

VFM® (Virtual File Manager™) 6.0.2

Release Notes

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 215-03607_A0
January 2008

Copyright and trademark information

Copyright information

Copyright © 1994–2008 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this file 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 owner.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETWORK APPLIANCE “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NETWORK APPLIANCE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the government is subject to restrictions 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

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, DataFabric, Data ONTAP, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, SyncMirror, Topio, VFM, and WAFL are registered trademarks of Network Appliance, Inc. in the U.S.A. and/or other countries. Cryptainer, Cryptoshred, Datafort, and Decru are registered trademarks, and Lifetime Key Management and OpenKey are trademarks, of Decru, a Network Appliance, Inc. company, in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of Network Appliance, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexShare, FPolicy, HyperSAN, InfoFabric, LockVault, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simplicore, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapFilter, SnapMigrator, SnapSuite, SohoFiler, SpinMirror, SpinRestore, SpinShot, SpinStor,

StoreVault, vFiler, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the U.S.A.

IBM, the IBM logo, AIX, and System Storage are trademarks and/or registered trademarks of International Business Machines Corporation.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Contents of the VFM 6.0.2 Release Notes

Topics covered

These release notes contain information about the following release, installation, and upgrade topics:

- ◆ [“VFM 6.0 New Features”](#) on page 2
- ◆ [“Installation Requirements”](#) on page 3
- ◆ [“Important Operational Notes”](#) on page 5
- ◆ [“Installing VFM”](#) on page 9
- ◆ [“Upgrading to VFM 6.0”](#) on page 12
- ◆ [“Upgrading the Server or the Client and Server”](#) on page 15
- ◆ [“Upgrading Replication Agents”](#) on page 16
- ◆ [“Issues Resolved in VFM 6.0.1”](#) on page 18
- ◆ [“Issues Resolved in VFM 6.0.2”](#) on page 19
- ◆ [“VFM 6.0.2 Known Operating Issues”](#) on page 20
- ◆ [“VFM 6.0.2 Known Upgrade Issues”](#) on page 24
- ◆ [“Documentation corrections”](#) on page 26
- ◆ [“Glossary for VFM 6.0”](#) on page 27

VFM 6.0 New Features

New features for VFM 6.0

VFM 6.0 is a major release that adds the following new features:

- ◆ **Phased migration**
This feature enables you to stage the data migration operation. You can run automatically repeated data copy operations before running the final copy and cutover, and you control when the migration operation moves from one phase to another. This feature is available for the migration, archival migration, and storage load-balancing policies.
- ◆ **Quick addition of multiple targets to a link**
This feature enables you to clone an existing link target to quickly multiply the number of targets linked: for example, cloning a WAFS edge device can quickly increase the number of such devices linked to a WAFS core.
- ◆ **Agent management**
This feature enhances the management of replication and monitoring agents and the VFM server, including deployment credentials.
- ◆ **Replication agent groups**
This feature enables you to add multiple replication agents to an agent group and assign the group to a policy to distribute the data migration workload. This improves flexibility and throughput in many-to-one replication scenarios.
- ◆ **DFS attributes supported for namespace backup and restore processes**
This feature enables you to use the new DFS attributes introduced in Windows Server 2003 release 2.

Installation Requirements

Basic system requirements

Before installing VFM, ensure that the computers on which the VFM components will be installed meet the following requirements.

Hardware requirements:

- ◆ At least 2 GHz or faster processor
- ◆ At least 2 GB of RAM
- ◆ 500 MB of free disk space

Note

Add 75 MB to disk space requirements for a typical or server-only installation when you install the Microsoft SQL Server.

Operating system requirements:

- ◆ 32-bit operating system (64-bit not supported)
- ◆ Microsoft® Windows® 2000 SP 4 or Microsoft Windows XP Professional SP 1 or later, to manage roots on separate servers
- ◆ Microsoft Windows Server™ 2003 SP 1, Microsoft Windows Server 2003 RS Standard or Enterprise Edition, or Microsoft Windows XP Professional SP 1 or later, to manage multiple roots on a single Windows Server 2003

Note

The number of connections between VFM components and used by other processes on the system might exceed the limits on inbound connections imposed by Windows 2000 Professional or Windows XP Professional, and VFM components could experience communication problems. Use the Computer Management MMC snap-in (compmgmt.msc) to review the number of connections in use. If you exceed the inbound connection limits, install the VFM server on a computer running Windows 2000 or Windows Server 2003. These limits are documented in the Microsoft Knowledge Base Articles 122920 and 314882.

