VFM® (Virtual File Manager™) 6.0.1
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 215-03436_A0
September 2007

Copyright and trademark information

Copyright information

Copyright © 1994–2007 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 Network Appliance material 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.

Portions copyright © 2005 Tree Menu, Inc. All rights reserved.

Permission to use the Tree Menu script in NetApp's product has been granted by Tree Menu; however, no permission is granted to extract the JavaScript and use such JavaScript in some other application. You can make changes to the Tree Menu script, provided you keep all the source comments (inside the code; not visible to the users) regarding the author of the script (Marcelino Martins) and the origin of the code (www.Treeview.net) in all the source files directly associated with the Tree Menu script (HTML, JS, ASP, etc.).

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. 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

NetApp, the Network Appliance logo, the bolt design, NetApp–the Network Appliance Company, DataFabric, Data ONTAP, FAServer, FilerView, 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, FlexClone, 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 United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the U.S.A.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States 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 United States 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 6.0.1 Release Notes

Release and upgrade topics

These release notes contain the following release and upgrade topics:

- "VFM 6.0 Changes" on page 2
- "Requirements" on page 3
- "Important Operational Notes" on page 6
- "VFM 6.0 Known Operating Issues" on page 10
- "VFM 6.0 Known Upgrade Issues" on page 14
- "Known Issues Resolved in VFM 6.0.1" on page 16
- "Upgrading to VFM 6.0" on page 17
- "Upgrading the Server or the Client and Server" on page 19
- "Upgrading Replication Agents" on page 20
- "Glossary for VFM 6.0" on page 23

VFM 6.0 Changes

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 archival migration, 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.

Requirements

Installation requirements

Before installing VFM, ensure that the system in which the VFM components are installed meets the following requirements:

- Microsoft® Windows® 2000 SP 2 or later or Windows XP Professional, to manage roots on Windows NT® 4 or Windows 2000 servers
- Microsoft Windows XP Professional or Windows Server™ 2003, to manage multiple roots on a single Windows Server 2003
- Microsoft SQL Server 2000 Desktop Engine (MSDE) Service Pack 3 or later, SQL Server 2000 Standard or Enterprise Edition Service Pack 3 or later, or Microsoft SQL Server 2005 Express Standard or Enterprise Edition, to install the VFM database and monitoring agents
- Microsoft .NET Framework 2.0
- Internet Explorer™ 5.5 or later
- Windows Script Host 5.6 or later
- At least 2 GB of RAM
- At least 2 GHz or faster processor
- 500 MB of free disk space

Note

Add 75 MB to disk space requirements for a typical or server-only installation when you install MSDE.

- Local fixed NTFS disks, to install the VFM components
- 32-bit operating system (64-bit not supported)
- 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, have exhibited screen rendering problems with VFM)

Note

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

Note

As part of the installation process, you are asked where to install the Application Data directory. To avoid problems with future upgrades, do not install this component in the same directory where you are installing VFM. Instead, browse to another location on a local NTFS file system to which you have write privileges and use an empty folder there.

Note

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

Note

The evaluation license of VFM places a 60-minute limit on the amount of data you can transfer. This limit is for each run of a policy.

Installation options

The following table describes the different VFM configurations.

Configuration	Description
Client and server	This is the typical configuration. The VFM components are installed on a single system.
Client	You are prompted to enter the location of the remote VFM server. This choice is useful if you installed the VFM server on an infrastructure machine and want access to the VFM console from your desktop machine.
Server	This choice is useful if you want to install the VFM server on a highly available machine in your server room and manage VFM from your administrative desktop machine.

Configuration	Description
Monitoring agent	You are prompted to enter the location of the remote VFM server. This choice is useful if you want to distribute VFM policy monitoring chores across multiple machines. 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 components are installed on a single system.

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 permissions and privileges for installing and running VFM

- The account installing VFM from media must have administrator privileges on the local system.
- The account used for the VFM server, which is specified during installation, must have the following permissions and privileges:
  - Appropriate permissions to administer the DFS roots that are managed

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.
Domain-based roots	Microsoft Active Directory must already be operational. The account used for VFM must have administrator permissions for both the domain and the server on which you create the DFS root. See the Microsoft DFS FAQ: `http://www.microsoft.com/windowsserver2003/community/centers/fileservices/dfsfaq.mspx?pf=true`

  - Administrator privileges on any machines hosting either source or destination of data replications
  - “Run as service” privilege
  - Local administrator privilege on the machine hosting the SQL database used by VFM
- The account running the VFM client and server must have permissions to write to the All Users\Application Data\ directory tree.

