VFM (Virtual File Manager) v6.0

Manage Physical Resources

May 29, 2007

Publication Number: 215-03206_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 the machines and NetApp filers that participate in the namespace or in VFM policies.

The guide is divided into the following sections.

- **Chapter 1 Introduction** provides an overview of the VFM Physical View tree.
- **Chapter 2 Working with NetApp filers** explains how to use VFM to manage NetApp filers.
- **Chapter 3 Setting replication properties** explains how to use VFM to configure replication properties on machines participating in the namespace.
- **Chapter 4 Working with Physical Resources** explains how to manage Windows® and UNIX® machines.
- **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**

CHAPTER 2 WORKING WITH NETAPP FILERS **3**

SET SNMP COMMUNITY STRING 3
CHANGE THE SHELL CREDENTIALS OF A FILER 4
To change the shell credentials of a filer *4*
SPECIFY THE ONTAPI CREDENTIALS OF A FILER 5
CREATE A REPORT OF MULTIPLE FILERS 5
ENABLE OR DISABLE ALL SNAPMIRROR BACKUPS 5
FILERS NOT IDENTIFIED CORRECTLY 6
CREATE A SNAPMIRROR ON A FILER 6
CREATE A VOLUME ON A FILER 6
CREATE A QTREE ON A FILER 7
ENABLE VFILERS TO PARTICIPATE IN A FILER DISASTER RECOVERY POLICY 7
SCHEDULE SNAPSHOTS ON MULTIPLE FILERS 8
To schedule snapshots on multiple filers *8*
ENABLE OR SUSPEND SNAPSHOT SCHEDULES FOR MULTIPLE FILERS 9
TAKE A SNAPSHOT OF A VOLUME IMMEDIATELY 10
CHANGE THE SNAPSHOT RESERVE FOR MULTIPLE VOLUMES 10
RESTORE A SNAPSHOT 11

CHAPTER 3 WORKING WITH PHYSICAL RESOURCES **13**

The Physical View *13*
ADD A MACHINE TO THE PHYSICAL VIEW 14
REMOVE A MACHINE FROM A FOLDER 15
To remove a machine *15*
To delete a user-defined folder *15*
SPECIFY NTFS CHANGE JOURNAL 15
CREATE SHARES 16
DUPLICATE SHARES 16
DISPLAY DRIVES 18
VIEW ATTRIBUTES OF A MACHINE OR DRIVE 18
VIEW ATTRIBUTES OF A SHARED FOLDER 19
VIEW ATTRIBUTES OF AN EXPORT 19
UPDATE SECURITY OF A FOLDER 19
REFRESH A MACHINE 20
To refresh a machine *20*
To refresh all the machines in a folder *20*
CHANGE THE SHELL CREDENTIALS OF A UNIX MACHINE 21
To change the shell credentials of a UNIX machine *21*
SET NFS CREDENTIALS 22
To set NFS credentials for a filer or UNIX machine *22*
To set default NFS credentials *22*

CHAPTER 4 SETTING REPLICATION PROPERTIES **23**

DISALLOW DEPLOYMENT OF REPLICATION AGENTS 23
SPECIFY A PROXY MACHINE 23
SPECIFY DEFAULT REPLICATION AGENTS 24
SET DATA TRANSFER RATE LIMIT 24

APPENDIX **25**

VFM GUIDES 25
GLOSSARY 27
INDEX 31

Chapter 1 Introduction

This guide provides instructions about how to use VFM to manage physical resources that participate in the namespace or in VFM policies.

Topics are arranged in the following subsections:

- Working with NetApp filers
- Setting replication properties
- Working with physical resources

Chapter 2 Working with NetApp filers

VFM enables you to integrate your NetApp filers into your namespace.

- NetApp filers in the Physical View tree
    - **Integrated management of NetApp filers -** VFM provides integrated in-context access to the FilerView® management tool. When a NetApp filer is selected in the Physical View, a **Manage** tab hosting the FilerView UI is added to the right pane.
    - **Display of NetApp-specific information -** VFM displays information from the NetApp filer, including Data ONTAP version, filer volume names, filer system status information, and NETBIOS aliases in use on the filer.
- NetApp vFiler in the Physical View tree
    - Unlike a NetApp filer, a vFiler does not display a **Manage** tab in the right pane when it is selected in the Physical View. vFilers are managed through their hosting filer.
    - The platform information for a vFiler is Data ONTAP without any revision number. This is because vFilers do not support SNMP.
- If VFM misidentifies a filer or vFiler , right-click the machine, click **Properties**, and select the correct machine identity setting.
- See "Troubleshooting" if filers are misidentified as either generic machines or as vFilers, or if FilerView does not appear in the **Manage** tab.

Set SNMP community string

VFM uses the SNMP community string in the process of identifying NetApp filers and UNIX machines and uses "public" as the default value. You can set the value for a specific machine.