Additional software requirements:

- ◆ Microsoft .NET Framework 2.0
- ◆ Internet Explorer™ 5.5 or later
- ◆ Windows Script Host 5.6 or later

Server and monitoring agent requirements

Before installing VFM, ensure that the computer on which the VFM server and monitoring agent components will be installed meets the following requirements.

Additional software requirements:

- ◆ Microsoft SQL Server 2000 Desktop Engine (MSDE) SP 3 or later, Microsoft SQL Server 2000 Standard or Enterprise Edition SP 3 or later, or Microsoft SQL Server 2005 Enterprise Edition, to install the VFM database and monitoring agents

Configuration requirements:

- ◆ Local fixed NTFS disks, to install the VFM components
- ◆ Minimum video display of 1,024 by 768 pixels with 256 colors (more than 256 colors recommended for best display)
- ◆ Remote Desktop Protocol (RDP) strongly recommended, to connect to remote machines (other products providing remote desktop access, such as VNC (Virtual Network Computing), have exhibited screen rendering problems with VFM)

Note

To generate reports when VFM uses the remote SQL database, make sure that the Microsoft OSQL utility is installed on the machine hosting the VFM server.

Note

The evaluation license of VFM places a 60-minute limit on data transfers. This limit is for each run of a policy.

Client requirements

Before installing VFM, ensure that the computer on which the VFM client components will be installed meets the following requirements.

Configuration requirements:

- ◆ Local fixed NTFS disks, to install the VFM components
- ◆ Minimum video display of 1,024 by 768 pixels with 256 colors (more than 256 colors recommended for best display)
- ◆ RDP strongly recommended, to connect to remote machines (other products providing remote desktop access, such as VNC, have exhibited screen rendering problems with VFM)

Important Operational Notes

Before you begin This section contains information that you should consider before you use VFM 6.0. Read these notes completely before you launch and use VFM. See the product online Help for full details.

- Account permission and privilege requirements**
- ◆ The account used to install VFM must be a member of the Administrators group on the local system.
 - ◆ The VFM server, monitoring agent, and replication agent service accounts must have the following permissions:
 - ❖ SeBackupPrivilege (“Back up files and directories”)—required to open source directories or files with backup semantics
 - ❖ SeRestorePrivilege (“Restore files and directories”)—required to open destination directories or files with backup semantics
 - ❖ SeSecurityPrivilege (“Manage auditing and security log”)—required to access SACLs (System Access Control Lists)
 - ❖ SeTakeOwnershipPrivilege (“Take ownership of files or other objects”)—required to delete directories or files

Note _____
Some Network Attached Storage (NAS) systems might require that the replication agent service account be a member of the local Administrators group and have Backup Operators permissions.

- ◆ The VFM server and monitoring agent service accounts must have the following permissions and privileges:
 - ❖ Appropriate permissions to administer the Distributed File System (DFS) roots

Account	Permission requirements
Stand-alone roots	The account must be a member of the local Administrators group on the system hosting the root and must have permissions to write to the root share on that system.

Account	Permission requirements
Domain-based roots	Microsoft Active Directory must already be operational. The account used for VFM must have Administrator permissions for both the domain controller computer and the server on which you create the DFS root. For more information, see the Microsoft DFS FAQ available at http://www.microsoft.com .

- ❖ Permission to log in and run as a service
- ❖ Membership in the local Administrators group on the computer hosting the SQL database used by VFM
- ❖ Permissions to write to the All Users\Application Data\ directory tree
- ◆ The VFM replication agent service account must have the following permissions and privileges:
 - ❖ Permission to log in and run as a service
 - ❖ Membership in the local Administrators group on the computer running the replication agent
- ◆ If you plan to use VFM to administer SnapMirror® information on a NetApp® storage system, your systems must meet the following configuration requirements:
 - ❖ The VFM service account must be a member of the local Administrators group on a NetApp storage system to access the \\filer\C\$ share and read and write files in the /etc directory of the storage system.
 - ❖ Source NetApp storage systems running Data ONTAP® 7.2 or later must have the “snapmirror.access” option set to “legacy” to enable VFM to manage SnapMirror relationships.
 - ❖ You must provide the remote shell (RSH) username and password for NetApp storage systems known to VFM so that VFM can communicate with the storage systems when managing SnapMirrors and qtrees. You can configure this information through the computer properties dialog box for the storage system.
- ◆ By default, VFM uses RSH to execute shell commands that configure and obtain data from NetApp storage systems and other non-Windows systems, such as Solaris and Linux computers.
 - ❖ On Solaris and Linux systems, RSH must be enabled as root. See the online Help for more information about how to enable RSH as root on Solaris and Linux computers.

