NetApp
Go further, faster

NETAPP TECHNICAL REPORT

Best Practices Guide:
Virtual File Manager

Jai Desai, NetApp

March 2008 | TR-3661

ENABLING COMPREHENSIVE DATA MANAGEMENT SERVICES

This document describes a best-practices approach to deploying Virtual File Manager™ (VFM®) 6.0.

The NetApp Virtual File Manager applications are described, and information is provided on how NetApp Virtual File Manager automated management differs from other solutions available today.

TABLE OF CONTENTS

1 VFM 6.0 NEW FEATURES 3

2 UPGRADING TO VFM 6.0 3

2.1 SERVER AND CLIENT-SERVER UPGRADE FOR VFM 6.0 4

2.2 REPLICATION AGENTS UPGRADE STEPS FOR CIFS 4

2.3 REPLICATION AGENTS UPGRADE STEPS FOR NFS 5

3 PREINSTALLATION 5

3.1 CLIENTS IN NT DOMAINS 6

3.2 OFFLINE FOLDERS 7

3.3 CONSOLIDATION ROOTS 9

3.4 DFS BEST PRACTICES 9

4 POSTINSTALLATION 9

4.1 CREATE APPLICATION SNAPSHOT 9

4.2 ADD VFM TOOLS CMD SHELL TO START PROGRAM LAUNCHER 9

4.3 DEFAULT SETTINGS IN VFM 10

5 REPLICATION AND MIGRATION 16

6 NAMESPACE 17

6.1 APPLIANCE DISASTER RECOVERY POLICY 18

6.2 UNIX REPLICATION 19

7 HIGH AVAILABILITY 19

7.1 NAMESPACE AVAILABILITY POLICY 19

7.2 NAMESPACE BACKUP POLICY 19

7.3 APPLICATION SNAPSHOT SCHEDULE 20

8 CONFIGURING RECOVERY POLICIES 21

9 GENERATING REPORTS 21

10 MAKING VFM 6.O HIGHLY AVAILABLE 21

11 AUTOMATING BACKUPS OF VFM CONFIGURATION FILES 22

12 MANUALLY BACKING UP VFM CONFIGURATION FILES 23

1 VFM 6.0 NEW FEATURES

The following features are new or enhanced in VFM 6.0:

- **Phased migration** enables you to stage the data migration operation. You can automatically run repeated data copy operations before running the final copy and cut over users to the new location. You control when the migration operation moves from one phase to another (initial, incremental, and final phases). The feature is available for archival migration, migration, and storage load-balancing policies.
- **You can quickly add multiple targets to a DFS link** to clone an existing link target in order to add multiple targets to a DFS link at one time. A typical use of this feature is to quickly add multiple link targets pointing to WAFS edge nodes that are based on an existing link target pointing to a WAFS core node. Users from any remote office can be directed to the closest referral point of the data.
- **Agent management** enhances the management of replication and monitoring agents and the Brocade VFM server, including deployment credentials, upgrades, and removal of agents. This is especially useful in a large deployment of agents, which can then be managed from a single console.
- **Replication agent groups** enable you to add multiple replication agents to an agent group and assign the agent group to a data movement policy to distribute the data migration workload. This improves flexibility and throughput in many-to-one replication scenarios. Sharing the workload among multiple agents in an agent group enhances data movement parallelism and scalability is enhanced.
- **Namespace backup and restore supports new DFS attributes** introduced in Windows® Server 2003 release 2.

2 UPGRADING TO VFM 6.0

To upgrade existing installations of versions 5.5, 5.6, or 5.8 to VFM 6.0, use the VFM 6.0 installation media. The upgrade will maintain existing information from the previous installation, such as policies, namespace backups, events, and tool option settings.

Following are configuration methods in VFM and the steps to upgrade them:

- Server only—Follow the steps in the section entitled “Server and Client-Server Upgrade Steps for VFM 6.0.”
- Client and server—Follow the steps in the section entitled “Server and Client-Server Upgrade Steps for VFM 6.0.”
- Client only—Close the VFM UI and perform the upgrade.
- Monitoring agent only—Perform the upgrade directly.
- Monitoring agent and client—Close the VFM UI and perform the upgrade.
- Replication agents—Follow the steps in the section entitled “Replication Agents Upgrade Steps.”

2.1 SERVER AND CLIENT-SERVER UPGRADE FOR VFM 6.0

Use the following procedure to upgrade server and client servers to Brocade VFM 6.0:

1. Cancel all policies currently running or let them finish running. For a server-only installation, complete these tasks from a client connected to the server.

2. (Optional) Go through each policy and uncheck the **Use schedule** checkbox in the policy properties dialog to ensure that no scheduled policies will attempt to run during the upgrade.

3. Manually back up the namespace by right-clicking **Logical View > Backup** and selecting all the roots that are being used in the environment.

4. Take an NetApp snapshot to save the current configuration as backup. Use the **Tools > Take Application Snapshot Now** option in the VFM UI and save the existing configuration locally on the VFM server. You can then use a replication policy or Windows Explorer to manually copy the application snapshot to a remote location to have another copy available.

5. Close the VFM UI.

6. (Optional and intended for large environments in which the VFM server is busy)
   Stop the VFM server service.