1. In the Physical View tree, right-click a machine and click **Properties**.
2. On the General tab, type a name in the **SNMP community string** field.
3. Click **OK**.

Note: To set application-wide defaults, click **Options** on the **Tools** menu and click **System Options**.

Change the shell credentials of a filer

To manage filers that are members of a policy, you must configure VFM with the system or administrative user account and password of NetApp filers. VFM normally uses RSH to communicate with filers. You can choose to use SSH.

Notes:

- **RSH**

  When user name and password are left blank, VFM uses "`root`" as the user name with no password. You can specify different credentials for a filer or UNIX machine. You can also change the default RSH shell credentials that all new filers and UNIX machines added to VFM will use.

- **SSH**

  Before you can use SSH, you must configure VFM to use the remote shell. See "Use SSH shell credentials" for instructions about how to perform the following tasks:

  - Install and configure OpenSSH.
  - Generate a key-pair.
  - Copy the public key to the filers using SSH.
  - Cache the keys.
  - Provide the location of the `plink` and `pscp` executables.

- **To set default RSH or SSH shell credential** that all new filers and UNIX machines will use, see "Set default remote shell credentials." Machines already known to VFM are not affected.

To change the shell credentials of a filer

1. Right-click the filer either in the Physical View or beneath the policy in which it is contained then click **Properties**.
2. Click the **Shell** tab.
3. Select a type in the **Shell Type** list.
4. Perform one of the following actions:
   - If you select RSH, type the username and password that will be used by VFM to communicate with the filer.
   - If you select SSH, type the location of the private key and the user name that will be used by VFM to communicate with the filer. When VFM uses SSH to communicate with UNIX machines and filers, SSH is configured without a password or passphrase.
5. Click **Fresh Filer Information**.
6. Click **OK**.

Specify the ONTAPI credentials of a filer

VFM uses ONTAPI to communicate with filers. Normally, VFM uses the DCE/RPC protocol. If you want to use HTTP to communicate with a filer or the filer is not running CIFS, you must update the ONTAPI credential information for the filer. If the filer is not known to VFM, add the filer to the Physical View tree before you complete the following instructions.

1. Right-click the filer in the Physical View and click **Properties**.
2. Click the **NetApp Filer** tab.
3. In the **Connection Type** list, select **HTTP**.
4. Type the credentials that VFM will use to communicate with the filer.
5. Click **OK**.

Note: When the DCE/RPC protocol is used to communicate with the filer, the credentials of the account used to run the VFM server and client are used.

Create a report of multiple filers

Create NetApp-specific reports containing information about multiple filers.

1. Perform one of the following actions:
   - On the **Reports** menu, point to **NetApp** then click a report.
   - Right-click Reports or Physical View, point to **NetApp**, and click a report.
   - Right-click the **Namespace Resources** folder under the Physical View tree or on the Properties tab of Physical View, point to **NetApp**, and click a report.
2. Select any or all filers.
3. Click **Next**.
4. Optionally, type a name for the report.
5. Click **Finish**.

Enable or disable all SnapMirror backups

You can enable or disable all the SnapMirror® backups on a filer.

1. Right-click a filer and click **Properties**.
2. Click the **NetApp Filer** tab.
3. Perform one of the following actions:
   - To enable all the SnapMirrors, select **Enable SnapMirrors**.
   - To disable all the SnapMirrors, clear **Disable SnapMirrors**.
4. Click **OK**.
5. Click **Done**.

Filers not identified correctly

You can change a machine setting if VFM does not correctly identify a NetApp filer or vFiler in the Physical View.

1. Right-click the machine and click **Properties**.
2. Select the appropriate machine identity.
3. Click **OK**. When a filer is correctly identified, additional properties tabs appear.

Create a SnapMirror on a filer

Configure a SnapMirror on a NetApp filer. To manage filers, you must configure VFM with the system or administrative user account and password of the filer. You must have write access to `C$\etc` on the filer. For more information, see "SnapMirror Policies."

1. Right-click the filer in the Physical View and click **Properties**.
2. Click the **SnapMirrors** tab.
3. Click **Create**.
4. Select the source and destination.
5. Click the **Options and Schedule** tab and set up the replication schedule.
6. Click **OK**.
7. Click **Done**.

Create a volume on a filer

Configure a traditional volume on a NetApp filer.

1. Perform one of the following actions:
   - Right-click a filer and click **Create Volume**.
   - Right-click the Volumes folder under a filer in the Physical View tree and click **Create Volume**.
   - Select a filer in the **Physical View** tree to show a **Properties** tab in the right pane. Right-click anywhere on the page and click **Create Volume**.
   - Select the **Volume** folder under a filer in the Physical View tree to show a **Properties** tab in the right pane. Right-click anywhere on the page and click **Create Volume**.
2. In the **New Volume Name** field, type the name of the volume. The name can contain alphanumeric characters and underscores "_". The first character must be a letter or an underscore.
3. In the **RAID Group Size** field, type the number of disks per RAID group in the volume. The maximum value is 28, and the default value is 14.
4. Select a language from the list provided.

