VFM (Virtual File Manager) v6.0

Manage Snapshots on Filers

June 28, 2007

Publication Number: 215-03207_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 guide describes how you can use Network Appliance® VFM® technology to manage snapshots to back up and restore data on NetApp filers and the namespace referencing the data.

The guide is divided into the following sections:

Chapter 1 Introduction defines snapshot access and snapshot scheduling policies.

Chapter 2 Snapshot Access Policies explains how to create and manage snapshot access policies.

Chapter 3 Snapshot Scheduling Policies explains how to create and manage snapshot scheduling policies.

Appendix provides a list and description of the VFM documents.

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)

Notes:

You can also contact technical support by clicking Support on the Help menu.

To get your product build number and license information, click About Virtual File Manager 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 Virtual File Manager**.
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**.

Table of Contents

PREFACE ..... **I**

CHAPTER 1 INTRODUCTION **1**

CHAPTER 2 SNAPSHOT ACCESS POLICIES **3**

CREATE A SNAPSHOT ACCESS POLICY 3
TAKE A SNAPSHOT IMMEDIATELY 4
To take a snapshot and capture an associated namespace *4*
To take a snapshot of one or selected volumes participating in the policy *4*
UPDATE CAPTURED NAMESPACES 5
SPECIFY WHICH VOLUMES PARTICIPATE IN A POLICY 5
BROWSE SNAPSHOT DATA 5
RESTORE DATA 6
RESTORE NAMESPACE AND DATA 6
RE-CREATE PART OF YOUR NAMESPACE 7
ACCESS SNAPSHOT DATA THROUGH THE NAMESPACE 7
ACCESS SNAPSHOT DATA DIRECTLY 8
CHANGE THE SNAPSHOT SCHEDULE FOR ALL VOLUMES 8
CHANGE THE SNAPSHOT SCHEDULE FOR SELECTED VOLUMES 9
CAPTURE THE NAMESPACE OF A SNAPSHOT 9
UPDATE THE PROPERTIES OF A SNAPSHOT ACCESS POLICY 10
DELETE A SNAPSHOT ACCESS POLICY 10

CHAPTER 3 SNAPSHOT SCHEDULING POLICIES **11**

Create a snapshot scheduling policy checklist *11*
CREATE A SNAPSHOT SCHEDULING POLICY 11
SCHEDULE SNAPSHOTS 12
To set the schedule for VFM-initiated snapshots *12*
To set the schedule for filer-initiated snapshots *13*
UPDATE THE PROPERTIES OF A SNAPSHOT SCHEDULING POLICY 13
SUSPEND THE SNAPSHOT SCHEDULE OF A POLICY 14
TAKE A SNAPSHOT IMMEDIATELY 14
DELETE A SNAPSHOT SCHEDULING POLICY 14

APPENDIX **17**

VFM GUIDES 17

GLOSSARY **19**

INDEX **23**

Chapter 1 Introduction

This guide provides instructions about how to create snapshot access and snapshot scheduling policies to manage snapshots on NetApp filers.

Topics are arranged in the following subsections:

Snapshot access policies

Snapshot scheduling policies

Chapter 2 Snapshot Access Policies

Snapshot access policies enable you to centrally manage snapshots on multiple NetApp filers. You can take snapshots of data and the logical structure of the namespace that references the data. You can take snapshots of volumes participating in your namespace and restore files and folders from snapshot backups.

To create a snapshot access policy, follow the steps listed below:

1. Create a snapshot access policy.
2. Browse the snapshot data.
3. Restore the data.

Create a snapshot access policy

Snapshot access policies enable you to back up and restore data on NetApp filers and the logical structure of the namespace that references the data. You select DFS roots, links, and folders in your namespace. A captured namespace is created that targets all scheduled snapshots on the volumes in the selected namespace.

1. Perform one of the following actions:

   On the **Tools** menu, click **New Policy**, point to **Snapshot Policies**, and click **Access Policy**.