7. Perform the upgrade.

2.2 REPLICATION AGENTS UPGRADE STEPS FOR CIFS

All replication agents used by VFM on machines that are reachable will be upgraded automatically by the server during its normal status checks; however, you can follow these steps for any agents that do not get upgraded:

1. Close the VFM UI.

2. Restart the VFM server service using the service control manager and reopen the UI.

3. Open **Tools > Agent Management** to check the current version for all replication agents. Use the **Upgrade** option in Agent Management to upgrade all agents that remain to be upgraded.

4. If the upgrade fails when using Agent Management, try to uninstall the replication agent and redeploy it.

5. If uninstalling the replication agent fails using Agent Management, here are the steps to do it manually:

   a. Log on to the server running the replication agent.

   b. Using the command prompt, browse to:
      `<C:\WINDOWS\system32\Brocade\VFM\ReplicationAgent>`

   c. Run the command `replicationagent.exe –uninstall`.

   d. Delete the contents of this directory and exit the command prompt.

   e. Using the service control manager, verify that the VFMReplicationAgent service no longer exists.

   f. Verify that the registry key:
      `<HKEY_LOCAL_MACHINE\SOFTWARE\Brocade\VFM\ReplicationAgent>` does not exist. If it does, delete it.

g. Reboot the machine and then deploy the new replication agent using Agent Management.

2.3 REPLICATION AGENTS UPGRADE STEPS FOR NFS

Follow these steps to upgrade an NFS replication agent:

1. Uninstall the older replication agent version using the procedure shown in product documentation. Make sure to delete the application directory.
2. Perform a clean install of the VFM 6.0 NFS replication agent.
3. Run the configure command.
4. Open Agent Management in the VFM UI to make sure that there is a record of the NFS replication agent with the correct version information.

   NOTE: NFS replication agents in VFM 5.8 were supported only on RHEL3 and Solaris™ 8. NFS replication agents on VFM 6 are NOT supported on RHEL3 and Solaris 8. VFM 6.0 replication agents run on RHEL4 and Solaris 10.

The following is a matrix of supported upgrades to VFM 6.0 and known issues:

From version	5.5	5.6	5.8
Client	✓	✓	✓
Monitoring agent	✓	✓	✓
Server	1, 2, 3, 4, 6	1, 4, 5, 6	1, 2, 3, 4, 6
Client/server	1, 2, 3, 4, 6	1, 4, 5, 6	1, 2, 3, 4, 6
Client/monitoring agent	✓	✓	✓

NOTES:

1. The replication agent on the VFM server is not upgraded. It has to be manually upgraded using Agent Management.
2. The upgrade does not retain shell properties for appliances.
3. The upgrade does not retain replication agent throttling settings. It reverts to default settings.
4. The upgrade deletes the Application Data Directory content if it is under the installation directory; thus, all the policies and application settings are lost.
5. Client-only installation tries to connect to the VFM server on the local machine (which does not exist). If this error occurs, manually point to the VFM server you want to connect to.
6. If the VFM upgrade installer fails to stop the server service in a timely fashion and the upgrade fails, continue with the roll-back process. Restart the VFM server service and restart the upgrade process.

NOTE: VFM application snapshots can be imported only into the same version of VFM in which they were created. VFM does not support taking a snapshot with one revision of the product and importing it into another revision of the product.

3 PREINSTALLATION

Here are tasks to perform before you start to install VFM 6.0:

- Identify the machines that will host VFM components (UI, server, replication agents) and validate network connectivity, name resolution, available disk space, and machine identity, including domain membership.

- Identify or create the service account that will be used by the VFM server and replication agents. This account must have the required permissions listed in the VFM documentation for managing the namespace and transferring data for migrations or replication, as well as for being a member of the local administrator's group on the machines in which VFM components will be installed. It is a best practice to run the VFM server service as a domain user who is a member of the local administrator's group on the VFM server and all other servers from/to which data will be transferred.

- NetApp does not recommend running the VFM server as a domain administrator, because its password may have to be changed. This change would cause extra work for the IT administrators when they have to update passwords for the VFM server, any monitor servers, and all servers on which replication agents have been deployed.

- Verify that no other processes are using TCP ports 6001, 6002, or 6005 on machines in which VFM or its replication agents will be installed. Some common applications that use ports in this range include X-Windows and Microsoft® Exchange Server components.

- If the Windows Server 2003 Security Configuration wizard was run on the system prior to the VFM installation, it is possible that ports required by VFM were locked down by the wizard. The ports required by VFM components must be unlocked before the VFM installation is performed. Windows Server 2003 locks down registry access in some configurations. Check `Administrative Tools > Local Security Settings > Security Options > Network access`. Remotely access registry paths and subpaths to be sure that registry paths required by VFM are accessible over the network and that the remote registry service is running on the system.

- Verify that RSH is enabled on any NetApp appliances that will be managed by VFM. If SSH will be used to communicate with the appliances, ensure that it is configured both on the appliance and in VFM. Verify that forward and reverse DNS lookups are accurate for systems in which VFM components are to be deployed.

- Determine which applications are accessing data that is to be incorporated in the namespace. How will the introduction of the namespace affect these applications? If a consolidation root is to be implemented, are applications connecting to the servers to be consolidated via other protocols such as FTP or Web servers? How will these applications be affected by the machine rename inherent in creating a consolidation root?

