NetworkAppliance®

The evolution of storage.™

VFM (Virtual File Manager) v6.0 Troubleshooting

May 29, 2007

Publication Number: 215-03211_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 provides a list of problems that you might encounter and explains how to fix the problems. It also provides a description of status indicators used as visual cues throughout Network Appliance® VFM®. The guide provides examples of exclusion and inclusion file formats.

The guide is divided into the following sections:

- **Chapter 1 Introduction** provides an overview of the document.
- **Chapter 2 Troubleshooting** provides troubleshooting information.
- **Appendix A Migration, replication, and status indicators** provides a description of migration task, replication status monitoring, and status indicators.
- **Appendix B Exclusion/inclusion examples** provides examples of exclusion and inclusion file and directory formats.
- **Appendix C VFM Documentation** 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)

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 TROUBLESHOOTING **3**

General problems 3
DFS root problems 6
Report problems 9
Target problems 10
Windows XP and Windows 2000 incompatibility problem 10
Problems connecting to the VFM Server service 11
Problems selecting a monitoring agent 12
Replication and migration problems 13
NetApp filer problems 25
Browse namespace problems 28
Windows powered NAS or Windows storage server filer identification problems 29
Problems running batch files 29
Problems running a policy 30
Snapshot access policy problems 31
Problems printing to PDF files 32
Name of machine is incorrect 32
Problems taking snapshots of the application 32
Permission based namespace policy problems 33
Problem installing a UNIX replication agent 33
Problems using NTFS Change Journal 34
Problem configuring the OpenSSh package on Solaris 35
Problem accessing a UNIX machine when using SSH 36
Problem importing snapshots of the application 37
Problems replicating data using VSS snapshots 37
Problems deleting items from the Logical View 38
Problem updating home directories 38

APPENDIX A MIGRATION, REPLICATION, AND STATUS INDICATORS **41**

Migration task indicators 41
Replication status monitoring indicators 41
Status indicators 43

APPENDIX B EXCLUSION/INCLUSION EXAMPLES **47**

Exclusion examples 47
Inclusion examples 50

APPENDIX C VFM DOCUMENTATION **53**

GLOSSARY **55**

INDEX **59**

Chapter 1 Introduction

This section provides a list of problems that you might encounter and explains about how to fix the problems. It also includes a list of events logged by VFM and lists of status indicators used throughout the application. The following topics are included in this manual:

- Troubleshooting
- Migration task indicators
- Replication status monitoring indicators
- Status indicators

Chapter 2 Troubleshooting

Start by checking the health of your VFM configuration then browse the list of problems in the table below.

- Are the VFM Server and StorageX Replication Agent services running on the machines where the VFM server or monitoring agent components are installed? Click **Agent Management** on the **Tools** menu to view the list of services installed on the system and ensure that the VFM Server and StorageX Replication Agent services are enabled and started.
- Does sufficient free space exist on the drive containing "Documents and Settings" directories on the system where VFM is installed?
- Does the account used by the VFM Server service have appropriate privileges to manage the selected DFS roots and access the source and destination of any data transfers?
- Does the account used to run the VFM console have administrator privileges on the system where it is installed?

General problems

If...	**Then do this...**
VFM seems slow to respond, or takes up a large amount of CPU.	• Check how many links are present in the DFS configuration. Larger configurations require VFM to gather additional information. • Verify that targets of links are reachable from the VFM console machine. • Verify that network browsing works correctly for regular Windows tools, such as Windows Explorer. • Check what level of status monitoring is enabled (root, link, storage) and what frequency monitoring is taking place. • Enabling the "show drives in physical views" option causes VFM to gather additional information and can slow operation, especially when target machines are not reachable from the VFM console machine.
You experience access denied errors while setting VFM system options.	The account running the VFM client must have permissions to write to the directory tree `All Users\Application Data\NetApp \VFM\GuiConsole`. Write permission for these directories is typically granted to members of the local administrators group and the local power users group.

General problems

If...	Then do this...
VFM reports an error about expired evaluation copy.	• Your evaluation copy expired. Contact your supplier to request an extension or to purchase a copy of VFM. • This error message can result when the currently logged in user attempting to run the VFM console is not a member of the administrators group on the local system.
VFM refuses to install.	• VFM currently supports installation only on Windows 2000 SP 2 or later. • Check whether the problem is installing MSDE. Microsoft KB article 315083 details various steps to take when troubleshooting a failed MSDE installation attempt.
You cannot drag-and-drop items out of Windows Explorer into VFM.	Items dragged to VFM must be network paths. You can map shares from remote machines as drives on your machine or address them as UNC paths. For local drives on your machine, you must address them as UNC paths (`\\server\dir\`).
You can only rearrange items displayed in **Bold** in the "Add Multiple Links" dialog box.	This is normal behavior. Use the VFM Logical View to make such changes when needed.
You encounter errors creating logical folders in your namespace	• Check that the permissions on the DFS root share allow the account running the VFM console the ability to make changes to the share. • Windows Server 2003 creates shares with default permissions of Everyone>Read. Windows 2000 creates shares with default permissions of Everyone>Full. The VFM server account must have permissions to write to the DFS root share to create logical directories in the namespace.
You changed your DFS configuration but client machines still access the old locations.	Clients cache referrals for a period of time. You can flush the client cache on Windows 2000 and later by performing one of the following actions: • Use the DFS tab of Windows Explorer Property dialog box to “clear history”. • Run `dfsutil` with appropriate options on the client machine. • You must reboot clients running older operating systems, such as NT 4, Windows 98, or Windows 95, to clear the cache.

If...	Then do this...
VFM shows the wrong date and time for a NetApp filer message appearing in the Event View.	Check whether you correctly set up remote shell credentials on the filer. Normally, VFM uses RSH to communicate with NetApp filers and other non-Windows systems. When the remote shell credentials on the filer are not properly configured, VFM shows the filer message with the same date and time as the VFM server.
You see the error message "Network resource not found" when you try to upgrade the replication agent installed on the same machine as the VFM server.	• Check whether the VFM 5.5 server was uninstalled and the VFM 5.5 R2 server was installed. • Before you upgrade the 5.5 replication agent, open a command prompt and change to the directory where the agent is installed and type the following command: `ReplicationAgent.exe -uninstall`
The VFM desktop does not display correctly. The left pane is blank.	• Check whether you are using the Virtual Network Computing (VNC) desktop protocol to connect to remote machines. • It is highly recommended that you use Remote Desktop to communicate with remote machines. Remote Desktop Protocol (RDP) is a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services. The server listens by default on TCP port 3389.
You installed the VFM client on the same machine that you previously installed a monitoring agent. When you select an item from a view on the left pane, the right pane is blank.	If you installed the VFM client after you installed the monitoring agent, perform the following actions to correct the problem: 1. Close the VFM client. 2. Start a command-line prompt window. 3. Change directory to the VFM installation directory. 4. Run the command: `REGSVR32 GuiControls.dll` You will see a message confirming that the registration was successful.

DFS root problems

If...	Then do this...
You do not see your roots in the VFM browse dialog box. You might see one of the following error messages: • "Unable to display the DFS Root <hostname>. The network resource was not found." • "Unavailable" status in the UI and the root shows error status .	• Check whether network browsing is working correctly in Windows Explorer and correct any browsing problems. • Type the root name directly rather than browsing. • Check whether the DFS service is started on the machines hosting the roots. Microsoft Windows Server 2003 SP 1 ships with the DFS service stopped as the default.
Changes made to domain roots (for example, creation or deletion) take a long time to appear in VFM.	Information about domain roots is hosted in Active Directory. There is a time lag while Active Directory replicates the changes. This time lag is affected by the Active Directory configuration.