5. Select one of the following options:
    - **Automatic Disk Selection** enables the system to decide which disks to add, based on your response to the **Number of Disks** to add to the volume and the **size of the disks** to be added.
    - **Manual Disk Selection** enables you to select the disks to add to the new volume.
6. Click **Create**.

Note: To manage filers, you must configure VFM with the system or administrative user RSH account and password of the filer. For more information, see "Manage SnapMirrors."

Create a qtree on a filer

Configure a qtree on a NetApp filer. To manage filers, you must configure VFM with the system or administrative user RSH account and password of the filer. For more information, see "Change the shell credentials of a filer."

1. Right-click a filer in the **Physical View** and click **Properties**.
2. Click the **QTrees** tab and click **Create**.
3. Select the filer.
4. Select the volume on the filer in which you want to create the qtree.
5. Type a name for the qtree.
6. Select the appropriate security style.
7. Select to enable or disable `oplocks`.
8. Click **OK**.

Enable vFilers to participate in a filer disaster recovery policy

To enable a vFiler to participate in a filer disaster recovery policy, the filer that hosts the vFiler must be known to VFM.

1. If the vFiler does not appear in a folder in the Physical View, add the vFiler to a folder.
2. Right-click the vFiler and click **Properties**.
3. Click the **NetApp Filer** tab.
4. Type the name of the filer hosting the vFiler in **Hosting Filer**, or select the filer from the list provided.
5. Click **OK**.
6. Click **Done**.

Schedule snapshots on multiple filers

This is a convenient way to change the snapshot schedule and reserve setting on multiple filers without requiring you to repeat the changes on each individual filer.

To manage filers, you must configure VFM with the system or administrative user account and password of the filer. You must also have write access to `C$\etc` on the filer. See "Managing SnapMirrors on NetApp filers" for more information.

Note: You are warned if some of the volumes on the selected filers are members of other snapshot scheduling policies. When a snapshot scheduling policy manages filer-initiated snapshots and the snapshot schedule of a volume is changed outside the policy, VFM restores the schedule to the policy settings the next time the policy schedule runs.

To schedule snapshots on multiple filers

1. Perform one of the following actions:
   - Right-click a folder in the Physical View and click **Set snapshot schedule**.
   - Select a folder in the **Physical View** to show a Properties tab in the right pane. Select multiple filers on the **Properties** tab, right-click and click **Set snapshot schedule**.
2. Perform one of the following actions:

If...	Then do this...
You want to manage the snapshots, select **Add this volume to a Snapshot Scheduling policy**.	• When you select an existing policy 1. Click **Next**. The name of the policy and a list of the volumes to be added to the policy appears. 2. Click **Finish**. The volumes on the selected filers are added to the policy. • When you click **New Policy** to create a new policy 1. Type a word or phrase that best describes the policy in the **Name** field. 2. Click the **Virtual File Manager Settings** or **Filers Settings** tab and set the schedule for the policy. 3. Click **OK**. A status report appears. 4. Click **Done**. The new policy appears on the list of snapshot scheduling policies. 5. Click **Next**. The name of the policy and a list of the volumes to be added to the policy appears. 6. Click **Finish**. The volumes on the selected filers are added to the new policy.
You want the volumes managed	1. Click **Next**. Normally, **Set the snapshot**

If...	Then do this...
by their respective filers, select **Set the schedule for this volume, but don't add it to a policy**.	**schedule** and **Enable scheduled snapshots** options are selected. 2. Type the number of weekly, daily, and hourly snapshots to retain. 3. Select the time you want to initiate snapshots on the volumes and click **Next**. 4. Perform one of the following actions: • Select **Don't modify the snapshot reserve** if you want to retain the current reserve on the selected volumes. • Select **Set the snapshot reserve** if you want all the selected volumes to have the same reserve. Type the amount of space on the volumes to reserve for snapshots. 5. Click **Next**. A list of the changes to be made appears. 6. Click **Finish**.

Enable or suspend snapshot schedules for multiple filers

You can stop the snapshot schedule from running on volumes on multiple filers. The schedules are not deleted.

1. Perform one of the following actions:
   - Right-click a folder in the Physical View and click **Set snapshot schedule**.
   - Select a folder in the Physical View to show a **Properties** tab in the right pane. Select multiple filers on the **Properties** tab, and right-click and click **Set snapshot schedule**.
2. Click **Next**. The option **Set the schedule for this volume, but don't add it to a policy** is selected.
3. Click **Next**.
4. Select or clear the **Enable scheduled snapshots** check box, depending on whether you want to enable or suspend the snapshot schedule for the selected items and click **Next**.
5. Click **Next**. A list of the changes to be made appears.
6. Click **Finish**.