- Determine the types of client machines that are accessing the data to be included in the namespace. DOS, Mac® OS, Win9x, and NT4 clients all have special considerations that must be taken into account as part of the move to a namespace. DOS clients do not support DFS. Mac OS requires software such as Thursby Dave in order to access a DFS namespace. Win 9x and NT4 clients, while containing a base level of DFS awareness, may benefit from software updates such as the AD (Active Directory) client pack available from Microsoft (if these have not already been installed).

3.1 CLIENTS IN NT DOMAINS

When a Windows 2000/2003 DFS server is set up in an environment in which the clients accessing it are in an NT domain, site awareness should be disabled on the DFS server. If this is not done, a five-second delay will occur before the client is given a referral as the DFS server tries in vain to query the Active Directory to obtain a SITE referral. In an AD environment, this information would be used to refer clients to resources that are closest on the network to the requesting client.

Microsoft added new functionality to the DFS service in Windows 2000 SP4 to address this problem. To bypass the DFS site discovery process in SP4, you can set a new registry key as follows.

1. Start Registry Editor.
2. Locate and click the following key in the registry: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dfs\Parameters`
3. On the Edit menu, click **Add Key**, and then add a REG_DWORD key named DfsDisableSiteAwareness.
4. Set the value to 1 to enable the new functionality, or set the value to 0 to disable the functionality (or delete the DfsDisableSiteAwareness key), so that Windows 2000 returns to the default behavior of searching for site coverage.

3.2 OFFLINE FOLDERS

Offline folders are not supported with DFS for all Windows clients. Review the link and table below to determine whether contingency plans must be made.
http://www.microsoft.com/windowsserver2003/community/centers/fileservices/dfsfaq.mspx?pf=true

Q: Can I use DFS with Offline Files and redirected My Documents folders?

A: Using DFS, roaming profiles, Offline Files, redirected My Documents, and FRS is supported in the following scenarios (see below for the corresponding number references):

Scenario	Client OS	DFS Only	DFS and Offline Files	DFS and FRS	DFS, Offline Folders, and FRS
Roaming Profiles	Windows NT 4.0	N/A (1)	N/A (2)	N/A (1)	N/A (2)
Roaming Profiles	Windows 2000	Yes (3)	No (4,8)	No (5)	No (4, 5, 8)
Roaming Profiles	Windows Server 2003	Yes (3)	No (8)	No (5)	No (5, 8)
Roaming Profiles	Windows XP	Yes (3)	No (8)	No (5)	No (5, 8)
Redirected My Documents	Windows NT 4.0	Yes	N/A (2)	No (6)	N/A (2)
Redirected My Documents	Windows 2000	Yes	No (8)	Not recommended (7)	No (8)
Redirected My Documents	Windows Server 2003	Yes	Yes (9)	Not recommended (7)	Not recommended (7, 9)
Redirected My Documents	Windows XP	Yes	Yes (9)	Not recommended (7)	Not recommended (7, 9)
Collaboration Shared Folder	Windows NT 4.0	Yes	N/A (2)	Depends (10)	N/A (2)

Scenario	Client OS	DFS Only	DFS and Offline Files	DFS and FRS	DFS, Offline Folders, and FRS
Collaboration Shared Folder	Windows 2000	Yes	No (8)	Depends (10)	No (8)
Collaboration Shared Folder	Windows Server 2003	Yes	Yes (9)	Depends (10)	Yes (9, 10)
Collaboration Shared Folder	Windows XP	Yes	Yes (9)	Depends (10)	Yes (9, 10)
Publishing Shared Folders	Windows NT 4.0	Yes	N/A (2)	Yes	N/A (2)
Publishing Shared Folders	Windows 2000	Yes	No (8)	Yes	No (8)
Publishing Shared Folders	Windows Server 2003	Yes	Yes (9)	Yes	Yes (9)
Publishing Shared Folders	Windows XP	Yes	Yes (9)	Yes	Yes (9)

NOTES:

1. Windows NT 4.0 profiles are stored in the user's My Documents directory.
2. The Offline Files feature is not available in Windows NT 4.0.
3. If the DFS root is a standalone root in a remote site or a domain-based root with no local targets, the profile might fail to load. To work around this issue, disable slow link detection or install a redundant root target at each client site. For more information, refer to Microsoft Knowledge Base article 830856, “A Roaming Profile Is Not Loaded from a DFS Share.”
4. Roaming profiles should not be enabled for Offline Files. For more information, refer to Microsoft Knowledge Base article 287566, “The Cache Option for Offline Files Must Be Disabled on Roaming User Profile Shares.”
5. Roaming profiles that are replicated via FRS to multiple link targets might lead to data loss (because of FRS conflict resolution) if a user logs in to multiple workstations, makes changes to the same file on different targets, and then logs off all workstations.
6. Windows NT 4.0 profiles are stored in the user's My Documents directory. This is equivalent to issue 5.
7. If there is replication latency between link targets, users' data might be out of date on the other link target, causing users to be confused if they ever fail over to another link target.
8. Enabling Offline Files on DFS link targets is supported only on client computers running Windows XP and Windows Server 2003. For more information, refer to Microsoft Knowledge Base article 262845, “Support for DFS-Based Shares for Offline Files.”
9. Administrators must not enable Offline Files on a path with the same first component as a path used for roaming profiles. For example, if roaming profiles are stored on a domain root named

`\\Domain\Roam`, Offline Files should not be enabled for a DFS root named `\\Domain\Project`. Similarly, if roaming profiles are stored on a stand-alone root or regular shared folder, such as `\\Server\Roam`, Offline Files should not be enabled for a path such as `\\Server\Other`. Offline Files treats the first component of the path name as if it was a server and caches everything under that "server." In the `\\Domain\Roam` and `\\Domain\Project` example above, enabling Offline Files for `\\Domain\Project` would result in the roaming profiles being cached by Offline Files as well.