If...	Then do this...
You cannot create a DFS root using VFM or you cannot create links on a root. You might see one of the following error messages: • "Error: the network resource was not found." • "An error occurred while trying to take the following action. Action: Create DFS root \\hostname \rootname on server 'hostname' using share <name of share>. • "The DFS Root, link or replica could not be added."	• Check network connectivity by pinging the server the root is created on from the VFM machine. • Check that the account running VFM has appropriate privileges for the domain and servers where the domain-based root is being created or server where the stand-alone root is being created. • Check whether forward and reverse DNS lookups are accurate for the machine on which you want to create the root. • Check whether you are trying to use a share to create the root that contains a root. • Check whether you are trying to use a folder to create the root that is a sub-directory of a share that contains a root. • Check whether the DFS service is started on the machine where you want to create the root. • Check whether the DFS service is started on the machine hosting the root where you want to create a link. • Check whether the DFS service is started on the machine hosting the root where you want to create a link.
You cannot add links to a DFS root.	• Check that the account running VFM has appropriate permissions for the DFS root being manipulated. • Check whether forward and reverse DNS lookups are accurate for the machine hosting the DFS root. • Verify that all root replica share names of a domain-based root match the name of the DFS root. This is particularly important for roots hosted on Windows Server 2003 systems.
Attribute sets are different between different types of roots.	The attributes that are available and capable of being set vary between NT4 roots, Windows 2000 stand-alone roots and domain-based roots. This is an artifact of DFS itself on these platforms and not a problem with VFM.

DFS root problems

If...	Then do this...
You have problems creating a domain-based root with replicas . After the domain-based root is created • It appears as a single replica root • The status of the root is displayed as inaccessible	• The creation of and operation on domain-based roots involves interactions with Active Directory. The Active Directory replication frequency affects how quickly changes appear in the VFM console. • Name resolution issues can affect the creation of domain-based roots. You might need to refer to the domain-based root by its fully-qualified domain name when accessing it when attempts to access it by its NETBIOS domain name are unsuccessful or result in inaccurate data. • Verify that all root replica share names of a domain-based root match the name of the DFS root. This is particularly important for roots hosted on Windows Server 2003 systems.
Morphed filenames appear in the namespace of domain root replicas	Do not enable FRS at the root level. The Microsoft DFS FAQ http://www.microsoft.com/windowsserver2003/techinfo/overview/dfsfaq.mspx describes this symptom in more detail.
You get the following error when accessing a link contained in a consolidation root: "No network provider accepted the given path"	• Check whether the link is under a logical folder. You must configure links in consolidation roots directly under the root. They cannot be referenced under logical folders. This restriction applies only to consolidation roots. • For more information about consolidation roots, see Microsoft Knowledge Base Article 829885.
You see the error message “The request is not supported” when attempting to create a DFS root.	This typically occurs when attempting to create a second DFS root on Windows 2000 or Windows Server 2003 Standard Edition server. Windows 2000 and Windows Server 2003 Standard Edition supports only one DFS root per computer. Windows Server 2003 Enterprise Server and Windows Server 2003 Datacenter support multiple DFS roots per server.

Report problems

If...	Then do this...
You experience errors attempting to run VFM reports.	The account running the VFM client must have permissions to write to the directory tree `All Users\Application Data\NetApp\VFM\GuiConsole`. Write permission for these directories is typically granted to members of the local administrators group and the local power users group.
Reports are slow to generate.	• Check the items under "General problems" for “VFM seems slow to respond....” • Check whether you created a new report group when you created the report. Before VFM can create the report, the report group must gather the data. To cut down on report generation, create report groups to gather data before you assign and run reports based on the data gathered. • Create multiple reports instead of one large report. • Schedule report groups so that reports assigned to the report groups are available when needed for review.

Target problems

If...	Then do this...
VFM does not enumerate (browse) shares hosted on NetWare®, Win9x, and WinME systems.	These operating systems do not support the system calls required by VFM to gather information about their shares. You can add shares from these systems to your namespace by dragging their UNC paths from Windows Explorer and dropping them into any of the following: VFM Logical View, Add Link dialog box, Add Multiple Links dialog box.
When selecting targets for links, I do not see any entries in the Browse dialog box.	You might have browsed into a leaf directory and there are no subfolders available at this level to which you can target links.
You see the error message, "There were no targets for disaster recovery link on a disaster recovery policy.	Links that are members of disaster recovery policies must have at least two replicated targets. Only one target can be online. When the server containing the active target becomes unavailable, VFM fails over the link to the replicated target and makes it the online target. For more information about failing over links, see "Failover and replication options."
You see the error message, "A new link was detected for the disaster recovery policy but the link cannot be added for the stated reasons."	• Check whether the root containing the link is hosted on NT4. NT4 does not support setting link target state. • Check whether the link is already in another disaster recovery policy. • See "Disaster recovery planning considerations" for more information.

Windows XP and Windows 2000 incompatibility problem

If...	Then do this...
Links for a stand-alone root installed on a machine running Windows 2000 do not appear when VFM is running on Windows XP.	Upgrade Windows 2000 to Service Pack 2 on the machine containing the stand-alone root.

Problems connecting to the VFM Server service

If...	Then do this...
The connection was refused by the VFM Server service.	• The VFM Server service might have been stopped through the Windows Service Control Manager. Restart the VFM Server service. • The machine hosting the VFM Server service might not be reachable by the VFM console. Check your network connectivity and the machine hosting the VFM Server service. • Check whether the account configured for the VFM Server service is in the local administrators group on the system where it is installed.
The VFM client reports access denied error attempting to connect to the VFM server.	Contact your VFM administrator to obtain access to the VFM server for your account.
The VFM client does not show updates.	Check whether there is a loss of network connection between the VFM client and server. Clear this problem by exiting and reentering the VFM client.

Problems selecting a monitoring agent

If...	Then do this...
A monitoring agent is installed but does not appear as a choice in the **Use the Monitor on** list when configuring a client disaster recovery policy.	• Check that the machines on which the monitoring agent and the VFM Server service are running have network connectivity with one another. • Check that the monitoring agent is configured with the correct hostname for the machine where the VFM Server service is running. This value is stored in the registry at *HKLM\Software\Brocade\Tapestry StorageX\ Services \Server\Primary*. • Check that no firewalls are blocking TCP port 6001 between the monitoring agent and the VFM Server service. **Note:** The following tables list the network ports used by DFS and VFM. **Network Ports Used by DFS** **Service Name** / **UDP** / **TCP** NetBIOS Datagram Service / 138 / NetBIOS Session Service / / 139 LDAP Server / 389 / 389 Remote Procedure Call (RPC) / / 135 Server Message Block (SMB) / 445 / 445 **Network Ports Used by VFM** **Service Name** / **UDP** / **TCP** VFM Server or monitoring agent / / 6001 and 6005 StorageX Replication Agent / / 6002 **Note:** • The VFM server and UNIX Replication Agent communicate with storage devices using NFS during NFS migrations. • The VFM server uses SNMP when identifying Network Appliance filers. • The VFM server uses RSH or SSH when issuing some commands to UNIX machines and Network Appliance filers.

Replication and migration problems

If...	Then do this...
VFM reports error messages indicating that the replication agent did not respond either in reports or in relation to replication tasks and your VFM server is installed on Windows 2000 Professional or Windows XP.	• Check the number of inbound connections on the machine hosting the VFM server. The VFM server accepts inbound connections from replication agents in response to commands sent from the server to the replication agents. If these connections in conjunction with other connections existing on the machine exceed the limits imposed by Windows 2000 Professional and Windows XP, the VFM server cannot receive responses from its replication agents and reports errors. Microsoft Knowledge Base article 122920 documents these limits for Windows 2000, and Microsoft Knowledge Base article 314882 describes the limits in Windows XP. If the connection count limits are an issue in your environment, run the VFM server on a Windows 2000 Server to avoid this problem. • Check whether the replication agent can communicate with the machine hosting the VFM server using the NETBIOS host name. Verify that the replication agent can ping the machine hosting the VFM server using the host name. If it is necessary, add an entry to the hosts file on the machine hosting the replication agent, or edit `resolv.conf` (UNIX replication agents only) so that the machine hosting the replication agent can communicate with the machine hosting the VFM server by using its NETBIOS host name.
VFM documentation mentions NFS file systems but you do not see them when you browse the network from your VFM console machine.	Windows clients need additional software to access NFS file systems. This additional software can be Microsoft tools, such as Services for UNIX® (either client or server), or various third-party NFS redirectors.
VFM reports an error when attempting to copy files when you can successfully copy them using Windows Explorer.	• VFM uses the backup read/write APIs to get the most accurate transfer of the source file and its associated attributes. Using these APIs requires specific privileges that your account might lack on the source or destination machines. Although Windows Explorer might copy the file data, attributes such as those governing security might be changed during the course of the transfer. • When copying files with summary information from Windows 2000 NTFS to NT4 NTFS, you must select “allow loss of additional file streams” to perform the transfer. Windows 2000 NTFS creates a sparse file stream associated with the file when summary information is added to the file. NT4 NTFS does not support sparse files. • Check network connectivity between machines hosting the replication agent and those hosting the VFM server or monitoring agent.

