 61
Apply rules to a home folder policy 69
Arrange links in the namespace 45
Attributes 19
Automatically configure UNIX clients to access
  a namespace 61
Automatically host the namespace on a filer 60
Automatically synchronize roots 53
Automatically update namespace 41
Automount files 61
Back up a DFS root 19
Back up the namespace 19, 74
Backup file 75
Batch files 63
Browse contents of a replica 22
Change a multiprotocol namespace policy 64
Change master root of a namespace availability
  policy 57
Change name of a folder 30
Change name of a link 30
Change properties 18, 31
Change schedule of a namespace creation policy
 43
Change status monitoring 38
Check status of a DFS link 31
Check status of a DFS link target 36
Check status of a DFS root 20
CIFS protocol 64
CIFS share 53
Clear status 20, 31, 36
Clone a link 33
Compare contents of targets 22
Consolidation root
  create a root 9
Consolidation root 9
Consolidation root 14
Contents of a replica 22
Contents of targets 22
Create a home folder policy 67
Create a stand-alone root 7
Data migration 70
Data move 70
Delete
  a DFS link 32
  a DFS root 20
  a folder 22, 26
  a home folder policy 71
  a link 26
  a multiprotocol namespace policy 65
  a namespace backup policy 75
  a namespace creation policy 46
  a replica 22
  a target 37
  a user from a home folder policy 70
Dependencies 19, 30
Detect FRS replication 36
DFS link
  add a link 23
  add multiple links 26
  add new shares 28
  add users' home directories 67
  assign DFS roots 26
  assign folders 26
  assign multiple shared folders 26
  assign subdirectories 28
  check FRS replication status 36
  check status 31
  clear status 31
  compare contents of targets 37
  delete a link 32
  modify properties 31
  monitor status 30
  refresh 31
  rename a link 30
  size of targeted shares 36
  view attributes 30
DFS link 23
DFS link status 36
DFS root
  assign to a link 23
  back up a root 19
  change storage status of all targets 35
  check FRS replication status 36
  check status 20, 36
  clear status 20
  compare contents of replicas 37
  create a consolidation root 9
  create a domain-based root 8
  create a stand-alone root 7
  delete a root 20
  delete a root replica 22
  display an existing root 18

domain-based 21
modify properties 18
monitor status.....18
remove from a namespace backup policy 75
remove from display 20
remove from policy.....56
restore a root.....76
set permissions 18
size of targeted shares 36
view attributes.....19
view replicas of a root.....21
DFS root status 36
Directories
as link targets 28
search for.....45
Directories 45
Disk space 36
Display an existing root.....18
Display targets of a link.....33
Domain-based root
create a root.....8
view root replicas.....21
Domain-based root 8
Domain-based root 21
Domain-based root 36
Domains 43
Drag an item from Windows Explorer 23, 26
Drag UNC paths 4
Edit properties 18, 31
Exclusion list.....44
Export access restrictions 61
Export files 60
exportfs -a command 60
Fault tolerance 21, 33, 53
File differences.....22
File Replication Service 36
Find a DFS root in the namespace.....70
Find a user in the namespace.....70
Folder
add a folder 23, 29
add multiple folders 26
change storage status of all targets.....35
rename a folder.....30
size of targeted shares 36
Folder 23
FRS.....36
FRS replication.....36
Home directories 67, 68, 69, 70
Home folder management 4
Home folder policy
add a link to a user home folder.....68
add new users.....68
apply rules.....69
create a policy 67
delete a policy 71
locate a DFS root in the namespace 70
locate a user in the namespace 70
move a user 70
refresh a policy..... 69
remove a user 70
resolve discrepancies..... 69
view properties 69
Home folder policy..... 68
Ignore list..... 44
Link target
check status 36
clear status..... 36
compare contents with other targets..... 22
monitor status..... 35
Link target 36
Load balancing 21, 33, 53
Locate a DFS root in the namespace 70
Locate a user in the namespace 70
Logical View tree
add a folder..... 29
Logical View tree 29
Make changes to multiprotocol namespace
policy..... 64
Manually scan for shares 45
Migrate data..... 70
Migrate user data 70
Modify properties 18, 31
Modify status monitoring 38
Monitor DFS link status 30
Monitor DFS root status 18
Monitor link targets 35
Monitor status.....18, 30, 35, 38
Move user data 70
Multiprotocol namespace policy
add a sync point..... 62
configure UNIX clients to access a namespace
..... 61
delete a policy 65
delete a sync point..... 64
export access restrictions..... 61
host the namespace on a filer 60
run batch files..... 63
synchronize namespaces immediately..... 64
update the policy 64
Multiprotocol namespace policy..... 62
Namespace
add a folder..... 29
back up the logical structure.....19, 74
make highly available..... 51
Namespace availability policy
a wide link namespace..... 56
add CIFS shares..... 56
add roots..... 56
change master root 57
configuration options..... 51
create a policy 53
create a wide link namespace 53