   Right-click the **Snapshot Policies** folder in the Admin View, point to **New**, and click **Access Policy**.

   Right-click the **Access Policies** folder and click **New Access Policy**.

   Drag a link, root, or folder in the Logical View that references data on NetApp filers to the **Access Policies** folder.

   Drag a NetApp filer or volume in the Physical View to the Access Policies folder.

   Right-click Admin View, click **New**, point to **Snapshot Policy**, and click **Access Policy**.
2. In the **Name** field, type a word or phrase that best describes this policy. The name appears under the Access Policies folder and on the **Properties** tab of items that are members of the policy.
3. Perform one of the following actions:

   Click **Add** to type or select a DFS root, link, or folder that references data on filers.

   Click **Add All Roots From the Logical View** to include all the DFS roots displayed in your namespace.
4. Optionally select **Limit selection to the following volumes** and click **Add** to type the host and volume name (for example, `secure:/vol/vol0`), or click **Browse** to locate the volume on your network or the Physical View tree. This enables you to select a subset of the volumes referenced from the namespace.
5. In the **Use the Monitor on** list, select the machine that contains the agent that you want to use to process the policy. Normally, the current VFM server is used to process the

policy. If you installed monitoring agents on other machines, you can select one of the locations where monitoring agents are installed as the location from which this policy is processed.

6. Click OK. The policy searches for snapshots on the volumes referenced in the selected namespace, captures the namespace targeting each snapshot, and displays the captured namespace files under a Captured Namespaces folder under the policy.

Notes:

Filers participating in a snapshot access policy must have "Show Snapshot" enabled in their CIFS configuration.

For more information about snapshots, see the NetApp document *Data ONTAP® System Administration Data Protection Guide*.

Monitoring agents are installed using the VFM media and uninstalled through normal Windows mechanisms for removing programs.

Take a snapshot immediately

You can override a snapshot schedule and manually create a snapshot any time you want.

To take a snapshot and capture an associated namespace

1. Perform one of the following actions:

   Right-click a snapshot access policy and click **Snapshot referenced volumes now**.

   Select a snapshot access policy to show tabs in the right pane. Right-click anywhere on the **Properties** tab and click **Snapshot referenced volumes now**.

2. Type the name of the snapshot.
3. Optionally run batch files before and after the snapshot process.
4. Click OK. The captured namespace appears under the Captured Namespaces\Manual folder.

To take a snapshot of one or selected volumes participating in the policy

1. Perform one of the following actions:

   Right-click a volume under a filer folder and click **Take snapshot now**.

   Select the Volumes folder under a snapshot access policy to show a **Properties** tab in the right pane. Select the volumes of which you want to take snapshots and click **Take snapshot now**.

2. Type the name of the snapshot.
3. Optionally run batch files before and after the snapshot process.
5. Click OK. To view the snapshot, double-click the volume and click the **Snapshots** tab.

   Select a snapshot on the list and click **Refresh**.

Note: When you take a snapshot of a volume referenced in a snapshot access policy, the namespace is not capture. To capture the namespace of the snapshot, see "Capture the namespace of a snapshot."

Update captured namespaces

VFM periodically checks for new filer-initiated and VFM-initiated snapshots on volumes participating in a snapshot access policy and updates the captured namespaces. You can update captured namespaces manually if you do not want to wait for the scheduled updates.

Perform one of the following actions:

Right-click a snapshot access policy and click **Update Volumes and Captured Namespaces**.

Select the **Snapshot Policies\Access Policies** folder to show a **Properties** tab in the right pane. Right-click a snapshot access policy and click **Update Volumes and Captured Namespaces**.

Specify which volumes participate in a policy

Specify which volumes referenced in your namespace participate in a snapshot access policy. You can select a subset of the volumes referenced in your namespace.

1. Perform one of the following actions:

   Right-click a snapshot access policy and click **Properties**.