Users whose accounts lack write permissions to these directories experience errors when attempting to run VFM reports or set VFM system options.

- When administering SnapMirror® information, the account running VFM must have administrator privileges on any managed NetApp® storage system to access the \\filer\C$ share and read and write files in the /etc directory of the storage system.

  VFM also uses RSH to communicate with NetApp storage systems when managing SnapMirror copies and qtrees. The RSH user name and password for VFM to use when communicating with storage systems is configured through the machine properties dialog box for the storage system.

  To enable VFM to manage SnapMirror relationships, source NetApp storage systems running Data ONTAP® 7.2 or later must have the option "snapmirror.access" set to "legacy".

- The account used by the VFM server, a replication agent, or a VFM monitoring agent 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 NAS systems might require that the account used by a replication agent be a member of the local administrators and backup operators groups.

RSH on Linux and Solaris machines

VFM normally uses RSH to execute shell commands to configure and obtain data from NetApp storage systems and other non-Windows systems, such as Solaris™ and Linux® systems.

- On Solaris and Linux systems, RSH must be enabled as root. See the online Help for instructions about how to enable RSH as root on Solaris and Linux systems.
- Where the environment does not support the use of RSH, you can configure VFM to use SSH to communicate with NetApp storage systems in place of RSH. See the online Help for requirements and instructions.

Windows replication agent requirements

VFM deploys a replication agent to machines running Windows 2000, Windows Server 2003, or Windows XP file systems.

- The account used by VFM to deploy a Windows replication agent must have administrator privileges on the machine that receives the replication agent. The account must be able to perform the following actions:
  - Access remote registry
  - 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 perform the following actions.

Step	Action
1	Disable the firewall on the machine on which you want to deploy the replication agent.
2	Restart the machine.

- If the machine to which you want to deploy a replication agent is running Microsoft VSS, it needs to also run Microsoft .NET Framework 2.0.

UNIX replication agent requirements

General requirements: The UNIX® machine on which you deploy a replication agent must be running Red Hat® Enterprise 4 or Solaris 10 operating system.

- 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 Linux:

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

Solaris 10: The following packages must be installed on the machine on which the replication agent will be deployed:

- SUNWcsl
- SUNWlibms
- SUNWcsu
- SUNWloc
- SUNWgzip

Red Hat Enterprise 4: The following packages must be installed on the machine on which the replication agent will be deployed:

- 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 or later

Note

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

VFM 6.0 Known Operating Issues

VFM 6.0 operating issues

This section describes issues found in this version of VFM.

- In certain configurations, the user and effective user fields in events generated by the server display as N/A by 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 along 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.
- Clock skew between the VFM console system and systems on which the VFM replication agent is deployed affects 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.
- NT4 DFS roots are typically created when DFS is installed on the server and cannot be created or deleted through VFM.
- 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 IE6 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 IE 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 will interfere with scripts used in VFM as part of the product installation as well as the application snapshot 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 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 (links 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.
- If the namespace is unavailable when a policy attempts to perform a namespace update during the final phase of a migration, the policy results will report that no links were updated.

  Workaround: Set the “Pause after this step” option to “always.” This allows you to verify the results of the namespace update before progressing with final phase actions.

- NFS file inclusions and exclusions in VFM policies might not function correctly.
- VFM performs a final copy during the final phase of data migration if data is copied during the initial or incremental phases.

VFM 6.0 Known Upgrade Issues

Known issues

This section describes issues encountered when upgrading to VFM 6.0 from previous versions. The following table provides a matrix of upgrades that are allowed and known issues for each version.

Installation option	VFM version from which you're upgrading to VFM 6.0		
	5.5	**5.6**	**5.8**
Client	No issues	No issues	No issues
Monitoring agent	See issue 1	See issue 1	No issues
Server	No issues	No issues	See issue 2
Client and server	No issues	No issues	No issues
Client and monitoring agent	No issues	No issues	No issues

Issue 1

When you try to upgrade a monitoring agent installed on a machine that is hosting a replication agent, the upgrade fails and you see the error message `Destination key already exists`.