delete a policy 57
remove a root 56
root synchronization options 54
schedule synchronization 55
start synchronization immediately 55
Namespace availability policy.....56
Namespace backup policy
create a policy 74
delete a policy 75
remove a root from a policy 75
schedule backups.....74
view contents of backup file 75
Namespace creation policy
arrange links in the namespace.....45
change search type 44
create an exclusion list 44
delete a policy 46
manually scan for shares 45
review search results 46
search options.....44
update list of domains to search 43
update list of servers to search 43
update schedule 43
update search criteria.....45
Namespace creation policy.....44
NFS protocol 61, 64
NIS 61
Offline 35
Online.....35
Permission based policies
Add items to an exclusion list 50
change how links are arranged.....50
change search criteria.....49
create a policy 47
delete a policy 50
manually scan for resources 50
update the schedule 50
Permission based policies.....47
Permissions.....18
Populate a namespace.....47
Properties
of a home folder policy 69
Properties.....18, 19, 30, 31
Properties.....69
qtree
search for.....44
qtree.....44
qtree.....45
Refresh
data from network 20, 31, 36
information of a home folder policy 69
Refresh 20
Refresh 31
Rename a folder.....30
Rename a link.....30
Replica
compare contents of targets..... 22
create a DFS root replica..... 21
delete a replica..... 22
display replicas of a link..... 33
view contents..... 22
view replicas of a link 33
Restore a DFS root 76
Restrictions 61
Root access 61
Root replica 8, 21
Root status 36
Root synchronization.....54, 55
Run batch files..... 63
Scan for shares.....45, 46
Schedule 43
Schedule root synchronization..... 55
Script settings 63
Search criteria..... 45
Search for
directories..... 45
filer qtrees..... 44
filer volumes.....44, 45
qtrees 45
shares.....43, 44, 45, 46
subdirectories 45
Search for..... 44
Search network 43
Security.....18, 61
Security groups.....47, 49
Servers 43
Set permissions..... 18
Share finder 4, 43
Shared folder
assign links to subdirectories..... 28
assign to a link.....23, 26, 28
create shares 28
put online..... 35
refresh..... 36
take offline 35
Shared folder 23
Shares
assign links to subdirectories..... 28
disk space 36
size 36
Shares 28
Shares 36
Shares 41
Shares 44
Shares 45
Stand-alone root
create a root..... 7
root synchronization options 54
Stand-alone root..... 7
Stand-alone root..... 53
Stand-alone root..... 55
Stand-alone root..... 55

Stand-alone root 56
Stand-alone root 56
Start synchronization immediately 55, 64
Status 20, 31, 36
Status monitoring 18, 30, 35, 38
Storage offline 35
Storage online.....35
Subdirectory
  as link target.....28
Subdirectory 28
Sub-folder
  assign to a link.....23
Sub-folder.....23
Synchronization.....63
Synchronization of data.....64
Synchronize namespaces immediately 64
Synchronize roots 53, 55
Target
  delete a target 37
  display target of a link.....33
Target 33
Target 36
Target 37
Target of a link 23, 33
Targets
  compare contents.....37
Targets.....37
Targets replicated with FRS 36
Templates 45
Toggle storage offline.....35
Toggle storage online 35
UNC paths 4
UNIX export files.....60
UNIX namespace.....59, 60, 61, 64
Update
  a link..... 31
  a multiprotocol namespace policy 64
  a share 36
Update 31
Update 36
Update 64
Update DFS configuration..... 20
Update information of a home folder policy.... 69
Update properties.....18, 31
Update schedule of a namespace creation policy
  43
Update status monitoring..... 38
User data migration 70
Users' home directories.....67, 68, 69, 70
Validate a DFS link 31
Validate a DFS link target 36
Validate a DFS root 20
View attributes.....19, 30
View contents of a file..... 75
View contents of a replica 22
View replicas of a link..... 33
View target of a link 33
Volumes..... 45
Wide link namespace
  remove from policy 56
Wide link namespace..... 53
Wide link namespace..... 56
Windows 2000.....4, 7, 8
Windows Explorer..... 23
Windows NT4 .....4, 7, 8
Windows Server 2003 .....7, 8, 9