If...	Then do this...
VFM Server service or StorageX Replication Agent service fail to start.	• Check the Windows NT event log for errors related to startup failure • Check the Service Control Manager to see whether the VFM Server or StorageX Replication Agent was stopped or the startup of either was disabled. • Check whether the account used by the service was removed from the domain. • Check whether the password was changed on the account used by the service. • Validate that the account and password information used by the service is correct. • Check whether the account used by the service has “logon as service” privilege enabled. • Check whether the VFM Server or StorageX Replication Agent is installed on the system. **Note:** When you install VFM, you are prompted for account and password for the VFM Server. The server caches password information using Windows 2000 LSA (Local Security Authority) facilities. The server uses the account and the cached password when deploying replication agents. To manually update information for the VFM server and deployed replication agents, click **Agent Management** on the **Tools** menu.
Deployment of replication agent fails.	• Check whether the system being deployed to is up and reachable. This can be done by pinging it as well as using the net view command to view the shares that it publishes on the network. • Check whether there are domain trust issues preventing deployment. • Check whether there are network routing and infrastructure issues preventing network connectivity in both directions between the system hosting the server or monitoring agent and the system that hosts the replication agent. • Check whether the intended host of the Replication agent is being communicated over a VPN connection. ICMP packets typically do not travel over VPN connections. This restriction prevents the VFM server from correctly identifying the machine type of the intended host machine. It is also possible that the network administrator has restricted ICMP traffic on non-VPN connected machines. • Verify that the target system running one of the following platforms: Windows 2000, Windows Server 2003, or Windows XP. Agents cannot be pushed to other platforms. **Note:** If the machine on 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 on which you want to deploy the replication agent. 2. Restart the machine. • If the target system is running Windows NT 4 (versions of VFM 5.5 or earlier), check whether MSXML3 is installed on the system. You can do this by checking for the existence of `msxml3.dll` in the system32 directory. MSXML3 is available for download from the Microsoft web site.

If...	Then do this...
	• Check whether the normal `admin$` shares are published on the destination system. Try viewing the `admin$` share for the target system using Windows Explorer. • Check whether the account under which the VFM Server service is running has privileges to write to the destination `admin$` share to install the replication agent. You can do this by using the Windows "run as..." facility to run Windows Explorer and browse the `admin$` share on the server. • Verify that there is space on the destination system to receive the replication agent. The replication agent requires approximately 700 KB to be installed. • Verify that the account under which the VFM Server service is running has privileges to install and run as a service on the destination machine. • Check whether there are any firewalls between the system hosting the VFM Server or Tapestry StorageX monitoring agent services and the intended destination system for the replication agents that are blocking the port where the VFM Server service listens (TCP ports 6001 or 6005). • Check whether any process is already listening on the port the VFM Server and StorageX Replication Agent services use and thus preventing VFM from operating. • Check whether the Remote Registry Service (`regsvc.exe`) is started on the machine where the replication agent is to be deployed. Stopping this service interferes with the deployment and operation of the Replication Agent. • Check whether the system running on the machine where you want to deploy a replication agent was upgraded from Windows 2000 to Windows 2003. After an upgrade from Windows 2000 to Windows 2003, the "Local Service" account might not have the required permissions to access certain registry keys. See the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/555335/en-us • If the intended destination is a Microsoft Cluster Server Cluster, additional steps are required to configure the replication agent to run on the cluster. Contact support for this configuration information. • Check whether you are being denied remote access to the registry on the machine where you want to deploy a replication agent. Check the network access settings on the machine where you want to deploy a replication agent. `Administrative Tools>Local Security Policy>Security ettings>Local Policies>Security Options>Network access: Remotely accessible registry paths` and `Network access:Remotely accessible registry paths and sub-paths`. • Check whether "File and Print Sharing" is enabled on the system where you want to deploy the replication agent. If this option is not enabled, VFM cannot deploy the replication agent. • If you are running a version of VFM that is later than 5.5, you cannot deploy replication agents to Windows NT 4 systems. If you migrated data to NT 4 systems prior to version 5.7 of VFM and VFM deployed a replication agent to the NT 4 system, you do not have to do anything. In the future, when

If...	Then do this...
	transferring data to NT 4 systems, specify a proxy machine. • Check whether the replication agent can communicate with the machine hosting the VFM server using the NETBIOS host name. **Note:** See the note in "Problem selecting a monitoring agent" for a list of network ports used by DFS and VFM.
VFM cannot communicate with replication agents.	• Check whether there are any firewalls between the system hosting the VFM Server or Tapestry StorageX monitoring agent services and the intended destination system for the replication agents that are blocking the port where the StorageX Replication Agent service listens (TCP port 6002). • Check whether the console system or agent system is running a personal firewall, such as ZoneAlarm or BlackIce and whether the appropriate ports are open on it to allow communication. • Check whether any process is already listening on the port the VFM Server and StorageX Replication Agent services use, thus preventing VFM from operating. • Check that the system hosting the replication agent can ping the system hosting the VFM server using the server name. • Check whether the replication agent can communicate with the machine hosting the VFM server using the NETBIOS host name. **Note:** See the note in "Problem selecting a monitoring agent" for a list of network ports used by DFS and VFM.
VFM does not display full information about shares hosted on my filer.	Depending on the filer implementation, VFM might not support the detailed level of information provided by Windows systems. VFM displays as much information as can be obtained about storage targets.

If...	Then do this...
Invalid security descriptor messages reported during migration operations.	• Check whether the source, the destination, and the machine hosting the DFS root are all in the same domain. If not, check whether trusts are set up appropriately among the systems. • Check whether the domain admin account under which the VFM Server service was installed has administrator privileges on the source and destination of the replication. • Check whether the files for which the problem is reported are owned by a local account on the source machine. This can cause this error to be reported. • It is possible that the security descriptor on the file is invalid. When logged into the account used by the VFM Server service, check whether you can view the security settings on the file from Windows Explorer. • Check whether the owner and primary group of the source files are valid on the destination machine. If the owner or primary group of a file is not present on the destination machine, warnings about invalid security descriptors can result. This can be the case if files and directories on the source machine have a local account as their owner or a local group as their primary group. You can use VFM replication options to control how local SIDs are processed during the replication process. • If the destination of the transfer is a NetApp filer, check the filer's `/etc/messages` file for any error messages indicating problems communicating with its domain controller.
Replication or migration operations produce error 1332 "No mapping between account names and security IDs was done."	• The files are owned by an unknown SID. Use Windows Explorer or another tool to assign ownership of the problem file to a known trustee. • This condition can arise if the account owning the file is removed from the system.
A replication or migration job is canceled after 60 minutes.	Check whether you have an evaluation license for VFM. Evaluation licenses enable you to copy only 60 minutes of data.

If...	Then do this...
Replication or migration operations produce the following errors: • "Disk is full" • "The system cannot find the file specified"	Use the following checks to diagnose environmental problems: • Check whether space is available on the destination. • Check whether the quotas are not limiting the ability of the replication agent to write to the destination. This applies to NTFS quotas in Windows systems or qtree quotas in NetApp filers. • If the destination is hosted on a NetApp filer, check whether the `/etc/messages` file of the filer for any errors related to `MAXDIRSIZE`. It might be necessary to increase the value of this parameter on the filer if the destination will contain a very large number of files. • If the destination is hosted on a NetApp filer, check whether any files have UNC paths longer than the limit of 256 characters set by Data ONTAP. This condition can occur if CIFS clients access data via shares of deeply nested subfolders and replication is attempted from the root of a volume, causing a longer UNC path to be used in referencing the file on the filer. • If the destination is hosted on a NetApp filer, check whether the destination volume has sufficient nodes available to accommodate the files being transferred.
Replication and migration operations produce the following errors: • "Resource not found" • "Path not found" • "Source not found" • "Destination not found" • "Destination could not be created"	Use the following checks to diagnose network problems: • Check whether the source server is accessible from the machine hosting the replication agent. For example, you can ping, net use, or browse for the machine in Microsoft Network neighborhood. • Check whether the destination server is accessible from the machine hosting the replication agent. For example, you can ping, net use, or browse for the machine in Microsoft Network neighborhood. • Check that the source and destination shares exist and are accessible from the machine hosting the replication agent. For example, you can try accessing source or destination shares via Windows Explorer. • Check whether the VFM Server service account is not explicitly denied share permissions on destination shares. • Check whether the VFM Server service account is in Local Administrators group of the source or destination server.