- ❖ Where the environment does not support the use of RSH, you can configure VFM to use SSH (secure shell) to communicate with NetApp storage systems in place of RSH. See the online Help for more information.

Windows replication agent requirements

Before deploying a Windows replication agent from VFM, ensure that the destination computer meets the following requirements.

Operating system requirements:

- ◆ Microsoft Windows 2000 SP 4, Microsoft Windows Server 2003 SP1, Microsoft Windows Server 2003 R2 Standard or Enterprise Edition, or Microsoft Windows XP Professional SP 1 or later

Additional software requirements:

- ◆ If the machine to which you want to deploy a replication agent is running Microsoft VSS, Microsoft .NET Framework 2.0 must also be installed.

Configuration requirements:

- ◆ The account used by VFM to deploy a Windows replication agent must be a member of the local Administrators group on the computer that receives the replication agent and must be able to perform the following actions on the destination computer:
 - ❖ Create, read, and write registry keys
 - ❖ Write to Admin\$ share
 - ❖ Install and run a service
- ◆ If the machine to which you want to deploy a replication agent is running Windows XP SP 2, you must ensure that the firewall on that computer is not blocking TCP port 6002, which is used to communicate with the VFM server. You can do this by either disabling the firewall or configuring it to allow port 6002.

UNIX replication agent requirements

Before deploying a UNIX® replication agent from VFM, ensure that the destination computer meets the following requirements.

Operating system requirements:

- ◆ Solaris 10 or Red Hat® Enterprise Linux® 4

Additional software requirements:

- ◆ If the machine to which you want to deploy a replication agent is running Solaris 10, the following packages must be installed:

- ❖ SUNWcsl
- ❖ SUNWlibms
- ❖ SUNWcsu
- ❖ SUNWloc
- ❖ SUNWgzip
- ◆ If the machine to which you want to deploy a replication agent is running Red Hat Enterprise Linux 4, the following packages must be installed:
 - ❖ glibc-2.3.4-2
 - ❖ glibc-common-2.3.4-2
 - ❖ bash-3.0-19.2
 - ❖ coreutils-5.2.1-31
 - ❖ gzip-1.3.3-9
 - ❖ grep-2.5.1-16
 - ❖ procps-3.2.3-7
 - ❖ Red Hat package manager version 4

Note

The version of the packages can be later than those listed.

Configuration requirements:

- ◆ The account used by VFM to deploy a UNIX agent must have root privileges on the machine on which you deploy the replication agent.
- ◆ NFS 3 or later must be installed on the source or destination if a UNIX replication agent is not installed. You do not have to install NFS on the source or destination that is hosting a UNIX replication agent, because the replication agent reads the files directly.
- ◆ The file system on which the replication agent will be installed must be mounted with read-write permission. If you attempt to install the replication agent on a read-only file system, the following error message appears:
 - ❖ On Solaris:


```
pkgadd: ERROR: Unable to make directory </opt/URA>
```
 - ❖ On Red Hat Linux:


```
error: unpacking of archive failed on file
/opt/ura/bin:
cpio: mkdir failed - No such file or directory
```

Installing VFM

Installation options The following table describes the different VFM installation options.

Setup type	Description
Client and server	This is the typical configuration recommended for most installations. Both the VFM client and server components are installed on a single system.
Client	Only the VFM client components are installed. You are prompted to enter the location of a remote VFM server. This is useful if you installed the VFM server on an infrastructure machine and want access to the VFM console from a desktop machine.
Server	Only the VFM server components are installed. This is useful if you want to install the VFM server on a highly available machine in your server room and manage VFM from a desktop machine.
Monitoring agent	Only the VFM monitoring agent functionality is installed. You are prompted to enter the location of a remote VFM server. This is useful if you want to distribute VFM policy monitoring chores across multiple machines. Note_____ If the host name of the remote VFM server is not entered accurately, the monitoring agent cannot communicate with the server. _____
Client and monitoring agent	The VFM client and monitoring agent components are installed on a single system.

Steps

To install VFM for the first time, complete the following steps.