   Select a snapshot access policy to show a **Properties** tab in the right pane. Click Edit.
2. Select **Limit selection to the following volumes**.
3. Click **Add** and type the path of a volume (for example, `safe:/vol/vol3`) on a NetApp filer containing data targeted by a link in your namespace, or click ... **Browse** to find a volume.
4. Repeat Step 3 to add more volumes.
5. Click **OK**.

Browse snapshot data

Browse the contents of a captured namespace and the snapshot data it references.

1. Open a folder under the **Captured Namespaces** folder of a snapshot access policy to show a list of captured namespace files.
2. Select one of the files to show the **Explorer** tab in the right pane.
3. The left pane on the **Explorer** tab shows the captured namespace. Click a link to show the data referenced by the link on the right pane.

Notes:

If you have the appropriate program, you can double-click a file to view its contents.

You can copy snapshot data to another location so users can access the data directly. See "Access snapshot data directly" for instructions.

If you have problems viewing files in the Explorer tab, see "Troubleshooting" for help.

Restore data

Restore snapshot data to its original location. The snapshot overrides corresponding files in the original location. The content of a file is restored to the state that existed at the time the snapshot was taken. If a corresponding file does not exist in the original location, the file in the snapshot is copied to the original location.

1. Perform one of the following actions:

   Right-click a captured namespace under the **Captured Namespace** folder and click **Restore**.

   Select a snapshot access policy to show tabs on the right pane. Click the **Explorer** tab. Right-click an item on the left pane or right pane and click **Restore**.
2. Select **Restore the Snapshot Files**.
3. Click **OK**.

Notes:

You can restore the data on one or more files by selecting items in the Explorer tab of a snapshot access policy.

You can browse a file before you restore it. For instructions, see "Browse snapshot data."

If you have problems restoring files, see "Troubleshooting" for help.

You can copy snapshot data to another location so users can access the data directly. For instructions, see "Access snapshot data directly."

Restore namespace and data

Restore a captured namespace to a root, an existing folder, or new folder in your namespace and restore snapshot data to its original location. The restored namespace and content of files referenced by the namespace are restored to the state that existed at the time the snapshot was taken. If a corresponding file does not exist in the original location, the file in the snapshot is copied to the original location.

1. Perform one of the following actions:

   Right-click a captured namespace under the **Captured Namespace** folder and click **Restore**.

   Select a snapshot access policy to show tabs on the right pane. Click the **Explorer** tab. Right-click an item on the left pane or right pane and click **Restore**.
2. Select **Restore the Captured Namespace and the Snapshot Files**.

3. Type the name of a root or folder in your namespace where you want to create the namespace to reference the current active file system, or click **Browse** to find the root or folder.
4. Click **OK**. The namespace is restored to the location you specified and the data is restored to the active file system.

Re-create part of your namespace

Recreate a portion of your namespace. You can restore the captured namespace to a root, an existing folder, or new folder in your namespace. The restored namespace references the current data.

1. Perform one of the following actions:

   Right-click a captured namespace under the **Captured Namespace** folder and click **Restore**.

   Select a snapshot access policy to show tabs on the right pane. Click the **Explorer** tab. Right-click an item on the left pane or right-click a folder or link in the right pane and click **Restore**.
2. Select **Restore the Captured Namespace**.
3. Type the name of a root or folder in your namespace where you want to create the namespace to reference the current data, or click **Browse** to find the root or folder.
4. Select **New namespace will target active file system**.
5. Click **OK**.

Access snapshot data through the namespace

Make snapshot data accessible to users through the namespace. You can copy the captured namespace to a root, an existing folder, or a new folder in your namespace. The links in the restored namespace reference the snapshot data.

1. Perform one of the following actions:

   Right-click a captured namespace under the **Captured Namespace** folder and click **Restore**.