10. FRS does not provide distributed file locking. Depending on the update patterns of users, the lack of distributed locking might cause one user's update to override another user's update. If the collaboration is such that end users are not writing to the same files simultaneously, this most likely would not be an issue.

3.3 CONSOLIDATION ROOTS

When implementing consolidation roots, take care to fully enumerate all applications that might be accessing the file servers to be consolidated. If these applications access the file servers directly (by IP address or DNS name for services other than file services), plan to change the method used to access the services.

3.4 DFS BEST PRACTICES

Administrators planning a namespace implementation should familiarize themselves with the following Microsoft documents:

- Distributed File System Technology Center
  http://www.microsoft.com/windowsserver2003/technologies/storage/dfs/default.mspx

- Distributed File System: Frequently Asked Questions
  http://www.microsoft.com/windowsserver2003/techinfo/overview/dfsfaq.mspx

4 POSTINSTALLATION

4.1 CREATE APPLICATION SNAPSHOT

Immediately after installing VFM, create an application snapshot of the clean, empty database to prevent having to do a complete install to get back to a pristine state that you might need during the learning and implementation phase. Should the need ever arise, the empty application snapshot can be imported in a shorter time than it takes to uninstall and reinstall the application. At this time, decide where you want to place the application snapshots so that your backup process will pick them up. A suggested location is `C:\VFM\` with a name such as "`%date%Empty`." The VFM directory can be used later to store reports, scripts, and so on.

4.2 ADD VFM TOOLS CMD SHELL TO START PROGRAM LAUNCHER

To make it easier to go to the VFM tools directory for importing an application snapshot, add a "cmd" link to the Start Program Launcher.

1. Use MS Explorer to navigate to:
   `C:\Documents and Settings\All Users\Start Menu\Programs\Brocade\Tapestry VFM`

2. Add a link called "VFM Tools in cmd shell" with target "`%SystemRoot%\system32\cmd.exe /f:on`" that starts in "`C:\Program Files\Brocade\Tapestry VFM\Tools\Export.`"

Then it will be easy to get to the export directory by selecting `Start > All Programs > Brocade > Tapestry VFM > VFM Tools` in cmd shell.

4.3 DEFAULT SETTINGS IN VFM

Set up best practice default settings in the VFM client console by selecting `Tools -> Options`. Then proceed down each option and adjust settings as follows:

NOTE: Not all options are referenced, only the ones deemed important to mention. Also, only new policies created after updating these settings are affected—even for subsequent updates beyond this initial pass.

4.3.1 User Options

Check the following options to enable them.

- Show tool tips
- Close status windows on success
- Show empty admin folders
- Auto refresh SnapMirror info (300 sec)
- Auto refresh filer events (300 sec)

4.3.2 System Options

- RSH and SSH settings and credentials (only needed if you are managing NetApp appliances with VFM and all user/password combinations are the same across all appliances).
- Enable Auditing if you want to write VFM events to an NT event log. See the VFM online help under the `Troubleshooting > Event ID` section for more information to help with this decision.
- Change the SNMP community string from the default of "public" only if another string is used on the appliances. The SNMP community string is used in identifying and then communicating with NetApp appliances. If the community string on appliances is other than the default of "public," the SX administrator needs to configure the right community string in VFM to identify systems as NetApp appliances.
- The recommended minimum level of application security is enabling "Admins" to have full control of the VFM application and then removing the "Everyone" group from having access to the same.
- Set up an application snapshot schedule. Refer to the "High Availability" section below.

4.3.3 Reporting

- Reporting**—**Must be enabled here or these options will be disabled (grayed out) when creating reports later on.
  - Enable report archiving, keeping five archives.
  - Output format—Enable Publish Report option
  - Enable the reporting engine to deploy replication agents. By selecting this option the data collection for a given Windows server can be done by the replication agent local to that server instead of across the network from the VFM server.
- Report publishing:
  - Enable Report Publishing and enter the default directory in which to publish reports.

4.3.4 Archival Migration

- Task options:

  - Uncheck “Automatically add migration tasks for migration candidates.”
  - Uncheck “Automatically delete completed tasks.”
  - Check “Calculate total size for migration candidates.”
    NOTE: Add size and size-on-disk columns to policy properties, migration candidates’ view. They are not included in the default view.

- Replication options:
  - Enable “Include subfolders.”
  - Disable “Delete orphan files,” because the data will generally not be in use.
  - Enable “Copy in place.”
  - Disable “NTFS change journal.”
  - Set “Copy files only if destination is older or missing.”
  - Retry failed file opens 0 times at 0-second intervals.
  - Event details—List only files with errors.
  - Agent options—VFM selects.
  - Disable “Replication differencing.”
  - Replication security:
    - Copy security descriptor only if target does not exist.
    - Process local trustees:
      - Check “Translate SID.”
      - Check “Create local group.”
      - Check “Translate to local admin group.”
  - Uncheck “Allow loss of security info.”
  - Replication attributes:
    - Match everything.
    - Uncheck **“**Preserve last access time ON SOURCE” since we are moving the data and none will be left behind on the source shares.
  - Incremental and final phase schedules:
    - Should be set manually based on the needs of the policy.
    - Cutover from incremental to final phase should always be manual.