Step	Action
1	Log in to the computer on which you want to install VFM using a user account that is a member of the local Administrators group.
2	Install the Microsoft .NET Framework 2.0, available at http://www.microsoft.com .
3	Browse to the location to which you saved the VFM installation package, run the Autorun.exe file, then click on the Install button.
4	In the Welcome window, click Next and then click Yes to accept the terms of the license agreement.
5	Review the Release Notes and then click Yes.
6	Select the setup type (described in “ Installation options ” on page 9) and then click Next. Note _____ If you want to change the combination of product components installed on a computer later, you must first uninstall the existing components before reinstalling new components on the computer. _____
7	Enter the following information: ◆ In the Serial Number field, type your serial number. ◆ In the License Type field, select your license type. ◆ In the Activation Key field, type your activation key. Click Next.
8	Specify where you want the setup program to install the VFM files and then click Next.

Step	Action
9	Specify a location for application data storage and then click Next. Attention _____ To avoid problems with future upgrades, <i>do not specify a location for application data storage in the same directory in which you are installing the VFM server files.</i> Instead, browse to a different, empty folder location on a local NTFS file system for which the VFM service account has write permissions.
10	If you want a desktop shortcut created, check “Create a desktop shortcut to this product” and then click Next.
11	Specify the logon credentials for the VFM service account and then click Next.
12	If you want to use an existing Microsoft SQL Server instance, perform the following actions. a. Click “I would like to use an existing SQL instance” and then click Next. b. In the Database Server field, specify the Microsoft SQL Server database you want to use. c. If you want to connect to the database using Windows authentication, check “Windows authentication.” d. If you want to connect to the database using Microsoft SQL Server authentication, check “SQL Server authentication using the Login AD and password below,” type a login ID and password, then click Next.
13	If you want to use MSDE for your database, click “Please install MSDE for me” and then click Next. Note _____ You can use MSDE for product evaluations and normal product use. However, if you anticipate very heavy usage of reporting features in VFM, consider using the Microsoft SQL Server instead.
14	Click Next and then click Finish.

Upgrading to VFM 6.0

Read before upgrading

Supported upgrades: You can upgrade to VFM 6.0.x from versions 5.5, 5.6, or 5.8. If you have already installed VFM 6.0 but have not installed VFM 6.0.1, you can install VFM 6.0.2 without first installing version 6.0.1.

Installing additional VFM components on a machine: Beginning with VFM 5.8, you cannot install a VFM component on a machine that already has a different VFM component installed. For example, if you installed the VFM client on Server A and now you want to install the VFM server on Server A as well, you must perform the following actions.

Step	Action
1	Uninstall the VFM client on Server A.
2	Install the VFM client and server during the installation process on Server A.

Renaming VFM components: Never rename a machine while the VFM server, monitoring agent, or replication agent is installed on it, as this can cause problems managing agents. To rename the machine on which the VFM server or monitoring agent is installed, perform the following actions.

Step	Action
1	Export your VFM configuration files.
2	Uninstall VFM.
3	Rename the machine.
4	Reinstall VFM.
5	Import the configuration files from Step 1.

See “Export configuration files” in the VFM online Help for detailed instructions.

Upgrade steps for installation options

Before beginning an upgrade, make sure that the computer on which you are performing the upgrade meets the requirements for the relevant components, as outlined in “[Installation Requirements](#)” on page 3

The following table lists the various installation options available in VFM and the steps required to upgrade each combination of components.

Installation option	Steps
Server only	1. Follow the instructions in “Upgrading the Server or the Client and Server” on page 15.
Client and server	1. Follow the instructions in “Upgrading the Server or the Client and Server” on page 15.
Client only	1. Log in to the computer on which the VFM client is installed using a user account that is a member of the local Administrators group. 2. Close the VFM client. 3. Perform the upgrade. See “Installing VFM” on page 9 for more information on installing the VFM components.
Monitoring agent only	1. Stop the VFM server. 2. Log in to the computer on which the VFM monitoring agent is installed using a user account that is a member of the local Administrators group. 3. Perform the upgrade. See “Installing VFM” on page 9 for more information on installing the VFM components. 4. Restart the VFM server.

Installation option	Steps
Monitoring agent and client	1. Stop the VFM server. 2. Log in to the computer on which the VFM monitoring agent and client are installed using a user account that is a member of the local Administrators group. 3. Close the VFM client. 4. Perform the upgrade. See “Installing VFM” on page 9 for more information on installing the VFM components. 5. Restart the VFM server.
Replication agents	Follow the instructions in “ Upgrading Replication Agents ” on page 16.