Workaround: Perform the following steps.

Step	Action
1	Delete the 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 replication agent on the same machine on which you installed the monitoring agent.

Issue 2

When you try to upgrade the VFM server on a machine on which a local instance of MSDE (an instance without a name) is already installed, because the InstallShield was designed to search for an instance name during the upgrade, you might get the following error message:

```
'Error 27502 Could not connect to Microsoft SQL Server... does not
exist or access denied.' Call technical support for assistance.
```

Workaround: Perform the following steps.

Step	Action
1	Ensure there are no running replication policies and that the VFM console is closed.
2	Stop the VFM server service.
3	Move the VFM 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 service.
7	Verify that you can access the VFM console.
8	Close the console.
9	Restart the VFM upgrade process.

Known Issues Resolved in VFM 6.0.1

Resolved issues

This following known issues have been resolved since the release of VFM 6.0:

- The unformatted event history error message reported during UNIX replication agent deployment has been corrected.
- In some cases where the NETBIOS domain name differed from the fully qualified domain name in DNS, the root could be displayed twice in the VFM user interface. This 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.
- Snapshot 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 the roots in the view.
- 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 snapshot replication.
- An error message is no longer reported when you use differential replication and snapshots together in a policy.
- Storage system recovery policy alternate schedule handling has been corrected.
- VFM now copies the Brocade File Lifecycle Manager (FLM) alternate data streams when they are present in files.
- Folder exclusions specified in a policy using Snapshot replication now correctly exclude the specified folders.

Upgrading to VFM 6.0

Read before upgrading

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 ServerA and now you want to install the VFM server on ServerA as well, you must perform the following actions.

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

Renaming VFM components: Never rename a machine while the VFM server, replication agent, or monitoring agent is installed on it. 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 requirements for Installation options

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

Installation option	Steps
Server only	**1.** Stop the VFM server service. **2.** Follow the instructions in “Upgrading the Server or the Client and Server.”
Client and server	**1.** Stop the VFM server service. **2.** Follow the instructions in “Upgrading the Server or the Client and Server.”
Client only	**1.** Close the VFM client. **2.** Perform the upgrade.
Monitoring agent only	**1.** Stop the VFM server service. **2.** Perform the upgrade.
Monitoring agent and client	**1.** Close the VFM client. **2.** Stop the VFM server service. **3.** Perform the upgrade.
Replication agents	Follow the instructions in “Upgrading Replication Agents.”

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 prior to 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 the "**Use…schedule**" check box 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	Make an application snapshot to 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 machine. You can use a replication policy or Windows Explorer to manually copy the application snapshot to a remote location to have a second copy of the configuration.
6	Close the VFM client.
7	Perform the upgrade.

Upgrading Replication Agents

Steps

The replication agents used by VFM are upgraded automatically by the server during its normal status checks. You can perform the following steps for agents that do not get automatically upgraded.

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

If attempts to uninstall a replication agent using the Agent Management dialog box 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.

Step	Action
2	Using the command prompt, browse to the following location: `c:\Windows\system32\Brocade\VFM\ReplicationAgent`
3	Run the following command: **`net stop storagexreplicationagent`**
4	Run the following command: **`replicationagent.exe -uninstall`**
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: `HKEY_LOCAL_MACHINE\SOFTWARE\Brocade\VFM\ReplicationAgent`
8	Reboot the machine and then deploy the new replication agent, using the Agent Management dialog box.

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	Perform a clean installation of the VFM 6.0 NFS replication agent.
3	Open the VFM client.
4	On the Tools menu, click **Agent Management**, then **Deploy**.
5	Specify the name of the machine that will host the replication agent and the account that will run it, then click **OK**.

Step	Action
6	When the replication agent appears in the list, click the agent to verify the version information.

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). It 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. It 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. 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 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 *See* NFS export.

fault-tolerant DFS *See* 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 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. 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 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

See 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 *volume*, *leaf*, or *branch*.

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. *See also* 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.