4.3.5 Disaster Recovery

- Uncheck “Automatic failover.”
- Search options—Leave all options unchecked for now.
- Target monitoring schedule—Set to monitor every five minutes.

- Resources monitoring options—Check find new links and find new qtrees options.
- Resources monitoring schedule—Leave at 10-minute interval.
- Agent options—VFM selects.
- Replication options:
    - Enable “Include subfolders.”
    - Disable “Delete orphan files” until you fully understand the effects of this option.
    - Enable “Copy in place” if you have high-speed links.
    - Disable “NTFS change journal.”
    - Set “Copy files only if destination is older or missing.”
    - Retry failed file opens 0 times at 0-second intervals.
    - Event details—Set to list only the files that encounter errors.
    - Disable “Replication differencing.”
- Replication schedule—Deselect “Use replication schedule.” This option should be enabled on a per-policy basis after you have added links to the policy and configured the link target ordering in the policy.
- Replication security:
    - Copy security descriptor each time the file or folder is copied.
    - Process local trustees.
        - Check “Translate SID.”
        - Check “Create local group.”
        - Check “Translate to local admin group.”
    - Uncheck “Allow loss of security info.”
- Replication attributes:
    - Match everything, but set the archive attribute in case the destination ever contains a restore of a backup to tape for a baseline data copy. By default, VFM considers file attributes when deciding if source and destination files are different. Setting the archive attribute prevents copying of data when the only difference between the source and destination files is the attribute.
    - Check “Preserve last access time ON SOURCE” because data will still be on the source for replications.
      NOTE: This may cause a slight performance impact, but is probably worth it if an Information Lifecycle Management (ILM) strategy is planned in the future and the access date will be used to judge the age of a file.

4.3.6 Migration

- Migration is broken into phases to make it easy for the admin to perform initial phase, incremental phase, and final phase actions.
- Migration actions:

  - In the initial phase, select “Perform a Baseline Copy.”
  - Specify the schedule at the time you create the policy.
  - In the incremental phase, select “Never advance tasks automatically.” Tasks will advance to the final phase by manual intervention.
  - Check “Update DFS by retarget links with pause only on error.”
  - Check “Prevent User Connections with pause only on error.”
  - Check “Do final replication prior to deleting the source share.”
  - Uncheck “Delete the source data.”
  - Uncheck “Stop sharing the source share.”

  NOTE: Leave the last two options to be enabled later on a per-policy basis.

- Replication options:
  - Enable “Include subfolders.”
  - Disable “Delete orphan files” until you fully understand the effects of this option. Once you are comfortable with this option, it should be enabled because data may be in use and migration may take a few passes to get a baseline plus any incremental changes to the source data.
  - Enable “Copy in place.”
  - Disable “NTFS change journal.”
  - Set “Copy files only if destination is older or missing.”
  - Retry failed file opens 0 times at 0-second intervals.
  - Event details—Set to list only the files that encounter errors. Do NOT turn on “List all files” because this will slow down data movement, and sometimes it generates an XML file that is difficult to view.
- Disable “Replication differencing.”
- Replication security:
  - Copy security descriptor only if target file or folder does not exist.
  - Process local trustees:
    - Check “Translate SID.”
    - Check “Create local group.”
    - Check “Translate to local admin group.”
  - Uncheck “Allow loss of security info.”
- Replication attributes:
  - Match everything, but set the archive attribute in case the destination ever contains a restore of a backup to tape for a baseline data copy. By default, VFM considers file attributes when deciding if source and destination files are different. Setting the archive

    attribute prevents copying of data when the only difference between the source and destination files is the attribute.

    - Check “Preserve last access time ON SOURCE” because data will still be on the source for replications.
      NOTE: This may cause a slight performance impact, but is probably worth it if an Information Lifecycle Management strategy is planned in the future and the access date will be used to judge the age of a file.

4.3.7 Namespace Availability

- Check “Synchronize after scanning.”
- Monitoring schedule—Leave at every 12 hours as a default.

4.3.8 Storage Load Balancing

- Check “Automatically add migration tasks” for data move suggestions.
- Replication options:
    - Enable “Include subfolders.”
    - Enable “Delete orphan files” because data may be in use.
    - Enable “Copy in place.”
    - Disable “NTFS change journal.”
    - Set “Copy files only if destination is older or missing.”
    - Retry failed file opens 0 times at 0-second intervals.
    - Event details—List only files with errors. Do not select “List all files.”
- Disable “Replication differencing.”
- Replication security:
    - Copy security descriptor only if target file or folder does not exist.
    - Process local trustees:
        - Check “Translate SID.”
        - Check “Create local group.”
        - Check “Translate to local admin group.”
    - Uncheck “Allow loss of security info.”
- Replication attributes:
    - Match everything.
    - Uncheck “Preserve last access time ON SOURCE” since the data will be moved and none will be left behind on the source shares.

4.3.9 Namespace Backup

- Check use schedule and perform daily backups, keeping 30 daily backups.
- Note that backups are stored in the database.