Upgrading the Server or the Client and Server

Steps

To upgrade the server or the client and server, complete the following steps.

Step	Action
1	Have the VFM serial number and license key information available and saved on a remote location before you begin the upgrade.
2	Cancel all policies currently running or let them finish running. If you are upgrading a server only, cancel all policies from a client connected to the server.
3	In the list of properties for each policy, uncheck “Use...schedule” to ensure that no scheduled policies attempt to run during the upgrade.
4	Back up the namespace by right-clicking Logical View and then clicking Backup. Select all the roots that are used in your environment.
5	Back up the current configuration by going to the Tools menu, clicking Take Application Snapshot Now, and saving the existing configuration locally on the VFM server. You can use a replication policy or Windows Explorer to manually copy the application backup to a remote location to have a second copy of the configuration.
6	Close the VFM client.
7	Stop the VFM server.
8	Perform the upgrade. See “ Installing VFM ” on page 9 for more information on installing the VFM components.

Upgrading Replication Agents

Steps

The replication agents used by VFM are upgraded automatically by the VFM server during its normal status checks. You can perform the following steps to verify that replication agents have been upgraded and to upgrade any agents that are not automatically upgraded.

Step	Action
1	Close the VFM client.
2	Restart the VFM server using the Windows service control manager.
3	Reopen the VFM client.
4	On the Tools menu, click Agent Management.
5	Select a replication agent and verify the version by viewing the replication agent's properties.
6	If the replication agent was not updated, right-click the agent and then click Upgrade.
7	Click Alerts to view any errors that might have occurred.
8	If the upgrade fails using this method, try to uninstall the replication agent and redeploy it.

If attempts to uninstall a replication agent using the Agent Management tool are not successful, complete the appropriate following steps for CIFS or NFS replication agents.

CIFS

To uninstall and redeploy a CIFS replication agent, perform these steps.

Step	Action
1	Log in to the server running the replication agent.
2	Open a command prompt and run the following command: <code>cd C:\Windows\system32\Brocade\VFM\ReplicationAgent</code>

Step	Action
3	Run the following command: <code>net stop storagexreplicationagent</code>
4	Run the following command: <code>replicationagent.exe -uninstall</code>
5	Delete the contents of this directory and exit the command prompt.
6	Using the service control manager, verify that the StorageXReplicationAgent service no longer exists.
7	Delete the following registry key if it exists: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Brocade\VFM\ReplicationAgent</code>
8	Reboot the machine and then deploy the new replication agent, using the Agent Management tool.

NFS

To uninstall and redeploy an NFS replication agent, perform these steps.

Step	Action
1	Uninstall the older version of the replication agent using the instructions provided in the online Help for the Agent Management tool. Make sure that you delete the application directory.
2	Open the VFM client.
3	On the Tools menu, click Agent Management, then Deploy.
4	Specify the name of the machine that will host the replication agent and the account that will run it, then click OK.
5	When the replication agent appears in the list, click the agent to verify the version information.

Issues Resolved in VFM 6.0.1

Resolved issues

The following VFM 6.0 known issues were resolved in VFM 6.0.1:

- ◆ The unformatted event history error message reported during UNIX replication agent deployment has been corrected.
- ◆ Where replication failed in response to the error message “RPC failed,” the replication agent now retries the operation.
- ◆ Upgrades of VFM no longer leave extra entries in the Add and Remove Programs list and the Start menu.
- ◆ Application backup replication now correctly copies data from the link target rather than from the share containing the link target.
- ◆ The VFM Logical View now correctly shows all roots in the view.
- ◆ In some cases in which the NETBIOS domain name differed from the fully qualified domain name in DNS, the root displayed twice in the VFM Logical View. This has been corrected.
- ◆ To facilitate viewing the details of recent events, the event history now shows the most recent events at the top of the list.
- ◆ The VFM user interface now prevents you from selecting mutually exclusive options when using cached hash sets with application backup replication.
- ◆ An error message is no longer reported when you use differential replication and application copies together in a policy.
- ◆ Storage system recovery policy alternate schedule handling has been corrected.
- ◆ VFM now copies the FLM alternate data streams when they are present.
- ◆ Folder exclusions specified in a policy using application backup replication now correctly exclude the specified folders.