If...	Then do this...
Replication and migration operations produce the following errors: • "Cannot delete source/destination. It is being used by another process" • "Cannot open source/destination. It is being used by another process"	Use the following checks to diagnose problems with locked files: • Check whether files or directories in question are being accessed by another application. Close all applications accessing the files or directories and retry data transfer. Files that are commonly locked include Outlook data files such as PSTs, database files used by Access, SQLServer, FoxPro, or Exchange. • Check whether nested data transfers are not in progress at the same time. The following example illustrates this problem: LinkA references \\source\shareA and LinkB references \\source\shareA\folderB. LinkA and LinkB are source links in two different replication policies. Starting replication policies at the same time may lead to above errors. • Check whether the destination of the transfer is a filer, verify that any virus scanning software was disabled, and retry the transfer. When enabled, virus scanning software can cause problems with locked files during large replications.

If...	Then do this...
Replication and migration operations produce the following errors: • "Unable to delete a file. Access is denied" • "Unable to delete source. Access is denied" • "Unable to delete destination. Access is denied" • "Access to a directory or file is denied" • "Access is denied" • "Access to source is denied" • "Access to destination is denied"	Permission problems can be diagnosed by checking whether the following conditions are true for your environment: • Check whether the VFM Server service account is in the Local Administrators group of the source server. • Check whether the VFM Server service account is in the Local Administrators group of the destination server. • Check whether the VFM Server service account is not explicitly denied share permissions on the source or destination share. • If the source or destination is a NetApp filer, use the command *testdc* to verify that the system can communicate with domain controllers. • Check the filer's `/etc/messages` file for errors related to communication with domain controllers.
There are warnings when you replicate or migrate data from Windows 2000 NTFS to NT4 NTFS.	The Windows 2000 version of NTFS supports a superset of the file information supported on NT4 NTFS. This means that not all the information associated with a file on a Windows 2000 NTFS file system can be transferred to an NT4 NTFS file system. VFM warns when this situation is encountered. This enables you to specify whether to carry out the operation.
VFM reports access-denied errors when attempting to transfer files to a filer and vscan is in use on the filer.	• Check whether the virus scanning software is operating correctly. It is possible to configure virus scanning software using the **vscan** interface to prevent any files from being written to the filer when the virus scanning software is inoperable. • Some conditions that can cause problems for virus scanning software include changes to the account under which the virus scanning software runs or network connectivity problems between the filer and the virus scanning host.

If...	Then do this...
Files and directories on the source and destination have different permission settings.	• Check inherited permissions on the source and destination directory trees. • Check whether the data transfer was interrupted before it was completed. VFM manipulates directory permissions on the destination during the migration process to ensure it has sufficient permissions to write to tightly ACL-ed destination directories. After VFM has completed its work in a directory tree, the permissions are set to the actual permission intended for the destination. If the transfer is interrupted, it is possible that extra permissions may be present on destination directories because VFM was prevented from completing the permission-setting phase of the transfer.. • Check whether local trustee processing is enabled for the policy. Perform the following steps: 1. Right-click the policy and click **Properties**. 2. Click **Replication Security**. **Note:** Local trustee processing is not applicable when the source of a transfer is a Domain Controller. Domain Controllers do not host local SIDs.
You see the error 1130 "Not enough server storage is available to process this command."	Check whether the IRPStackSize parameter is set too low on the system reporting the error. Microsoft KB article 177078 describes the default values for this parameter and explains how to increase it through the registry for versions of Windows, including Windows Server 2003. http://support.microsoft.com/default.aspx?scid=kb;en-us;177078

You have problems transferring data using the NFS protocol	• Check whether the machine where the UNIX replication agent is running can resolve the name of the NFS server you are trying to contact.
	  • Log in to the machine where the UNIX replication is installed and ping the NFS server.
	  • In a mixed Windows and UNIX environment, always use the fully qualified DNS name.
	• Log in to the NFS server and run "exportfs" with no arguments. Check whether the path you are trying to contact or one of its parent directories appears with the rights you expect.
	• Check the `exports` file on the NFS server you are trying to contact. This file is found in the following locations:
	  • **Linux** - `/etc/exports`
	  • **Solaris** - `/etc/dfs/dfstab`
	  • **NetApp** - `<`*`the name of the root volume`*`>/etc/exports` OR `/etc/exports`

If...	Then do this...

	• Check whether the path you are trying to contact or one of its parent directories is in the `exports` file. If the path exists, check whether the rights granted are correct. To clarify the instructions that follow, VFMmachine is used to represent the machine communicating with the UNIX server. The machine can be the VFM server or UNIX replication agent. The entry for the machine is its IP address or fully qualified DNS name.
	  • **Linux** - Search for an entry that contains *(rw) or VFMmachine(rw).
	  Note: Within the parentheses, there can be other rights, however, it is very important that "rw" (read/write) access is granted.
	  • **Solaris and NetApp** - Entries are separated by commas. Search for the entry "rw", "rw=VFMmachine", or "root=VFMmachine."
	  Note: Make sure that "ro" or "ro=VFMmachine" are not specified. The VFM machines might appear in a colon-separated list with other machines.
	• Normally, VFM uses root (uid 0). You can specify a different uid for a UNIX machine or filer. When the uid is not root, the replication agent might not be able to copy some security information and therefore reports data transfer failures. To suppress these error reports, perform the following actions:
	  1. Right-click the policy that contains the UNIX machine or filer and click **Properties**.
	  2. Click **Security Replication**.
	  3. Select **Allow loss of security information**.
	  4. Click **OK**.
	• When an export is used as root (uid 0), special entries are required in the exports file.
	  • **Linux** - The VFM machine entry <u>must</u> include "no_root_squash" or "anonuid=0" (for example, "rw,no_root_squash"). Make sure that "root_squash" is <u>not</u> specified.
	  • **Solaris and NetApp** - When the VFM machine is not given explicit "root" access, the entry "anon=0" must be included in the exports file.
	  Note: After changing the exports file, run the following commands:
	  `exportfs -ua`
	  `exportfs -a`
	  To check what the NFS machine is exporting, execute the command **exportfs**.
	• Check the UNIX security mode-bit rights on the NFS machine and compare them with the rights of the files you are trying to access.
	• Check whether the replication agent can communicate with the machine hosting the VFM server using the NETBIOS host name.

<table>
<tr><th>If...</th><th>Then do this...</th></tr>
<tr><td></td><td>

For NetApp filers, check whether the volume/qtree is set to use UNIX security. If the security mode is NTFS, VFM cannot perform attribute settings on the filer volume or qtree. Perform the following actions:

The UNIX user must be mapped to an NTFS user in the file <code>/etc/usermap.cfg</code>.
Select "Allow loss of security information" in the properties of the policy. This suppresses error messages reported by the UNIX replication agent.

</td></tr>
<tr><td>Links are not updated after a migration</td><td>
Make sure that the UNC paths of the source and the link targets you want to update match. If the UNC paths do not match, VFM cannot update the namespace.

This example illustrates what happens when the UNC path of a migration source and link targets that match the search criteria do not match:

You create a migration task and specify a source and destination.

<table>
<tr><th>Source</th><th>Destination</th></tr>
<tr><td><code>\\Saturn.npb.com\c$\Sales\Reports</code></td><td><code>\\Pluto.npb.com\Sales</code></td></tr>
</table>

You scan for migration candidates and find one candidate.