4.3.10 Namespace Creation

- Check “Automatically modify namespace after scanning.”
- Uncheck “Remove links whose shares no longer exist” to start with the selected string.
- When searching for shares, set “Detect shares not already targeted” from this policies folder.
- Monitoring schedule—Leave at default of every 12 hours.

4.3.11 Replication Policy

- Replication options:
  - Enable “Include Subfolders.”
  - Enable “Delete orphan files as data may be in use.”
  - Enable “Copy in place.”
  - Disable “NTFS change journal.”
  - Set “Copy files only if destination is older or missing.”
  - Retry failed file opens 0 times at 0-second intervals.
  - Event details—Set to list only files that encounter errors.
- Disable “Replication differencing.”
- Replication security:
  - Copy security descriptor each time the file or folder is copied.
  - Process local trustees:
    - Check “Translate SID.”
    - Check “Create local group.”
    - Check “Translate to local admin group.”
  - Uncheck “Allow loss of security info.”
- Replication attributes:
  - Match everything, but set the archive attribute in case the destination ever contains a restore of a backup to tape for a baseline data copy. By default, VFM considers file attributes when deciding if source and destination files are different. Setting the archive attribute prevents copying of data when the only difference between the source and destination files is the attribute.
  - Check “Preserve last access time ON SOURCE” because data will still be on the source for replications.
    NOTE: This may cause a slight performance impact, but is probably worth it if an Information Lifecycle Management strategy is planned in the future and the access date will be used to judge the age of a file.

4.3.12 Snapshot Scheduling (for NetApp Appliance Snapshots)

- VFM settings:
  - Check “Use VFM-initiated snapshot schedule” and keep four snapshots.

- Appliance settings:
  - Uncheck “Manage filer-initiated snapshot schedule.”

5 REPLICATION AND MIGRATION

The following is a list of best practices for VFM replication and migration activities.

- Avoid configuring overlapping data movement sources or destinations (multiple shares hosted in the same directory hierarchy) because multiple replication processes will attempt to copy the same data as many times as it is referenced. This results in interference that can cause the policy to fail (i.e., the same files being written simultaneously).
- Avoid configuring multiple data movement policies into a common destination directory structure because they may interfere with one another if file and path names are identical.
- Think about locked files on your sources and destinations. The snapshot replication option integrates with Windows Server 2003 VSS snapshots and NetApp appliance snapshots to allow replication of locked files. Files such as Outlook PST files are typically locked while Outlook is running. MS Access files are also locked when open, while MS Word and Excel docs are only locked in read-only mode to the second accessing process.
- Virus scanning software can greatly slow replication throughput and in some cases can cause locked file errors during the transfer. It is best to disable virus scanning software during migrations or replications.
- Think about network infrastructure prior to beginning a large transfer or migration. Is the available bandwidth suitable to transfer the data in the desired amount of time?
- Be aware of path lengths, because some systems impose limitations on the length of paths that can be manipulated on the system. If users access data through shares of directories that are deeper down in the directory tree and then a migration is attempted using a share at the root of the directory tree, it may be possible that paths will be too long for the underlying storage system to handle.

  WORKAROUND: Transfer data using one of the shares farther down in the directory tree rather than a share at the root of the directory tree. VFM will handle the maximum path length supported by Microsoft as it copies using the file functions in kernel32.dll, most of which can be extended to support a path length of 32,767 characters by prepending the path with \\server\.
- Think about where the replication agent that is doing the work for the replication (that is, proxy for non-Windows boxes, fan-in, and fan-out considerations) will reside. When multiple-source machines go to the same destination machine, it is best to use the replication agent on the source. When differential replication is turned on across slow links, then agent groups should be used as proxies in the data center.
- Agent groups share the load via a round-robin. The algorithm is not based on how busy the agent is. It is based on the number of tasks in the pipeline of the agent. Generally, an agent can handle the replication from 20 servers.
- Consider how permissions are structured on the source files and whether local trustees (local users and groups) are an issue. VFM will create local groups on the destination, but not local users.

  NOTE: Local trustee processing is not supported when the data source is on a DC. Remember, Windows does not support local users and groups on DCs.

- Think about how NTFS security is set on the source and destination directories and how NTFS permission inheritance will affect file permissions on both the source and destination. If VFM is not able to take/have full control of the files on the source and destinations, it will only partially complete the tasks it is given.

- Think about manifest settings and use the List All Files setting in data movement policies sparingly to avoid creating huge manifests. NetApp typically recommends using the List Only Files with Errors setting. List All Files has significant performance impact and should be used only with small data sets.

- Determine whether there will be network outages during the planned transfer time. If a reboot occurs during a replication, the transfer will be disrupted.

- In Migration Policies, for which the source machine is to be retired, it is better to clear the checkbox for Preserve Access Time on Source.

- In some situations in which there are extremely slow links, it may be beneficial to do a baseline copy outside VFM. For example, it is possible to back up the files to a DVD and restore on the destination. Then VFM can pick up the replication and continue from that point onward.

- A Migration Policy is designed to be run in three phases: initial, incremental, and final. For example, you may want to run the Migration Policy on Friday night and let it run all weekend. You may want to run the incremental backups every night from Monday through Friday. The following weekend, you may want to do the cutover into the final phase.