   Select a snapshot access policy to show tabs on the right pane. Click the **Explorer** tab. Right-click an item on the left pane or right-click a folder or link in the right pane and click **Restore**.
2. Select **Restore the Captured Namespace**.
3. Type the name of a root or folder in your namespace where you want to create the namespace to reference the data in the snapshot, or click **Browse** to find the root or folder.
4. Make sure **New namespace will target snapshot data** is selected.
5. Click **OK**.

Notes:

For instructions about how to browse the contents of a snapshot file, see "Browse snapshot data."

For instructions about how to copy snapshot data to another location so users can access the data directly, see "Access snapshot data directly."

Access snapshot data directly

You can copy snapshot data to another location so that users can access the data directly.

1. Select a snapshot access policy to show tabs in the right pane.
2. Click the **Explorer** tab.
3. Click a link in the right or left pane to show the files referenced by the link.
4. Drag a file to Windows Explorer.

Note: A snapshot access policy enables you to make snapshot data available to users through the namespace. For instructions, see "Access snapshot data through the namespace."

Change the snapshot schedule for all volumes

You should ensure that snapshot schedules for the volumes participating in your snapshot access policy are aligned so that snapshots of all the volumes occur as close to the same times as possible. You can quickly update the snapshot schedule for the volumes referenced in a snapshot access policy. A wizard steps you through the process of creating a new snapshot scheduling policy or adding the volumes to an existing policy.

1. Right-click the snapshot access policy and click **Set Snapshot Schedule for Referenced Volumes**.
2. Click **Next**.
3. Select **Add this volume to a Snapshot Scheduling policy**. Adding the volumes to a snapshot scheduling policy enables you to manage the schedule of the snapshots on all volumes participating in the policy.
4. Click **Next**.

5. Perform one of the following actions:

   Click **New Policy**.

   a. Type a word or phrase that best describes the policy in the **Name** field.
   b. Select whether you want VFM or the filer to perform the snapshots.

      Click the **Virtual File Manager Settings** tab and select **Use Virtual File Manager-initiated snapshot**. Type how often you want VFM to take snapshots.

      Click the **Filer Settings** tab and select **Manage filer-initiated snapshot schedule**. Type how many snapshots you want to retain and how often you want the filer to take snapshots.
   c. Click **OK**.
   d. Select the new policy and click **Next**.

   Select an existing policy and click **Next**.
6. Click **Finish**. A new policy appears under the **Snapshot Policies\Scheduling Policies** folder.

Change the snapshot schedule for selected volumes

Change the snapshot schedule for some of the volumes participating in a snapshot access policy.

1. Select the policy to show a **Properties** tab in the right pane.
2. Under **Volumes**, select the volumes for which you want to change the snapshot schedule.
3. Right-click the selected volumes and click **Set snapshot schedule**.
4. Continue with Step 2 of "Change the snapshot schedule for all volumes."

Capture the namespace of a snapshot

Capture the namespace of a manual snapshot of a volume. The volume must be referenced by the namespace and participate in a snapshot access policy.

1. Right-click the policy and click Properties.
2. Click Capture Namespaces.
3. Click Add and type the name of a manual snapshot.
4. Click OK. The captured namespace appears under the Captured Namespaces\Manual folder.

Update the properties of a snapshot access policy

Add or remove volumes or namespace items from the policy or change the monitoring agent for the policy.

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. Click **Edit**.
2. Update the appropriate information.
3. Click **OK**.

Delete a snapshot access policy

When a snapshot access policy is deleted, all the captured namespace files are also deleted. Snapshots of the data are not deleted.

1. Perform one of the following actions:

   Right-click the policy and click **Delete**.

   Select the **Snapshot Policies** folder to display a **Properties** tab in the right pane. Under the **Snapshot** policies folder, right-click the policy and click **Delete**.
2. Click **Yes**.

Chapter 3 Snapshot Scheduling Policies

Snapshot scheduling policies enable you to schedule snapshots on NetApp filer volumes. You can centrally manage filer-initiated and VFM-initiated snapshots on multiple filers with a single operation. This is a convenient way to change the snapshot schedule and reserve setting on multiple filers without having to repeat the changes on each individual filer.