<table>
<tr><th>Migration candidate</th></tr>
<tr><td><code>\\Saturn.npb.com\c$\Sales\Reports\HoustonRegion</code></td></tr>
</table>

The namespace contains a link named Sales that targets the migration candidate. Notice the difference in the UNC paths between the migration candidate and the link target.

<table>
<tr><th>Namespace link</th><th>Target of link</th></tr>
<tr><td>Sales</td><td>\\Saturn.npb.com\Sales\Reports\HoustonRegion</td></tr>
</table>

You run the policy to start the migration. VFM successfully migrates the data to the destination but does not update the link target because the UNC paths of the migration candidate and the link target do not match.

<table>
<tr><th>Destination after migration</th></tr>
<tr><td><code>\\\Pluto.npb.com\Sales\HoustonRegion</code></td></tr>
</table>
<table>
<tr><th>Namespace link</th><th>Target of the link after migration is not updated to target the destination</th></tr>
<tr><td>Sales</td><td><code>\\Saturn.npb.com\Sales\Reports\HoustonRegion</code></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>If...</th><th>Then do this...</th></tr>
<tr><td></td><td>

After migration, the target for the link Sales does not contain any data because the data was migrated to the destination.
To avoid this problem, the source path should match the link target path.

<table>
<tr><th>Correct source path</th></tr>
<tr><td>\\Saturn.npb.com\Sales\Reports</td></tr>
</table>
<table>
<tr><th>Migration candidate</th></tr>
<tr><td>\\Saturn.npb.com\Sales\Reports\HoustonRegion</td></tr>
</table>
<table>
<tr><th>Namespace link</th><th>After migration, the target of the link is updated to target the destination</th></tr>
<tr><td>Sales</td><td>\\Pluto.npb.com\Sales\HoustonRegion</td></tr>
</table>
</td></tr>
<tr><td>The Event Details dialog box shows that more data was copied than what you expected</td><td>The Event Details dialog box does not accurately show bytes transferred when only the security descriptor is copied to the destination. This occurs when you select the security replication option to "Always copy security settings."</td></tr>
<tr><td>You cannot uninstall a replication agent using the VFM Agent Management tool.</td><td>Check whether the option "Allow replication agent to be deployed to this host" is selected in the properties of the machine hosting the replication agent.

In the Physical View, right-click the machine and click Properties.
Click the Agent tab.
Make sure that "Allow replication agent to be deployed to this host" is selected.
Click OK.
Go back to Agent Management and uninstall the replication agent.
</td></tr>
</table>

NetApp filer problems

If...	Then do this...
NetApp filers are identified as generic machines.	Check network connectivity between the VFM console machine and filer. VFM provides a batch file to which you can pass arguments to check the filer. The **FilerCheck.bat** file is in the **Tools\FilerCheck** directory in the VFM server installation directory. At a command prompt type **Filercheck** *<filer> <username:password> <community name>*, where "filer" is the name or IP address of the filer, "username:password" is the username and password used to access the filer through RSH, and "community name" is the SNMP community name used to access the filer through SNMP. **Filercheck** performs the following checks: • Checks whether the current account has administrator privileges on the filer or vFiler™. The lack of these privileges prevents accurate identification. • Checks whether the current account can access `\\filer\IPC$` through a “net use” command. If *IPC$* cannot be accessed, VFM cannot complete the filer identification process. • If you have access to an account with administrator privileges on the filer, you can explicitly map a drive on your VFM console machine to the `\\filer\c$` share using that account to administer the filer through VFM.

If...	Then do this...
NetApp filers are identified as vFilers rather than as filers.	Check that SNMP is enabled on the filer and that the community string used by VFM to communicate with the filer is correct. VFM uses “public” as the default community string. You can override this through the **Tools**>**Options** dialog box, as well as on a per-machine basis through the machine properties dialog box for each specific machine. VFM provides a batch file to which you can pass arguments to check the filer. The **FilerCheck.bat** file is in the **Tools\FilerCheck** directory in the VFM server installation directory. At a command prompt, type **Filercheck** *<filer> <username:password> <community name>*, where "filer" is the name or IP address of the filer, "username:password" is the username and password used to access the filer through RSH, and "community name" is the SNMP community name used to access the filer through SNMP.
FilerView does not appear as expected in the Manage tab.	Check whether you can browse to `http://filer/na_admin` using Internet Explorer on the VFM machine to get to the FilerView Web user interface.
Attempting a filer management operation, such as creating or initializing a SnapMirror® function or showing a filer in the Admin View, causes the following errors: • "Device command didn't report an output" • "SnapMirror is too busy, please try again later"	• The NetApp filers are under an extremely heavy load. Retry the operation when the load on the filers has decreased. • Check whether the `/etc/snapmirror.conf` file is 0 bytes. If `snapmirror.conf` does not contain the normal comment showing when the file was generated by Data ONTAP software, add a placeholder comment or delete the file. • Check the file `/etc/messages` on the filer for SnapMirror-related error messages or RSH-related error messages. **Note:** VFM does not support automatic creation of SnapMirrors on separate network interfaces other than the primary interface used by VFM to communicate with the filers.

If...	Then do this...
Refreshing filer information or filer event information results in "access denied" errors.	VFM provides a batch file to which you can pass arguments to check the filer. The **FilerCheck.bat** file is in the **Tools\FilerCheck** directory in the VFM server installation directory. At a command prompt type: **Filercheck** *<filer> <username:password> <community name>* where "filer" is the name or IP address of the filer, "username:password" is the user name and password used to access the filer through RSH, and "community name" is the SNMP community name used to access the filer through SNMP. Filercheck performs the following checks: • Checks whether the current account has administrator access to the `c$` share on the filer. To manually check access, try to browse the `c$` share using Windows Explorer (for example, `\\<filename>\c$`). • Checks whether the current account has administrator privileges on the filer or vFiler. Lack of these privileges results in "access denied" errors. • If RSH reports: "*<filername>*: Permission denied. RSH: cannot establish connection," the filer is configured with the administrator name and possibly the administrator password. • If RSH reports something like: "NetApp Release 6.3: Wed Aug 7 23 : 04 : 57 PDT 2002," the RSH command succeeded against the filer. If the filer is configured with a user name and password, you must enter the user name and password on the Filer Account tab of the machine's properties in VFM. If the RSH check is indeterminate, you can use telnet to check whether the filer is prompting for a user name and password. From a command prompt on the VFM client machine, telnet to the filer and check whether the filer prompts for a user name and password.

If...	Then do this...
SnapMirrors do not appear in the properties of a NetApp filer.	Check whether the SnapMirrors were created using a command-line prompt. • When a SnapMirror is created using FilerView, the SnapMirror configuration is added into a file named `snapmirror.conf.` • When FilerView receives the command to display SnapMirrors on a filer, the product reads the information in the `snapmirror.conf` file. • When a SnapMirror is created using a command-line prompt, the configuration of the SnapMirror is not added to the `snapmirror.conf` file.

Browse namespace problems

If...	Then do this...
Attempts to browse or manage the DFS namespace yield “RPC server not available” error messages.	Check whether the DFS service is running on the machine hosting the DFS root.
Attempts to browse the namespace yield “access denied” errors.	Check whether the current account has privileges to access the share hosting the DFS root, as well as to the root itself in the case of domain roots. If access denied errors are reported when attempting to browse folders in the namespace, check the permissions of the shares hosting these folders as well as the permissions on the folders themselves. When accessing resources through the namespace, the credentials used for the access are those used when the user initially accesses the namespace. This can cause problems in environments where users typically use explicit credentials to map network drives.

Windows powered NAS or Windows storage server filer identification problems

If...	Then do this...
Windows Powered NAS or Windows Storage Server filers are being identified as generic machines.	Check whether the current account has administrator privileges on the Windows Powered NAS or Windows Storage Server machine by using `RegEdit.exe` to connect to the filer's registry. Inability to open the filer's registry prevents VFM from accurately identifying the filer as a Windows Powered NAS or Windows Storage Server filer.