- Namespace updating is a critical feature of a Migration Policy. It is good practice to always pause after this step and verify the changes made. If a DFS root is unavailable to the VFM server when the policy runs, the namespace will not be updated. Care should be taken to make sure that DFS links get updated before hiding the source share, deleting the source data, and so on.

- Perform a Namespace Backup before starting a Migration Policy. This allows the administrator to know what a namespace looked like prior to the migration and provides a vehicle to restore the namespace.

- Do not turn on Byte-Level Replication (BLR) on a LAN. BLR is best used when there are slow links in the WAN, because it sacrifices CPU cycles on each side to optimize the network.

6 NAMESPACE

The following is a list of best practices for VFM namespaces.

- When designing a domain-based root, create the root first as a standalone DFS root and do all the dragging and dropping of links against the standalone root first to optimize performance. Later, when the namespace is fully created, back it up with VFM, delete it, create a new domain-based root, and restore the backup to the domain-based root.

- Think about namespace size (also known as “link count”), bearing in mind Microsoft’s recommendations. Refer to the document titled “Deploying DFS Facts Summary.”

- Think about location of DFS root servers in relation to clients accessing the namespace. Begin with a DFS root server in every location where there is a DNS server. The reason for this is that the DFS referral mechanism is analogous to the DNS referral—a location for a resource is requested of a server (DFS or DNS) and then cached.

- Consider the share permissions. Windows 2003 creates shares with permissions defaulted to everyone read-only. After creating a new DFS root, be sure to add the VFM service account to the share permissions and give it full control. This will allow VFM to perform logical directory operations on the root or root replica. It is also a good practice to ensure that all other users, including admins, only have traverse and/or read access to the DFS root share and all subfolders to prevent any data from being placed in the root folders.

- Ensure that the share name of any root target matches the name of the root itself.
- Think about whether a domain or standalone root is more suitable.
    - Microsoft recommends a maximum of 5,000 links for a domain-based root while 10,000 to 50,000 links are allowed for a standalone root, depending on the OS on the hosting server.
    - Active Directory is required for a domain-based root.
    - Creating and managing a domain-based root requires domain admin privileges by default. Hence, the VFM server can be run as a domain admin (not recommended—refer to the "Preinstallation" section) or VFM can be run as a domain user who is a member of the local administrator's group on the VFM server and all other servers from/to which data will be transferred. NetApp recommends the latter and in the case of managing a domain-based root, but the VFM service account must be given permission to update the Active Directory object for the root. The object is Active Directory Users and Computers' > %DOMAIN% > System > DFS-Configuration.
    - Two alternatives to a domain-based root that also provide some degree of high availability are:
        - Installing a DFS root on a MS Cluster server with a VFM namespace high-availability policy to keep a backup root on another server in case the cluster becomes unavailable.
        - Installing a DFS root on two servers, using a VFM namespace high-availability policy along with round-robin DNS such that the DFS referrals for clients could come from either of the synchronized root servers.
- If you want to deploy a WAFS solution, you can use the Clone Link functionality to add multiple targets to a DFS link. The best way to accomplish this is to add a link target to the back-end file share. Then, add a replica to one WAFS edge node. Using that replica, you can clone the link target by replacing the UNC path with the names of the other WAFS nodes.
- Perform a manual backup of the namespace before running a Migration Policy.

6.1 APPLIANCE DISASTER RECOVERY POLICY

Creating a new Appliance Disaster Recovery (DR) Policy to monitor a volume or qtree that has multiple shares as link targets under them could take a very long time. VFM has to quiesce and resync the SnapMirror copy for every share creation.

WORKAROUND: Create the link replicas before the Appliance DR Policy is created using the following procedure:

1. Create the SnapMirror copy for the source resource (volume/qtree) on the destination appliance.
2. Once the copy is in a SnapMirror state and the status is ”idle,” quiesce the copy and break it. This should be done on the destination appliance using a telnet session.
3. Create duplicate shares on the destination appliance for all shares on the primary appliance that are link targets referenced in the namespace.

4. Add these shares as the link replicas in the namespace.

5. Resync/resume the SnapMirror process.

6. Create the Appliance DR Policy in the normal way.

The new Appliance DR Policy picks up the existing link replicas on the destination appliance and makes them offline. Since there are no new shares to be created on the destination appliance, the SnapMirror relationship is not broken.

6.2 UNIX REPLICATION

Take into consideration the following information when planning a UNIX® migration/replication:

- Unsupported File Types—VFM UNIX Replication Agent ignores the following unsupported file types while replicating data: *Block special device*, *Character special device*, *Socket,* and *Named Pipe*. These files are generally application or environment specific and should be regenerated on the target machine if and when required. These files will be mentioned in the VFM console as ignored and the replication will continue for the rest of the data set.

- Object Mismatch Situation—When VFM UNIX Replication Agent encounters a situation in which the source contains one type of object (for example, a folder) and the destination contains a different object (for example, a symlink) with the same name, it behaves in one of the following ways:

  - "Delete Orphans" replication option is enabled—The UNIX Replication Agent will match the destination with the source. It will delete the different destination object first and copy the source object.

  - "Delete Orphans" replication option is disabled—The UNIX replication agent will report this situation as an error in the VFM console; skip past these files and move on with the rest of the replication.

- Replication agents do not run on RHEL3 and Solaris 8 platforms. You can still migrate data from these platforms by installing the replication agent on Solaris 10 or RHEL4 platforms and setting it as a proxy for the older platforms.