Create a snapshot scheduling policy checklist

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

1. Create a snapshot scheduling policy.
2. Schedule snapshots.

Create a snapshot scheduling policy

Create a snapshot scheduling policy to schedule snapshots on multiple filers.

1. Perform one of the following actions:

   On the **Tools** menu, click **New Policy**, point to **Snapshot Policy**, and click **Scheduling Policy**.

   Right-click the Snapshot Policies folder in the Admin View, point to **New**, and click **Scheduling Policy**.

   Right-click Admin View, click **New**, point to **Snapshot Policy**, and click **Scheduling Policy**.
2. In the **Name** field, type a word or phrase that best describes this policy. The name appears under the **Snapshot Policies\Scheduling Policies** folder and on the **Properties** tab of items that are members of the policy.
3. Click **Add** and type the host and volume name (for example, `secure:/vol/vol0`), or click ... Browse to locate the volume on your network or the Physical View tree.
4. Repeat Step 3 to add more volumes to the policy.

5. You can select another location where the policy is monitored. The default is to monitor from the VFM server. From the **Use the Monitor on** list, optionally select the machine hosting another monitoring agent.
6. Click OK.

Notes:

Monitoring agents are installed using the VFM media and uninstalled through normal Windows mechanisms for removing programs.

If you uninstall a monitoring agent, ensure that policies that formerly used the uninstalled agent are reassigned to a currently available agent. Right-click a snapshot access policy and click **Properties**. On the **General** tab, select a new monitoring agent from the **Use the Monitor on** list.

Schedule snapshots

Set the schedule for filer-initiated as well as VFM-initiated snapshots. A snapshot scheduling policy can have both types of snapshots.

Perform one of the following actions:

Right-click a snapshot scheduling policy and click **Properties**.

Select a snapshot scheduling policy to show a **Properties** tab in the right pane. Click Edit **Edit**.

To set the schedule for VFM-initiated snapshots

VFM-initiated snapshots enable you to run batch files before and after a snapshot.

1. Click **Virtual File Manager Settings**.
2. Select **Use Virtual File Manager-initiated snapshot**.
3. Type the number of snapshots you want to retain. By default, the latest four snapshots are retained.
4. Optionally, select **Run batch before snapshot** and type the UNC path of a script file that you want to run.
5. Optionally, select **Run batch after snapshot** and type the UNC path of a script file that you want to run.
6. Type the time and date when and how frequently to take snapshots.

Note:

See "Running batch files" for detailed information about running batch files in VFM.

VFM provides sample batch files that you can modify. The sample batch files are in the

`Examples\Scripts\Snapshot scheduling`

directory in the VFM server installation directory.

To set the schedule for filer-initiated snapshots

Filer-initiated snapshots enable you to configure snapshots and snapshot reserves on multiple volumes and maintain the filer schedule settings. If a filer-initiated snapshot schedule is changed outside the policy, VFM restores the schedule back to the settings in the policy the next time the policy runs.

1. Click the **Filer Settings** tab.
2. Select **Manage filer-initiated snapshot schedule**.
3. Type the number of weekly, nightly, and hourly snapshots you want to retain. By default, the two most recent weekly snapshots and the four most recent nightly and hourly snapshots are retained.
4. Select the hours at which you want to start taking snapshots.
5. Optionally, select **Apply the same Snapshot Reserve to all volumes** and type the amount of space to reserve for snapshots on all volumes in the policy.

Update the properties of a snapshot scheduling policy

Add, edit, or remove volumes from the policy and change the snapshot schedule.

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. Click Edit **Edit**.
2. Update the appropriate information.
3. Click **OK**. A status report appears.
4. Click **Done**.

Suspend the snapshot schedule of a policy

You can stop a snapshot schedule from running on the volumes that are members of a policy. The schedule is not deleted.