Problems running batch files

If...	Then do this...
Problems are encountered trying to run batch files configured to run with VFM storage policies.	• See "Running batch files" for information about running batch files in VFM. • See "Batch files" for detailed information about the example scripts provided by VFM. • Save your BAT file log to a text file. You can examine the contents of the text file to diagnose potential problems. Adding a line such as `“echo %date% %time% The arguments passed from server are: %*  >> Decision.txt”` will record all the arguments passed to your BAT file along with the date and time that the script ran. This information is appended to the file “`Decision.txt`” located in the directory where the BAT file is running.
You get the following error when you know that you correctly typed the path of the batch file: "Script was not found"	Check whether the script path contains spaces. If the path contains spaces, you must enclose the path in double quotes. If you browse for the script, VFM encloses the path in double quotes for you.

If...	Then do this...
You specify a script, run the policy, and the script does not run.	Check whether the script path is valid. VFM *does not validate the path* to the script you specify. It is your responsibility to ensure that the path is accurate and accessible to the VFM server or monitoring agent that invoke the script.

Problems running a policy

If...	Then do this...
You see the following error messages: • The namespace backup policy failed. • Manually running the namespace backup policy failed.	• Check whether the account running VFM has appropriate permissions for the DFS root being manipulated. • Check whether VFM can communicate with the DFS root. Check network connectivity by pinging the server where the root is located from the VFM machine. • Check whether there is a problem communicating with the VFM database.
You see the following error messages: • The server disaster recovery policy was unable to retrieve the active link information • The server disaster recovery policy failed to activate the primary server target for the link • The server disaster recovery policy failed to activate the secondary server target for the link	• Check whether VFM can communicate with the servers that contain the link targets. • Check whether the account running VFM has appropriate permissions for the DFS root being manipulated. • Check whether VFM can communicate with the DFS root. Check network connectivity by pinging the server where the root is located from the VFM machine.

If...	Then do this...
You see the following error messages: • The policy scan for the storage load balancing policy encountered problems • Failed updating DFS links for a task in the storage load balancing policy	• Check whether the account running VFM has appropriate permissions for the DFS root being manipulated. • Check whether VFM can communicate with the DFS root. Check network connectivity by pinging the server where the root is located from the VFM machine. • Check whether VFM can communicate with the storage resources. • Check whether the account running VFM has appropriate permissions to access the storage resources.

Snapshot access policy problems

If...	Then do this...
The restore operation is not working.	Check whether the volume hosting the files has the *.snapshot* directory visible. VFM cannot restore data hosted on a volume where the *.snapshot* directory is not visible.
You cannot view files on the Explorer tab of a snapshot access policy.	• The *.snapshot* directory on the volume hosting the data might not be visible. Make sure that the operating system is configured to show hidden files. • To access snapshots from CIFS clients, type the following command on a command prompt: `\\<filename>\<share>\.snapshot` Where "filename" is the name of the filer you are using and "share" is the name of the share you want to access.
You encounter "network resource not found" errors when attempting to use the SnapRestore™ function to retrieve items from the Snapshot Access Namespace Explorer view.	Check to see whether there is a mismatch between the exact local path on disk of the shared directory and the local path entered when creating the path. These two items must match exactly, including upper/lower case of the path components, for SnapRestore to work. You can correct this by removing and re-creating the share using the exact name of the local path and re-creating your Snapshot access policy.

Problems printing to PDF files

If...	Then do this...
You cannot print from VFM to PDF files.	Check whether VFM was upgraded using terminal services. You need to upgrade from the machine console and not through terminal services.

Name of machine is incorrect

If...	Then do this...
The name of a machine in the Physical View is incorrect.	Check whether DNS forward and reverse lookups are configured correctly for the machine.

Problems taking snapshots of the application

If...	Then do this...
You see "access denied" errors while trying to take a snapshot of the application.	Check the permissions on the snapshot save location (both share and local directory) to ensure that both the account under which MSDE and the account under which the VFM server are running have permission to write to the snapshot save location.
The application snapshot fails to complete	• Check whether the MSDE database runs with the LOCALSYSTEM account. Application snapshots cannot be written to UNC path hosted on a different machine. • Use the Service Control Manager to change the logon account for the appropriate MSDE services to an account with privileges to write to a network share. • It is not recommended that MSDE run as the same account as the VFM server because the account used by the VFM server has administrator privileges. If MSDE is attacked by programs such as Slammer, the damage might be lessened if MSDE is running as a minimally privileged account.

Permission based namespace policy problems

If...	Then do this...
Links were not created when you ran the policy.	• Check whether you tried to add multiple links with the same name. If you selected domains to search for resources and the domains contain groups with the same name (for example, `domain1\sales` and `domain2\sales`), make sure that you select a template that sorts by domain, such as Domain-Group Name-Machine-Shares, Machines-Domain-Group Name-Shares, or Domain-Group Name-Shares. You cannot create links with the same name under the root or a logical folder of the namespace. • Check whether the NTFS permissions for a folder hosting a share to which you want the policy to create link contain `<hostname>\users`. Remove the `<hostname>\users` group from the NTFS permissions on the folder and run the policy. • Check whether the resources you wanted to add to the namespace have the local users group in their permissions. Remove the local user group from the permissions for each folder and run the scan again.

Problem installing a UNIX replication agent

If...	Then do this...

You get the following error message while trying to install a UNIX replication agent:
• On Solaris:
`pkgadd: ERROR: Unable to make directory </usr/local/URA>`
• On Linux:
`error: unpacking of archive failed on file /usr/local/ura/bin:`
`cpio: mkdir failed - No such file or directory`
	Check whether the file system where you are installing the replication agent is mounted read-write. The file system where a replication agent is installed must be mounted read-write.

Problems using NTFS Change Journal

If...	Then do this...
You see one of the following error messages: • "Change Journal could not be used because this is the first time the job ran." • "Change Journal could not be used because it is not active and auto-enabling is not permitted." • "Change Journal could not be used due to an unexpected failure."	• The NTFS Change Journal is supported on Windows 2000 NTFS which is available on Windows version 2000 and later of the Windows operating system. • When you enable the NTFS Change Journal on a volume, the size of the volume is used to determine the amount of space dedicated to the change journal. For each 50 GB of space on the volume, 128 MB is assigned for use by the change journal up to a maximum of 10 GB. On Windows 2000 SP2 or below, the amount of space dedicated to the change journal is always 128 MB, regardless of the size of the volume. • Use of this option requires that VFM deploy a replication agent on the machine where the source data resides and enable the change journal on the NTFS volume hosting the source data. The VFM machine properties dialog enables you to control whether the replication agent can be deployed to a machine and whether VFM can enable the NTFS change journal for volumes on the machine. • Use of this option means that changes made on the source are replicated to the destination and changes made on the destination are not overwritten by data from the source unless the corresponding file on the source changes as well. This differs from standard VFM replication, wherein changes made on the destination are detected and overwritten with data from the source. • In cases where the change journal wraps, VFM must perform a full scan of the source and destination to determine what files need to be transferred. • When both Delete orphaned files in destination folders and Use NTFS Change Journal are selected, VFM deletes a destination file when its corresponding source file is deleted. If a new file is added to the destination, the file is not deleted unless the file is contained in a directory that is deleted on the source.

Problem configuring the OpenSSh package on Solaris

If...	Then do this...
You see the error message "Privilege Separation user sshd does not exist"	Edit the `/etc/passwd` file and add the following line at the bottom of the file: `sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin` **Note:** The command should not have line breaks. It should be written in one line.

Problem accessing a UNIX machine when using SSH

If...	Then do this...
You are prompted for a password when you access a UNIX machine when VFM is configured to use SSH	• If you generated a SSH2 (RSA) or SSH2 (DSA) key, check whether you created the file "authorized_keys2." See Step 3 in "Copy the public key to a UNIX machine." • Check whether you generated the keys without a password or passphrase. See Step 5 in "Generate a key-pair." • Check whether OpenSSH is installed on the UNIX machine. See "Install and configure OpenSSH on Solaris" or "Install and configure OpenSSH on RedHat" for detailed instructions about how to install OpenSSH. • Make sure that you have the appropriate permissions. See Step 6 in "Copy the public key to a UNIX machine." • Check whether the private keys were added into the memory of the VFM client and server machines. To check whether the private keys were added to the pageant key list, perform the following actions: 1. Right-click the pageant icon on the system tray and click **View Keys**. 2. If the private key is not listed, click **Add key** or follow the instructions in "Add private keys to pageant."