Notes:

- Suspending a snapshot schedule does not prevent you from manually taking a snapshot. Select a folder in the Physical View that contains filers to show a **Properties** tab in the right pane. Select the filers with volumes you want to take a snapshot of, and right-click and click **Take snapshot now**.
- Existing snapshots on the selected volumes are not deleted when you suspend the schedule.

Take a snapshot of a volume immediately

Manually take a snapshot of NetApp filers.

1. Perform one of the following actions:
    - To take a snapshot of all the volumes on a NetApp filer, right-click the filer and click **Take snapshot now**.
    - To take a snapshot of selected volumes on a NetApp filer, select the filer to show a **Properties** tab in the right pane. Under **Volumes**, select the volumes, right-click, and click **Take snapshot now**.
    - To take a snapshot of the volumes on multiple NetApp filers, right-click the folder in the Physical View that contains filers 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**.

Change the snapshot reserve for multiple volumes

You can change the snapshot reserve for volumes on multiple filers.

1. Perform one of the following actions:
    - To change the snapshot reserve for all the volumes on a NetApp filer, right-click the filer and click **Set snapshot schedule**.
    - To change the snapshot reserve for selected volumes on a NetApp filer, select the filer to show a Properties tab in the right pane. Under Volumes, select the volumes, right-click, and click **Set snapshot schedule**.
    - To change the snapshot reserve for the volumes on multiple NetApp filers, right-click the folder in the Physical View that contains filers and click **Set snapshot schedule**.
2. Click **Next**.
3. Make sure that the option **Set the schedule for this volume, but do not add it to this policy** is selected. Click **Next**.

4. Select **Don't modify the snapshot schedule** and click **Next**.
5. Make sure that the option **Set the snapshot reserve** is selected. Type the amount of space the volumes must reserve for snapshots.
6. Click **Next**. Verify the changes that are to be made to the volumes.
7. Click **Finish**.

Restore a snapshot

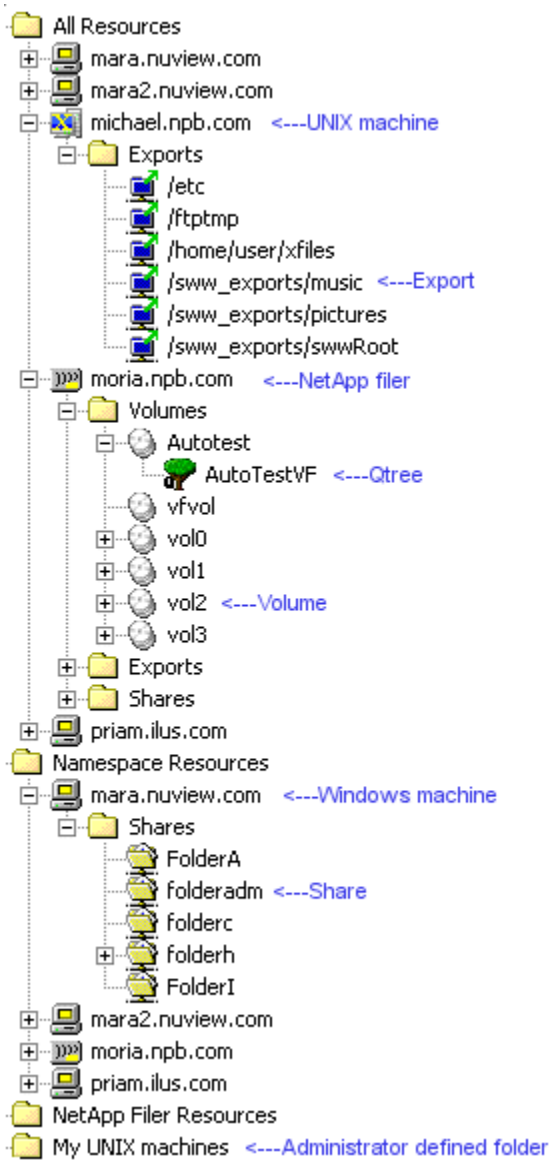
Restore snapshot data to its original location on a NetApp filer.

1. Select a filer or volume in the **Physical View** to show tabs in the right pane.
2. Click the **Snapshots** tab.
3. Right-click a snapshot and click **Restore**.
4. Click **Yes**.

Chapter 3 Working with Physical Resources

This section provides instructions about managing machines from the Physical View.

The Physical View



The Physical View shows machines participating in the namespace or a policy and machines you add to folders that you create in the Physical View tree.

- The **Namespace Resources** folder in the Physical View tree is automatically populated with a list of the machines participating in the logical namespace. You can create additional folders in the Physical View to organize your view of the machines. You can add machines to the folders you create whether or not the machines participate in the logical namespace.
- Machines in the Physical View tree that do not participate in the namespace are indicated by .
- A machine can appear in multiple folders.
- You can only add and remove machines from Physical View folders that you create. VFM automatically maintains the contents of the following folders:
    - All Resources
    - Namespace Resources
    - NetApp Filer Resources
- After you add a machine to a user-defined folder in the Physical View tree, you can drag a shared folder on the machine to a root in the Logical View to create a link in the namespace. When you do this, the machine is added to the **Namespace Resources** folder.