Issues Resolved in VFM 6.0.2

Resolved issues

The following VFM 6.0.1 known issues are resolved in VFM 6.0.2:

- ◆ If the namespace was unavailable when a policy attempted to perform a namespace update during the final phase of a migration, the policy results reported that no links were updated. This has been corrected.
- ◆ If data was copied during the initial or incremental phases, VFM would perform a final copy during the final phase of data migration even if this option was not selected. This has been corrected.
- ◆ When the renaming of a .tmp file fails during replication, VFM now rolls back the file, preventing unintended accumulation of temporary files.
- ◆ VFM now consistently copies Brocade File Lifecycle Manager (FLM) metadata when copying FLM minifiles from the source directory.
- ◆ The VFM user interface now prevents you from selecting the mutually exclusive options “Preserve last access time on source” and “use snapshot data.” If both were selected, it would cause a policy to fail.
- ◆ Client Data Recovery failover did not initiate the associated namespace availability policy when it should have, resulting in the slave root becoming out of sync with the master root until the namespace availability policy either ran on schedule or was started manually. This issue has been resolved.
- ◆ If administrators were removed from the ACL list on the source, and a synchronization of changed files was then performed with safe copy enabled, the replication failed and left behind temporary files. This issue has been resolved.
- ◆ The VFM user interface no longer shuts down unexpectedly when you change various replication policy options from the Tools > Options menu.

VFM 6.0.2 Known Operating Issues

Known operating issues

This section describes outstanding issues found in VFM 6.0.2.

- ◆ In certain configurations, the user and effective user fields in events generated by the server display as N/A for the client. For example, when the VFM client and server reside in separate domains, there is a one-way “forest trust” by the server domain of the client domain, and the client and server are running under different accounts in the two domains.
- ◆ Large namespaces such as those with thousands of links cause VFM to start up more slowly than do smaller configurations. Startup times increase with the size of the configuration.
- ◆ Cascaded domain-based roots appear as machines in the physical view if any of their links are themselves targets of links in a managed namespace.
- ◆ Time differences between the VFM console system and systems on which the VFM replication agent is deployed affect the order in which events are displayed in the VFM console.
- ◆ Changes made to domain-based roots can take time to appear in the VFM display. This is due to the time needed for the changes to propagate through the Active Directory domain controllers.
- ◆ If the server hosting the new target is online, then the directory being targeted by the link must exist or VFM gives a “network resource was not found” message.

Workaround: When modifying link targets, if the server hosting the new link target is offline, you can still retarget the link to the offline server. This implementation enables you to configure your namespace when servers are offline, while providing additional validation of the configuration when the targeted servers are online.

- ◆ Share names containing apostrophes might prevent VFM from accessing data on the share. The symptom is an “access-denied” error when attempting to migrate data to or from the share.
- ◆ Certain combinations of file permissions can cause VFM to report access-denied errors during the evaluation phase of a data transfer.

Workaround: If you allow the evaluation to continue, it will succeed.

- ◆ Limitations present in Internet Explorer 6 cause changes to print orientation to be applied to the printer specified for the item being printed rather than to just the print item itself.

Workaround: Restore the orientation for the selected printer to the desired default setting after the report has been printed. This limitation is not present in Internet Explorer 5.5.

- ◆ Limitations present in Windows 2000 prevent management of DFS roots on Windows Server 2003 systems when VFM is installed on a Windows 2000 system and a Windows Server 2003 system hosts more than one DFS root.

Workaround: To manage roots hosted on a Windows Server 2003 system containing more than one DFS root, you must install VFM on Windows XP or Windows Server 2003.

- ◆ Antivirus software configured to prevent scripts from running interferes with scripts used in VFM as part of the product installation as well as the application backup feature and customized scripts configured for use with VFM storage policies.

Workaround: To avoid this problem, configure virus scanning software correctly so that VFM can be installed and the scripts associated with the product can function.

- ◆ If you upgrade VFM using terminal services, you might encounter problems printing from VFM to PDF files.

Workaround: To avoid this problem, upgrade from the machine console and not through terminal services.