Problem importing snapshots of the application

If...	Then do this...

You see the following error message when you try to import a snapshot of the application:
`ERROR: Cannot execute command: "C:\Program Files\NetApp\VFM\Server.exe""-restore:\\jsmith\myshare\mydatabase"`
`ERROR:  desc: Run status: -1`
	Check whether the SQL service is running on the Local Network Account. When the SQL service is running on the Local Network Account on the backup machine, perform one of the following tasks:
	• Save the exported snapshot on the local drive of the backup machine before you import it to VFM.
	• Make sure that the SQL service is running under an account that has full privileges across all domains.

Problems replicating data using VSS snapshots

If...	Then do this...
Time-out errors occur in volume shadow copy service writers, and shadow copies are lost during backup of high input/output activity	Apply a hot fix update to the Volume Shadow Copy service (VSS) for Microsoft Windows Server 2003 which is available at the following Web site: http://support.microsoft.com/kb/833167#8 The update addresses this and other known VSS problems.

Problems deleting items from the Logical View

If...	Then do this...
• You cannot delete a root, link, or link target from the Logical View. • You get the following error message when you try to delete a link from the Logical View: "Unable to delete link because the link is being reference by another object" • You get the following error message when you try to delete the target of a link: "Deleting the last replica for a DFS link will cause the link to be deleted. This link is being referenced by another object and may not be deleted."	The item that you want to delete is a member of a policy. Before you can delete the item, you must remove it from the policy or policies that reference the item.

Problem updating home directories

If...	Then do this...
You run a user data management policy after you manually delete a link managed by the policy. In the Alerts tab, you see the following error message: “Namespace link was not found. This error will prevent you from applying the namespace options.”	The links that a user data management policy creates in the namespace should always be managed by the policy. If you manually delete a link that was created by a user data management policy, the policy cannot manage the home directory the link targeted because the location of the directory is no longer available. **Links targeting home directories contained in Windows systems** • If you deleted a link targeting the home directory of an **active user**, manually update the user's Active Directory Home Folder property. Type the correct physical UNC path and run the policy again. • If you deleted a link targeting the home directory of a **disabled user** and the user data management policy was configured to migrate or retarget links of disabled users, update the user's Active Directory Home Folder property. Type the correct physical UNC path and run the policy again.

If...	Then do this...
	• If you deleted a link targeting the home directory of a **deleted user** and the user data management policy was configured to migrate or retarget the links of deleted users, you must create a VFM migration policy to migrate the data. • If you deleted a link targeting the home directory of an **unmanaged user** and the user data management policy was configured to update the user's Home Folder property in Active Directory, you must manually update the Home Folder property with the physical UNC path to the user's data. **Links targeting home directories contained in NetApp filers in which the `/etc/cifs_homedir.cfg` file is configured** If you deleted a link targeting the home directory of any user, the user data management policy creates the link again the next time the policy runs.

Appendix A Migration, replication, and status indicators

Migration task indicators

The following list specifies status indicators that are used as visual cues.

Source Share	Description
	The task is scheduled to be processed.
	User action is required.
	A task was completed successfully or was canceled.

Replication status monitoring indicators

The following list specifies status indicators that are used as visual cues.

Replication policy	Description	Example
	Replication is in progress or completed.	
	Warning • A link in the policy is in an abnormal state. • A target in the policy is in an abnormal state.	• Replicas could be offline. • Access permissions prevent VFM from completing some aspects of a link. • A target might be unreachable due to network or machine problems. • Access permissions on a target might prevent VFM from accurately assessing the state of the target.
	Error - VFM detected a serious problem.	• The policy has no source link or no destination link. • The last synchronization attempt failed. • The source link has more than one target.
	Unknown - VFM cannot determine the state information for one or more items in the policy.	

Replication status monitoring indicators

Target	Description	Example
●	**In progress** - Data is currently being moved to the target.	
✓	**Completed** - Data move to the target was completed successfully.	• All files were copied. • No files needed to be copied.
⚠	**Warning** - Data move to the target encountered some failures.	• Some files failed to be copied. • No files were copied, but some failed to copy due to sharing violations. • All files were copied, but some files had warnings.
⊗	**Error** - The target is in an abnormal state.	• The target might be unreachable due to network or machine problems. • Access permissions on the target might prevent VFM from accurately assessing the state of the target. • There were problems with a DFS root. • No files were copied for reasons other than sharing violation.
?	**Unknown** - VFM cannot determine the state information for the target.	

Status indicators

The list below specifies status indicators that are used as visual cues for the following items:

- DFS root
- DFS link
- Shared folder
- Export
- Logical folder
- Machine
- Volume
- Qtree
- Export
- VFM server and monitoring agent

DFS root	Description	Example
Note: Single and replicated DFS roots have the same status symbols.	Online	
	Warning - VFM detected that one or more elements being monitored are not operating correctly.	• A DFS link has some replica shares that are unavailable. • Access permissions prevent VFM from monitoring the status of some portion of the root. • FRS is enabled for some, but not all of the replicas for this domain-based root.
	Error - VFM detected a serious problem.	• The internal data structure of the DFS root is corrupted. • All the replicas for a link are offline. • The DFS root is offline or does not respond to queries.
	Unknown - VFM cannot determine the state information for one or more DFS elements.	

Status indicators

DFS Link	Description	Example
Note: Single and replicated DFS links have the same status symbols.	Online	
	Warning - VFM detected that one or more shared folder replicas being monitored are not operating correctly.	• A DFS link has some replica shares that are unavailable. • Access permissions prevent VFM from monitoring the status of some portion of the link. • FRS is enabled for some, but not all of the replicas for this link in a domain-based root. • A single-target link is a member of a disaster recovery policy.
	Error - VFM detected a serious problem.	All the replicas for a link are unavailable.
	Unknown - VFM cannot determine the state information for one or more replicas.	

Shared folder	Description	Example
	Online	
	Warning - VFM detected that the shared folder being monitored is not operating correctly.	• The shared folder is unavailable. • Access permissions prevent VFM from monitoring the status of the shared folder.
	Error - VFM detected a serious problem.	The shared folder is offline.
	Unknown - VFM cannot determine the state information of the shared folder.	

Logical folder	Description	Example
	Online	
	Warning - VFM detected that the folder being monitored is not operating correctly.	• The shared folder is unavailable. • Access permissions prevent VFM from monitoring the status of the shared folder.
	Error - VFM detected a serious problem.	The shared folder is offline.
	Unknown - VFM cannot determine the state information of the folder.	

Machine	Description	Example
Note: All the machines have the same status symbols.	Information about the machine was updated without errors or **Unknown** - The machine was not refreshed.	
	Refreshing - Information about the machine is being updated.	
	Error - VFM detected a problem.	• There is a problem refreshing the server information (for example, comment, IP address or platform) • There is a problem refreshing the NetApp filer information (for example, volume or SnapMirror) • There is a problem refreshing the NetApp filer events.

Volume	Description	Example
	Information was updated without errors or **Unknown** - The volume was not refreshed.	
	Refreshing - Information about the volume is being updated.	

Qtree	Description	Example
	Information about the qtree was updated without errors or **Unknown** - The volume was not refreshed.	
	Refreshing - Information about the qtree is being updated.	

Export	Description	Example
	Online	
	Warning - VFM detected that the export being monitored is not operating correctly.	• The export is unavailable. • Access permissions prevent VFM from monitoring the status of the export.
	Error - VFM detected a serious problem.	The export is offline.
	Unknown - VFM cannot determine the state information of the export.	

VFM server and monitoring agent	Description	Example
	No problems were detected	
	Warning - VFM server is in an unknown state.	
	Error - VFM detected a problem.	• The database data file is full. • The database log file is full.