Note: You cannot drag an export in the Physical View to a root in the Logical View because links cannot reference exports.

- NetApp filers appear in the Physical View tree with a NetApp-specific icon or , indicating whether they participate in the namespace.
- NetApp vFiler images appear in the Physical View tree with a NetApp-specific icon or , indicating whether they participate in the namespace.
- UNIX machines appear in the Physical View with a unique icon .

Add a machine to the physical view

Create a folder in the Physical View to contain the machines that you want to add.

1. Right-click Physical View and click **Add folder**.
2. Type a name for the folder and click **OK**.
3. Perform one of the following actions:
    - Drag a machine from the **Namespace Resources** or **All Resources** folder to the folder you created.
    - Drag a machine from Windows Explorer to the folder you created in the Physical View tree or on the **Properties** tab of Physical View .
    - Right-click the folder you created and click **Add Machine**. Use this option to add UNIX NFS machines to the Physical View.

Notes:

- It is recommended that you reference machines using their NETBIOS name rather than IP address or fully qualified DNS name.
- If a machine appears in the Physical View with a name that is not what you expect, check whether DNS reverse lookups are configured correctly for the machine.

Remove a machine from a folder

Remove a machine from a user-defined folder and delete user-defined folders in the Physical View tree.

To remove a machine

1. In the Physical View tree, open a user-defined folder.
2. Right-click a machine and click **Remove from folder**.

Notes:

- If the machine participates in the namespace, it continues to appear in the **Namespace Resources** folder.
- If the machine is not participating in the namespace but appears in more than one user-defined folder, it is removed only from the folder you indicated.

To delete a user-defined folder

Right-click a folder and click **Delete**.

Specify NTFS Change Journal

You can enable NTFS Change Journal for NTFS volumes on machines running Windows 2000 and later. When this option is enabled, VFM deploys a replication agent on the machine where the source data resides. This is a deviation from the standard VFM replication agent deployment algorithm.

1. Right-click a machine in the **Physical View** tree and click **Properties**.
2. Click the **Agent** tab.
3. Click **Allow replication agent to be deployed to this host**.
4. Click **Use NTFS Change Journal on this host**.
5. Click **OK**.

Notes:

- For information about problems you might encounter using NTFS Change Journal, see "Problems using NTFS Change Journal."
- For an explanation about how VFM distributes replication agents, see "Distributed replication."

Create shares

Create a share on one or more machines and set share and folder permissions. In addition, you can add the shares to a new or existing link, or create new links for each share. This is a quick way of setting up shares for use in a disaster recovery or replication policy.

1. Right-click a machine in the **Physical View** tree and click **Create shares**.
2. Click **Next**.
3. Type the appropriate information and click **Next**. When creating shares on a NetApp filer, you must use the NetApp naming convention (for example, `c:\vol\voln\<directory name>`, where "*n*" is the appropriate volume number and "`<directory name>`" is the name of the directory to be shared.
4. Select the machines where you want to create the share and click **Next**.
5. Perform one of the following actions:
   - Select **Do not modify any DFS links** if you do not want to add the shares to a link.
   - Select one of the other options if you want to add the shares to the namespace. Click **Next**. Select a DFS root or DFS link, depending on the option you selected.
6. Click **Next**.
7. Click **Finish**.

Notes: You can also create shares on a machine by performing one of the following actions:

- Drag a share from a machine in the Physical View tree to another machine in the Physical View tree.
- Drag a share on the **Properties** tab of any item in the Logical View or Physical View to a machine in the Physical View tree.

Duplicate shares

Copy multiple shares from one server to another server. You can specify whether to copy all the shares on the source server or only the shares referenced in your namespace. You can also run batch files before and after each share is created.

Note: Data is not migrated. To migrate data, create a migration policy.

1. On the **Tools** menu, click **Create shares**.
2. Click **Next**.
3. Select **Duplicate Shared From** and type the name of the source and destination servers or browse for the servers in your network.
4. Click **Next**.
5. Select one of the following options:
   - **Only duplicate shares referenced by the logical namespace** - Select this if you want to duplicate only the shares on the source server that are referenced in your namespace.
   - **Duplicate all shares** - Select this if you want to duplicate all the shares on the source server. This option enables you to duplicate hidden shares.