- ◆ Microsoft changed the implementation of DFS roots in Windows Server 2003. Because of these changes, BLOB size is reported as zero for roots hosted on Windows Server 2003 in the VFM Namespace Properties report.
- ◆ Incorrect name resolution configurations in DNS can cause problems when managing or referencing domain-based DFS roots. The troubleshooting section of the VFM documentation provides details on how to diagnose and correct DNS name resolution problems.
- ◆ If you initiate a manual scan for a Namespace Creation policy and no items are found, the resulting instruction dialog must be closed by clicking Cancel.
- ◆ When copying files from mixed-security mode locations on NetApp storage systems, permissions must be set so that VFM can read security information from the system. UNIX permissions are not transferred. Errors will occur if VFM cannot read the security settings from the source data.
- ◆ VFM does not show users without home folders in the following situation:
During home folder policy creation, you select the option “Show users without a home folder.” You select a user or users without home folders, click Next, and then click Back. Any users without home folders that you selected do not appear in the list.

Workaround: After you click Back, clear the existing selections and select the option “Show users without a home folder.” Click Next and then Finish.

- ◆ When the target monitoring schedule runs, server disaster recovery policies incorrectly run associated policies instead of running associated policies only when a failover is required. This problem causes extra namespace update activity.
- ◆ Application-wide default credentials for SSH that you specify do not take effect properly.
Workaround: Set SSH credentials on individual machines in the Physical View rather than in the Options dialog box. Right-click the machine in the Physical View and click Properties. Click the Shell tab. See the online Help for further instructions.
- ◆ You cannot drag a link with two targets, one each on the primary and secondary servers, to the Active Link list of a server disaster recovery policy.
Workaround: Right-click a link in the Nonactive Links list and click Move to Active Links List.
- ◆ UNIX replication agents cannot be deployed by VFM monitoring agents. This can result in an unexpected replication agent performing a data transfer.
Workaround: Use Agent Management to manually deploy the UNIX replication agent to the source or destination machines before starting the policy. On the Tools menu, click Agent Management and follow the online Help instructions to deploy a UNIX replication agent.
- ◆ You see the following error message when you try to uninstall a VFM component, such as the client or server, using Add or Remove Programs from the Windows Control Panel:

```
A fatal error has occurred. This process will now abort. Reason:  
Installation of VC runtime library failed.
```


Workaround: Run the installation package again instead of using Add or Remove Programs to uninstall the product.
- ◆ The VFM Browse dialog box incorrectly shows two copies of the same root when the NETBIOS domain name differs from the hostname portion of the fully qualified domain name.
- ◆ NFS file inclusions and exclusions in VFM policies might not function correctly. When configuring policies that use inclusions and exclusions, assess the replication results carefully.
- ◆ When VFM migrates files from a Brocade File Lifecycle Manager (FLM) active store and the VFM replication agent is not hosted on a restore-blocked computer, only partial file contents are copied to the VFM destination. FLM restores the full file contents to the active store, but VFM transfers only the amount of file content that corresponds to the size of the minifile.

Workaround:

If...	Then...
The sources on the FLM active store have not been deleted	Rerun the VFM data transfer after selecting “different or missing files” in the replication options for the policy.
The sources on the FLM active store have been deleted following the VFM transfer	Restore from a Data ONTAP Snapshot™ copy, or use the FLM Manager tool to restore copies of the files from the FLM offline store.

To prevent this issue in future migrations: Set the “different or missing files” option in the migration or replication policy and allow the policy to repeat the data transfer phase at least twice. The first transfer restores the FLM data and the second transfer copies the restored data to the VFM destination. Alternatively, you can use FLM Manager of the FLM Web interface to restore any files migrated with FLM before transferring them with VFM.

VFM 6.0.2 Known Upgrade Issues

Known upgrade issues

This section describes issues encountered when upgrading to VFM 6.0.2 from previous versions.

Upgrading a monitoring agent

When you try to upgrade a monitoring agent installed on a machine that is hosting a replication agent, the upgrade fails and you get the following error message:

`Destination key already exists.`

Workaround: Perform the following steps before starting the VFM upgrade.

Step	Action
1	Delete the existing replication agent. For instructions about how to delete replication agents, see the online Help.
2	Delete the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Brocade.
3	Upgrade the monitoring agent.
4	Deploy a new replication agent on the same machine on which you upgraded the monitoring agent.

Upgrading a server if MSDE is already installed

Because InstallShield searches for an instance name, if you try to upgrade the VFM server on a machine on which a nameless local instance of MSDE is already installed, you get the following error message:

`Error 27502 Could not connect to Microsoft SQL Server... does not exist or access denied.`

Workaround: Perform the following steps before starting the VFM upgrade.