Appendix B Exclusion/Inclusion Examples

Exclusion examples

When creating exclusion lists, remember the following points:

- Exclusion terms are processed before inclusion terms. Files or directories matching an exclusion term are not processed further and cannot be included by a subsequent inclusion term.
- Directory exclusions are search expressions comprised of folder names and/or folder paths that can be used to exclude any folders matching the specified exclusion criteria.
- File exclusions are search expressions comprised of file names or extensions that can be used to exclude files matching the specified exclusion criteria.
- DOS wildcards can be used alone or in concert with a character string to exclude file or folders of similar name or type.
    - To match a string of characters of any length including an empty string, type an asterisk (*). For example, "s*d" finds "sad", "suddenly", and "Saturday,"
    - A question mark (?) can be used to match any single character in the search text. For example, "s?t" finds "set" and "sit", but not "Saturday."
- To exclude a subfolder and its contents, the trailing backward slash or forward slash is optional (The subfolder and its contents are excluded whether or not the trailing backward slash or forward slash is present).
- When you enable “delete orphans” as a replication option, the exclusion list affects how VFM handles orphan files on the destination. Orphan files on the destination that match the exclusion term are not deleted, while orphan files not matching the exclusion term are deleted.
- You must delimit multiple directory or file exclusion parameters with double quotes or you can click **Expand** to specify multiple files, file types, or directories.
- When the "Include subfolders" replication option is enabled and you specify file exclusions, VFM traverses subfolders for files to exclude from the destination. Subfolders are always transferred to the destination even when they are empty.

The following table provides examples of valid file and folder exclusion formats and descriptions for each format.

Exclusion examples

Item	Format	Applies to	Description
1	*	Files or Directories	When this example is used specifically as a directory exclusion parameter, all files and folders will be excluded. When used specifically as a file exclusion parameter, folders are still included, but all files contained in those folders will be excluded.
2	*.*	Files	All files contained within the specified parent and their associated child folders are excluded.
3	\ (Windows) / (UNIX)	Directories	When the slash is used as a directory exclusion parameter, all files and folders contained within the specified parent and child folders are excluded.
4	* (Windows) /* (UNIX)	Files or Directories	When used as a directory exclusion parameter, this example will exclude all files and all folders. When used as a file exclusion parameter, this example will result in the exclusion of all files.
5	*.* (Windows) /*.* (UNIX)	Files	When used as a file exclusion parameter, this string excludes all files contained in the parent.
6	*.tmp	Files	This example can be used to exclude files that contain the literal character string ".tmp."
7	listing	Files or Directories	Exclude files or directories named "listing."
8	listing.txt	Files	Exclude files named "listing.txt."
9	listing???.txt	Files	This example can be used to exclude files that begin with the string “listing” followed by any three characters that contain the literal character string "txt."

Item	Format	Applies to	Description
10	listing*.txt	Files	Used to exclude all text files with names that begin with the literal character string "listing."
11	\listing (Windows) /listing (UNIX)	Directories	When prefaced with the \ character, this example will traverse the directory tree and exclude folders named "listing."
12	listing\ or \listing\ (Windows) listing/ or /listing/ (UNIX)	Directories	This example will traverse the directory tree and exclude folders that are subfolders of the “listing” directory.
13	*\listing (Windows) */listing (UNIX)	Directories	Exclude subfolders named "listing."
14	*\listing\file.txt (Windows) */listing/file.txt (UNIX)	Files	This example can be used to exclude files named “file.txt” located in folders named “listing.”

Inclusion examples

When creating inclusion lists, remember the following points:

- Exclusion terms are processed before inclusion terms. Files or directories matching an exclusion term are not processed further and cannot be included by a subsequent inclusion term.
- Directory inclusions are search expressions comprised of folder names or folder paths that can be used to include any folders matching the specified inclusion criteria.
- File inclusions are search expressions comprised of file names or extensions that can be used to include files matching the specified inclusion criteria.
- DOS wildcards can be used alone or in concert with a character string to include file or folders of similar name or type.
    - To match a string of characters of any length including an empty string, type an asterisk (*). For example, "s*d" finds "sad", "suddenly", and "Saturday,"
    - A question mark (?) can be used to match any single character in the search text. For example, "s?t" finds "set" and "sit", but not "Saturday."
- To include a subfolder and its contents, specify a backward slash “\” (Windows) or a forward slash "/" (UNIX) after the directory name.
- To include just a subfolder and not its contents, omit the trailing backward slash or forward slash.
- When you enable “delete orphans” as a replication option, the inclusion list affects how VFM handles orphan files on the destination. Orphan files on the destination that match the inclusion term are deleted.
- You must delimit multiple directory or file inclusion parameters with double quotes or you can click **Expand** to specify multiple files, file types, or directories.
- When the "Include subfolders" replication option is enabled and you specify file inclusions, VFM traverses subfolders for files to include in the destination. Subfolders are always transferred to the destination even when they are empty.

The following table provides examples of valid inclusion formats and descriptions for each format.

Item	Format	Applies to	Description
1	*	Files or Directories	When this example is used specifically as a directory inclusion parameter, only folders (no files) of the specified parent will be included. When it is used as a file inclusion parameter, all files and all folders will be included.
2	*.*	Files	All files contained within the specified parent and their associated child folders will be included.
3	\ (Windows) / (UNIX)	Directories	When used as a directory inclusion parameter, all folders contained within the specified parent are included.
4	* (Windows) /* (UNIX)	Files or Directories	When used as a directory inclusion parameter, this example will include all folders. When used as a file inclusion parameter, this example will include all files and related folders.
5	*.* (Windows) /*.* (UNIX)	Files	When used as a file inclusion parameter, this string includes all files contained in the parent.
6	*.tmp	Files	This example can be used to include files that contain the literal character string ".tmp."
7	listing	Files or Directories	Include Files or Directories named "listing."
8	listing.txt	Files	Match files or directories named "listing.txt."
9	listing???.txt	Files	This example can be used to include all text files with names that begin with the string “listing” followed by any three characters.

Inclusion examples

Item	Format	Applies to	Description
10	listing*.txt	Files	Used to include all text files with names that begin with the literal character string “listing.”
11	\listing (Windows) /listing (UNIX)	Directories	When prefaced with the \ character, this example will traverse the directory tree and include folders named “listing.”
12	listing\ or \listing\ (Windows) listing/ or /listing/ (UNIX)	Directories	This example will traverse the directory tree and include folders that are sub directories of the “listing” directory.
13	*\listing (Windows) */listing (UNIX)	Directories	Include subfolders named “listing.”
14	*\listing\file.txt (Windows) */listing/file.txt (UNIX)	Files	This example can be used to include files named “file.txt” located in a subfolder named “listing.”

Appendix C VFM Documentation

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
6.	*Manage Snapshots on Filers*	VFMSnapshots.pdf	Explains how to use VFM to manage snapshots on NetApp filers

No.	Title	File name	Contents
			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 block any further updates.

R

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

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

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

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

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

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

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

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

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

S

Secondary target: SEE Standby target.

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

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

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

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

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

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

T

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

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

U

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

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

W

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

Index

D

Data migration 41
DFS link
  check status 43
DFS root
  check status 43

M

Machines
  status 43
Migration policy
  task status indicators 41
Monitor status.....43
Monitoring status of link targets.....41

N

NTFS Change Journal 34

O

OpenSSH.....35

Q

qtree
  status 43
qtree.....43

R

Replication.....41

S

SSH.....36
Status indicators 41, 43
Status monitoring 41, 43
System status 43

T

Troubleshooting
  browse namespace problems 28
  DFS root problems 6
  general problems 3
  migration problems 13
  name of machine is incorrect..... 32
  NetApp filer problems..... 25
  permission based namespace policy problems 33
  problem accessing a UNIX machine when using SSH 36
  problem configuring OpenSSh..... 35
  problem installing a UNIX replication agent33
  problem taking snapshots of application 32
  problems connecting to the application service 11
  problems printing PDF files 32
  problems running a policy..... 30
  problems running batch files 29
  problems selecting a monitoring agent..... 12
  problems using NTFS change journal 34
  replication problems..... 13
  Report problems 9
  snapshot access policy problems..... 31
  Target problems 10
  Windows 2000 incompatibility problems ... 10
  Windows powered NAS ID problems..... 29
  Windows storage server filer ID problems.. 29
  Windows XP incompatibility problems 10
Troubleshooting..... 3

V

Volumes
  status..... 43