6. Select **Run pre-creation batch file** and type the path of the batch file or click **Browse**. The batch file runs before each share is created. See the notes at the end of this topic for information about running batch files in VFM and more information about the batch file.
7. Select **Run post-creation batch file** and type the path of the batch file or click **Browse**. The batch file runs after each share is created. See the notes at the end of this topic for information about running batch files in VFM and more information about the batch file.
8. Click **Next**.
9. Review the list of source and destination shares.
    - Clear the shares that you do not want to duplicate.
    - To change a destination path, click the destination path and type a new path or click **Browse** to locate a new share.
    - To change the destination path for multiple selected shares, click **Rebase**.
    - Clear **Warn if destination already contains files or folders** if you do not want to check for destination shares that are not empty.
10. Click **Next**. The policy checks for empty destination shares and destination shares that do not exist.
11. If destination shares that are not empty are found, the shares appear in a list. You can continue or select each share and type a different destination share, browse for another share, or remove the share from the duplication process. If destination shares that do not exist are found, the shares appear in a list with a suggested local path for each share.
    - To change the local path for multiple items, select the items and click **Rebase**. Type your changes and click **OK**.
    - To change one local path, select the item and type a new path.
    - To accept all or some of the suggested local paths, select the items on the list and click **Create Destination Share**.
12. Click **Next**.
13. A list of source and destination paths that are validated display. You can clear items that you do not want to duplicate or change the destination path of an item.
14. Click **Next**.
15. Perform one of the following actions:
    - Select **Do not modify any DFS links** if you do not want to add the shares to a link.
    - Select one of the other options if you want to add the shares to the namespace. Click **Next**. Select a DFS root or DFS link, depending on the option you selected.
16. Click **Next**.
17. Click **Finish**.

Notes:

- For detailed information about configuring batch files to run in storage policies, see "Running batch files" in the Tapestry StorageX *Advanced Configuration and Techniques* guide.
- For detailed information about the example scripts provided by VFM, see "Batch files" in the Tapestry StorageX *Advanced Configuration and Techniques* guide.

Display drives

By default, servers and shared folders are displayed in the **Physical View** tree. You can select to display the drives.

1. On the **Tools** menu, click **Options**.
2. Select the **Show drives in physical views** check box.
3. Click **OK**.

Note: Displaying drives in the Physical View requires gathering additional data from servers; this process can slow the display of information in VFM when managing a large configuration or configurations in which servers are inaccessible.

View attributes of a machine or drive

View the properties and references of a machine or drive that appear in the Physical View tree. In the Physical View tree, click the machine or drive to display the following tabs in the right pane:

- **Properties -** Displays the characteristics or parameters of the selected machine or drive. Right-click an item on the tab to view a context menu.
- **Status** - Shows information concerning attempts by VFM to communicate with the machine or filer.
- **Replication Tasks -** Shows information about replication operations.
- **Snapshots** - Shows information about snapshots. This tab only appears if a folder contains a NetApp or Windows Powered NAS/Windows Storage Server filer or if the item selected is a filer or a volume on a filer.
- **References -** Shows the DFS link referencing the machine or shared folder. Right-click a root or link to view a context menu.
- **Events** - Shows the history of events for the item selected.
- **Manage** - Only appears if the device selected is a NetApp or Windows Powered NAS/Windows Storage Server filer. You can access FilerView or the Windows Powered NAS/Windows Storage Server Web Management UI from this tab.
- **Reports** - Shows a list of reports generated that reference the machine or filer.

View attributes of a shared folder

View the attributes of a CIFS shared folder. The Physical View tree can contain shared folders that participate in the namespace and shared folders that do not participate in the namespace.

In the Physical View tree, click a machine, click the **Shares** folder, and click the share. The following tabs appear in the right pane:

- **Properties** - Displays the characteristics or parameters of the selected share. Right-click anywhere on the tab to view a context menu.
- **Replication Tasks** - Shows information about replication operations.
- **References -** Shows the DFS links that reference the shared folder. Right-click a root or link to view a context menu.
- **Events -** Shows the history of events for the item selected.
- **Reports** - Shows a list of reports generated that reference the shared folder.

Note: The application displays share information that is returned by the system hosting the share. Information such as local path and connection limit might not be displayed for a share if the system hosting the share does not provide this information.

View attributes of an export

View the attributes of an export . In the Physical View tree, click a machine, click the **Exports** folder, and click the export. The following tabs appear in the right pane:

- **Properties** - Displays the name and security permissions of the selected export. Right-click anywhere on the tab to view a context menu.
- **Replication Tasks** - Shows information about replication operations.
- **Events** - Shows information about the export.
- **Reports** - Shows a list of reports generated that reference the export.

Update security of a folder

Update permissions for a shared folder.

1. Perform one of the following actions:
    - Click a link in the **Logical View**. On the **Properties** tab, right-click a target.
    - Click a domain-based root in the **Logical View**. On the **Properties** tab, right-click a replica.
    - Right-click a folder in the **Physical View**.
    - Click a replication policy under the **Replication Policies** folder in **Admin View**. Click the **Replication** tab that appears in the right pane. Right-click a shared folder.
2. Click **Properties**.
3. Click the **Security** tab.

4. Update permissions and click **OK**.

Note: If the "Unable to display security information" message appears when you click the **Security** tab, you do not have permission to view or edit the security of the folder.