Step	Action
1	Ensure that there are no running replication policies and that the VFM console is closed.
2	Stop the VFM server.
3	Move the VFM main database and VFM report databases to a named instance of MSDE.
4	Locate the Server.exe.config file in the installation directory and open it in a text editor.
5	Edit the Server.exe.config file to reflect the new location of the databases in the definition of the “Data Source” in the “add key” line. For example, “Data Source=SERVER_NAME” would be changed to “Data Source=SERVER_NAME\INSTANCE.”
6	Restart the VFM server.
7	Verify that you can access the VFM console.
8	Close the console.

Upgrading using a nondefault MSDE or SQL Server Express instance

When you try to upgrade the VFM server on a machine on which you are using a nondefault instance of MSDE or SQL Server Express, the upgrade process fails with SQL connection errors. This is because TCP is disabled by default for nondefault instances of MSDE and SQL Server Express.

Workaround: Perform the following steps before starting the VFM upgrade.

Step	Action
1	Navigate to the following folder: C:\Program Files\Microsoft SQL Server\80\Tools\Binn
2	Run the file SVRNETCN.exe.
3	In the SQL Server console, enable the “Named Pipes” protocol (TCP).
4	Restart the SQLSERVER and SQLAGENT services.

Documentation corrections

Corrections to the VFM 6.0 documentation

The following change has been made in the documentation originally released with VFM 6.0:

- ◆ The documentation incorrectly indicates that VFM is compatible with PuTTY suite 0.55 or later. However, later versions of PuTTY introduced compatibility issues with VFM, so only programs from PuTTY suite 0.55 should be installed.

Glossary for VFM 6.0

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.
CIFS	Common Internet File System. A file-sharing protocol based on the Microsoft Server Message Block (SMB), CIFS enables you to share file systems over the network. 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. The consolidation DFS root allows one server to take over the name of another server.
dependencies	The servers, drives, and shared folders that together contain the data published through the DFS namespace.
DFS	Microsoft Distributed File System. 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. <i>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.</i>
DFS link	Located under the namespace root. Forms a connection to one or more shared folders or 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	The 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.
export	<i>See</i> NFS export.
fault-tolerant DFS	<i>See</i> domain-based DFS root.
FQDN	Fully qualified domain name. A host, a second-level domain, and a top-level domain. For example, www.netapp.com is a fully qualified domain name in which www is the host, .netapp is the second-level domain, and .com is the top-level domain.
FRS	Microsoft File Replication Service. A data replication service used in Windows 2000.

GID	Group identification number. A unique number assigned to identify a group of users in UNIX environments.
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.
link target	A shared folder, DFS link, or DFS root that is referenced by a DFS link. A DFS link can have one of the following as its target: 1 to N shared folders, 1 to N stand-alone DFS paths, or only 1 domain-based DFS path.
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 of policies that migrate data.
monitoring agent	The component that can be installed to evaluate storage policies from a different machine than the one on which the application server is installed.
NFS	Network File System, developed by Sun Microsystems. A file-sharing protocol that enables you to share file systems over the network. 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.
pool	A group of storage locations.
primary server	An active application server or monitoring agent.

primary target	In a disaster recovery policy, the active target to which users are referred by the root or link.
qtree	A special directory of the root of a NetApp volume that behaves like a virtual subvolume with special attributes.
quiesce	To wait for all existing SnapMirror transfers to both NetApp volumes and qtrees to complete and then block any further updates.
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 which the data is to be migrated.
references	The DFS link targeting the selected physical item. For example, when you click a server in 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. In Windows NT 4 terminology, this is referred to as an <i>alternate volume</i> .
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 off-load 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 in which 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 or after the information is gathered.
report type	Determines which information is gathered. Report types are assigned to report source groups.
secondary target	<i>See</i> standby target.
server	The component that responds to requests from the client component, monitors the DFS namespace, and processes storage policies.
shared folder	A folder in the DFS namespace that can be accessed by users who have proper permissions. In Windows NT 4, this is referred to as a DFS <i>volume</i> , <i>leaf</i> , or <i>branch</i> .
SID	A 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.
target	A link target is a shared folder, a DFS link, or a DFS root that is referenced by a DFS link. A root target is a shared folder that is referenced by a DFS root. <i>See also</i> link target.
trustee	The user account, group, or logon session to which an Access Control Entry (ACE) applies.
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.
widelink namespace	A logical namespace hosted on a NetApp storage system CIFS share that provides the benefits of a namespace without requiring additional Windows servers.