1. Right-click the snapshot scheduling policy and click **Properties**.
2. Perform one of the following actions:

   If the schedule is VFM-initiated, click **Virtual File Manager Settings** and clear **Use Virtual File Manager-initiated snapshot**.

   If the schedule is filer-initiated, click **Filer Settings** and clear **Enable scheduled snapshots**.
3. Click **OK**. A status report appears.
4. Click **Done**.

Notes:

Existing snapshots on the selected volumes are not deleted when you suspend the schedule.

Suspending a snapshot schedule does not prevent you from manually taking a snapshot. Right-click the policy and click **Take snapshot now**.

Take a snapshot immediately

Take a manual snapshot of one or more volumes in a snapshot scheduling policy.

1. Perform one of the following actions:

   Double-click a policy under the **Scheduling Policies** folder to show the volumes that are members of the policy. Right-click a volume and click **Take snapshot now**.

   Select a policy to show a **Properties** tab in the right pane. Select one or multiple volumes, right-click, and click **Take snapshot now**.
2. Type a name for the snapshot.
3. Optionally, select **Run batch before snapshot** and type the UNC path of a script file that you want to run.
4. Optionally, select **Run batch after snapshot** and type the UNC path of a script file that you want to run.
5. Click **OK**.
6. Click **Done**.

Delete a snapshot scheduling policy

When you delete a snapshot scheduling policy, the schedule for VFM-initiated snapshots is also deleted. The management of filer-initiated snapshots returns to the respective filers. Changes made to a filer-initiated snapshot after the deletion of the policy remain in effect. The parameters set by the policy are no longer enforced.

1. Perform one of the following actions:

   Right-click the policy and click **Delete**.

   Select the **Scheduling Policies** folder to show a **Properties** tab in the right pane. Right-click the policy and click **Delete**.

2. Click **Yes**.
3. Click **Done**.

Appendix

VFM Guides

The following table lists the VFM guides. The list is arranged in ascending order by document title.

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

No.	Title	File name	Contents
			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
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 blockany 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

A

Access snapshot data directly 8

B

Browse contents of a file 5

C

Captured namespaces
  create a captured namespace 9
  update 5
Captured namespaces 9
Change snapshot schedule 8, 9
Check for new snapshots 5
Create a snapshot manually 4

F

Filers
  configure snapshots 3
  schedule snapshots 11, 12

M

Manually check for new snapshots 5
Manually create a snapshot 4

N

Namespace
  access snapshot data 7
  recreate the namespace 7
Namespace 7
NetApp filers
  schedule snapshots 11, 12

R

Recreate namespace 7
Restore data 6
Restore data and namespace 6
Restore namespace 7

S

Schedule snapshots on multiple filers 12
Snapshot access policy
  access snapshot data 7, 8
  browse contents of a snapshot file 5, 8
  capture the namespace 9
  create a snapshot immediately 4
  delete a policy 10
  manually check for new snapshots 5
  recreate the namespace 7
  restore data 6
  restore data and namespace 6
  specify volumes 5
  update captured namespaces 5
  update properties 10
  update snapshot schedule 8, 9
Snapshot scheduling policy
  create a policy 11
  delete a policy 14
  schedule snapshots 12
  suspend the snapshot schedule 14
  take a snapshot immediately 14
  update properties 13
Snapshot scheduling policy 11
Snapshots
  browse contents of a snapshot file 5
  capture the namespace 9
  make data available to users 7, 8
  manually check for new snapshots 5
  restore data 6
Snapshots 8
Suspend snapshot schedule 14

T

Take a manual snapshot 14

U

Update properties of a snapshot access policy. 10
Update snapshot schedule 8, 9

V

View contents of a file 5
Volumes
  schedule snapshots 11
  specify volumes for snapshot access policy .. 5
  suspend the snapshot schedule 14
  take a snapshot immediately 14
  update snapshot schedule 8, 9

W

Windows Explorer 8