Refresh a machine

Update the information about a machine and all the shared folders on the machine.

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 View or Physical View, right-click **Logical View** or **Physical View** in the tree and click **Refresh**.

To refresh a machine

Perform one of the following actions:

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

To refresh all the machines in a folder

Update the information about all the machines in the **Namespace Resources** folder or a user-defined folder in the **Physical View**.

Perform one of the following actions:

- Right-click the **Namespace Resources** folder or a user-defined folder and click **Refresh**.
- Select the **Namespace Resources** folder or a user-defined folder and press **F5**.
- Select the **Namespace Resources** folder or a user-defined folder and click **Refresh** on the main toolbar.
- Select the **Namespace Resources** folder or a user-defined folder and click **Refresh** on the **View** menu.

Change the shell credentials of a UNIX machine

To manage UNIX machines that are members of a policy, you must configure VFM with the system or administrative user account and password of the machines. Normally, VFM uses RSH to communicate with UNIX machines. You can choose to use SSH.

Notes:

- **RSH**

  When user name and password are left blank, VFM uses `root` as the user name with no password. You can specify different credentials for a filer or UNIX machine. You can also change the default RSH shell credentials that all new filers and UNIX machines added to VFM will use.

- **SSH**

  Before you can use SSH, you must configure VFM to use the remote shell. See "Use SSH shell credentials" for instructions about how to perform the following tasks:

  - Install and configure OpenSSH.
  - Generate a key-pair.
  - Copy the public key to the filers using SSH.
  - Cache the keys.
  - Provide the location of the `plink` and `pscp` executables.

- To set default RSH or SSH shell credential that all new filers and UNIX machines will use, see "Set default remote shell credentials." Machines already known to VFM are not affected.

To change the shell credentials of a UNIX machine

1. Right-click the UNIX machine either in the **Physical View** or beneath the policy in which it is contained and click **Properties**.
2. Click the **Shell** tab.
3. Select a type in the **Shell Type** list.
4. Perform one of the following actions:
   - If you select RSH, type the username and password that will be used by VFM to communicate with the machine.
   - If you select SSH, type the location of the private key and the user name that will be used by VFM to communicate with the filer. When VFM uses SSH to communicate with UNIX machines and filers, SSH is configured without a password or passphrase.
5. Click **OK**.

Set NFS credentials

Normally, UNIX replication agents use `root(0)` when communicating with the source and destination during NFS data transfers. You can change the NFS credentials for individual filers and UNIX machines appearing in the Physical View. You can also set default NFS credentials for all new UNIX machines and filers added to the Physical View. The NFS credentials of filers and UNIX machines already appearing in the Physical View are not changed.

To set NFS credentials for a filer or UNIX machine

1. Right-click the UNIX machine either in the Physical View or beneath the policy in which it is contained and click **Properties**.
2. On the **General** tab, type a different **Default User ID** and/or **Default Group ID**.
3. Click **OK**.

To set default NFS credentials

1. On the **Tools** menu, click **Options**.
2. Click **System Options** to show a dialog box in the right pane.
3. Under NFS Settings, type a different **Default User ID** and/or **Default Group ID**.
4. Click **OK**.

Chapter 4 Setting Replication Properties

This section provides instructions about how to set replication properties on machines participating in the namespace or a storage policy.

- To specify a Windows or UNIX machine as a proxy to host a replication agent instead of having the agent deployed to a Windows or UNIX machine participating in a policy, see "Specify a proxy machine."
- To prevent deployment of a replication agent to a machine, see "Disallow deployment of replication agents."
- To specify application-wide default Windows and UNIX replication agents, see "Specify default replication agents."
- To set bandwidth throttling for a machine hosting a replication agent, see "Set data transfer rate limit."

Disallow deployment of replication agents

Replication agents are installed on Windows or UNIX machines participating in policies that transfer CIFS or NFS data. You can prevent deployment of agents to individual machines.

1. On the Physical View tree, right-click a machine and click **Properties**.
2. Click the **Agent** tab.
3. Clear **Allow replication agent to be deployed to this host**.
4. Click **OK**.

Note: For detailed information about replication agents, such as system requirements and instructions about how to manually deploy agents, see "Manage replication agents" in the Tapestry StorageX *Advanced Configuration and Techniques* guide.

Specify a proxy machine

VFM deploys Windows and UNIX replication agents to machines participating in policies that transfer data. You can specify a proxy machine to host the replication agent instead of having the agent deployed to a machine participating in the policy.

Notes:

- If the machine to which you want to deploy a replication agent is running Windows XP SP 2, you must perform the following actions:
    1. Disable the firewall on the machine to which you want to deploy the replication agent.
    2. Restart the machine.
- For Windows and UNIX replication agent system requirements, see "Manage replication agents."

1. In the Physical View tree, right-click a machine and click **Properties**.
2. Click the **Agent** tab.
3. Perform one of the following actions:
   - Select **Use default proxy** to use the machine you specified as the application-wide default system option.

     Note: To set application-wide default Windows and UNIX replication agents, see "Specify default replication agents."

   - Select **Use this specified proxy** to select a machine to which you want to deploy a replication agent. Type the path of the machine in the appropriate text box, or click ... **Browse** to locate the machine in your network.
4. Click **OK**.

Specify default replication agents

You can specify application-wide default proxy replication agents for policies that transfer data. You can specify a replication agent for Windows and UNIX. When VFM cannot deploy a Windows or UNIX agent onto the source or destination, VFM uses the default agents you specify.

1. On the **Tools** menu, click **Options**.
2. Select **Systems Options**.
3. Under **Default Replication Agents**, specify a machine hosting a Windows or UNIX replication agent or a machine to which you want to deploy a replication agent during data transfer.
4. Click **OK**.

Set data transfer rate limit

Set the replication data transfer rate limit or bandwidth throttling for a machine that is hosting or will host a replication agent.

1. In the Physical View tree, right-click a machine and click **Properties**.
2. Click the **Agent** tab.
3. Select **Allow replication agent to be deployed to this host**.
4. Under **Throttling for replication agent on this host**, select the business hours for weekdays and weekends.
5. Type or select a rate, in bytes per second, for business and non-business hours.
6. Click **OK**.

Note: If you change throttling on a machine hosting a replication agent while the agent is replicating data, the changes are not implemented for the task currently running. Changes in throttling values appear in the replication tasks view and replication ToolTips the next time the task runs.

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 Windows and UNIX machines

No.	Title	File name	Contents
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

Add a machine 14
Agents
disallow deployment of replication agents ... 23
Agents 23
Attributes
of a share 19
of an export 19
Community name 3
Computers
view properties 18
view references 18
Computers 18
Configure a qtree 7
Create a qtree 7
Create a volume on a filer 6
Data distribution 19
Data replication 6
Data transfer
disallow deployment of data move agents ... 23
Data transfer 6
Data transfer 23
Disable SnapMirrors 5
Display drives 18
Drag a machine to a user-defined folder 14
Drives
view properties 18
view references 18
Drives 18
Drives 18
Enable SnapMirrors 5
Export
view properties 19
Export 19
Filers
change NFS credentials 22
change snapshot reserve on multiple volumes 10
create a volume 6
data transfer 6
enable snapshot schedules 9
misidentified 6
NetApp reports 5
schedule snapshots 8
specify ONTAPI credentials 5
suspend snapshot schedules 9
take a snapshot on multiple volumes immediately 10
Filers 5
Folder
add a folder 16
add a machine 14
add multiple folders 16
create a share 16
remove a machine 15
Hide drives 18
HTTP 5
Machine identity 6
Machine properties 3, 6
Machines
add a machine 14
create a share 16
disallow deployment of data move agents ... 23
misidentified 6
refresh a machine 20
remove from a folder 15
set SNMP community name 3
view properties 18
view references 18
Machines 14
NetApp filers
change snapshot reserve on multiple volumes 10
configure a qtree 7
configure a SnapMirror 6
disable SnapMirrors 5
enable SnapMirrors 5
enable snapshot schedules 9
reports 5
schedule snapshots 8
suspend snapshot schedules 9
NFS credentials 22
ONTAPI 5
Permissions 19
Properties
of a share 19
of an export 19
Properties 18
Properties 19
Properties 19
qtree
create a qtree 7
qtree 7
References 18
Refresh
data from network 20
Refresh 20
Replication agent
disallow deployment 23
Replication policy
share permissions 19
Reports
NetApp filer reports 5
Restore data 11
RPC 5
RSH 4, 21
SAK filer 18

Security.....19
Set SNMP community name 3
Shared folder
  create a share.....16
  permissions 16, 19
  view properties.....19
Shares
  duplicate shares.....16
Shares 16
Shell credentials 4, 21
SnapMirror
  disable SnapMirrors on a filer.....5
  enable SnapMirrors on a filer.....5
SnapMirror 5
Snapshots
  change reserve on multiple volumes 10
  enable the schedule on multiple filers.....9
  restore data 11
  suspend the schedule on multiple filers.....9
  take a snapshot immediately 10
SNMP community name 3
SSH.....4, 21
Suspend snapshot schedules 9
Take a manual snapshot..... 10
Turn off SnapMirrors..... 5
Turn on SnapMirrors 5
UNIX machine
  change NFS credentials..... 22
  shell credentials..... 21
UNIX machine..... 21
UNIX machine..... 22
Update information about a machine..... 20
User-defined folder..... 14
vFilers
  add to filer disaster recovery policy 7
  misidentified..... 6
vFilers..... 7
View drives in the Physical View tree..... 18
Volumes
  change snapshot reserve 10
  enable the snapshot schedule..... 9
  suspend the snapshot schedule 9
  take a snapshot immediately..... 10