7 HIGH AVAILABILITY

High availability can be configured in VFM in the namespace availability and namespace backup policies and in the application snapshot schedule.

7.1 NAMESPACE AVAILABILITY POLICY

This policy mirrors or replicates the DFS root between a master DFS root server and a backup DFS root server on a schedule. It should be used for sites that do not have a domain-based root containing at least two member DFS root servers or replicas. For most sites a daily replication should suffice. For testing in the lab, set up a policy to replicate the root every two minutes; make some changes to the primary root and verify that these changes are propagated to the backup root server.

7.2 NAMESPACE BACKUP POLICY

This policy backs up the DFS root to the VFM database on a schedule to protect against corruption or loss of the DFS root because the root server[s] is down. *A good policy for most sites is a daily backup keeping the first 30 versions.* Coordinate the root backup such that it occurs just before the application snapshot. For testing in the lab, set up a policy to back up the root every two minutes; make some changes to the primary root, and verify that these changes are reflected in the root backups.

The root backups can be used to see where files were located before and after migrations with DFS link updates. This will be useful when a user wants to restore a file from backup (for example, from two weeks before) that has become lost or corrupted, even though a migration was done the week before. To users accessing data in the namespace, the file appeared to be in the same place both before and after the migration, so that is the path where they want the file restored. To find the physical location of this file from two weeks before so that it can be restored from tape, browse the DFS root backup in VFM and look at where the link was pointing at that time. Then restore the file to the new virtual path location.

7.3 APPLICATION SNAPSHOT SCHEDULE

This policy backs up the VFM database and associated files to protect against corruption or loss of application functionality. This includes disaster recovery share monitoring, policy-based data movement, and other events scheduled and implemented with VFM. For most sites, set this to once per day and keep the first 30 versions. *After the first month, a weekly backup that keeps 12 versions or 3 months' worth of data would be ideal*. Usually it is not necessary to enable the "include reporting database information in snapshot" option because this can add a lot of space to the application snapshot.

For testing in the lab, set up a policy to create an application snapshot every five minutes. Make some changes to the policies and verify that those changes are reflected in the different VFM application snapshot versions. Note that the loss of the VFM application service and/or database does not affect the DFS namespace managed by VFM. The users of the namespace will still have access to their data. Test this in the lab by stopping the VFM service followed by using MS Explorer to access the namespace.

8 CONFIGURING RECOVERY POLICIES

Links added to VFM Client Recovery policies will have the target that is alphabetically first in the list activated as the primary target for the link. You must reorder the link targets in the policy if the default link target chosen by VFM is not correct for your environment. You must also reorder the links if you move a link from one recovery policy to another. Enabling replication on a recovery policy before ensuring that the link targets are properly ordered can lead to loss of data.

9 GENERATING REPORTS

The idea behind reports is to have separate reporting databases within the MSDE or Microsoft SQL Server™ instance. Then for each reporting database, you select a scope of computers and shares from which to collect data, followed by a selection of attributes for those resources. Once the data is collected in each reporting database, you can generate reports through querying the collected information without having to go back out to the network to find the data. The best practice is to create a report group (really a database) for each of the report categories, that is, create report groups called "Admin," "Logical," "Physical," "File System," and, optionally, "NetApp."

Create reporting folders with the same names as the report groups and create reports related to the report folder category in their respective folders. This keeps the databases from growing too large (the MSDE limit is 2GB per database in an instance) with collected data and also keep the reports logically grouped.

Finally, go back and edit each report group to set the scope and attributes as desired. When doing this make sure that the attribute selection gathers only information related to the report group category (for example, for logical reports about the namespace, use a scope of one or more DFS roots only followed by an attribute selection of namespace properties and root blob size). Check the report group database sizes by looking in `C:\Program Files\Microsoft SQL Server\MSSQL$VFM` and observe the `SX_#.mdf` files in detail view. (Note that # represents an integer signifying one of the reporting databases.)

10 MAKING VFM 6.O HIGHLY AVAILABLE

The challenge in making VFM highly available is described as follows: VFM enables the administrator to configure standby servers to enable the primary VFM server to perform failover/failback operations. The method of incorporating the application snapshot feature to export data from the primary server directly to a known location on the secondary server (standby server) such that the configuration data from the primary server can be imported to the standby server, returning VFM to a known state should the primary VFM server become temporarily unavailable.

The process requires the installation of the VFM server software on both a primary and standby server. The backing up of VFM configuration files can be completed automatically or manually:

- VFM enables scheduling of automatic snapshots of the VFM configuration.
- VFM allows the administrator to manually create application snapshots of the VFM configuration information at any time.
- VFM command-line utilities enable you to manually export VFM configuration information when the VFM console is not available.
- If the primary server on which VFM is installed becomes unavailable, all that is required is the import of the configuration files on the machine that will act as the VFM standby server—at which point the backup machine takes ownership of all monitoring agents in the imported configuration data.
- When the primary VFM machine becomes available, the administrator has the option of taking a manual snapshot of the current VFM configuration information from the S\standby server or using the export.bat command-line utility to export the VFM configuration files from the backup machine and import them back to the primary VFM machine.

NOTES:

- VFM should not be installed on the same machine as FLM. FLM is resource intensive and will negatively impact VFM performance.

- Prior to implementing the following steps, it is advisable to create an initial application snapshot of the standby server for use in restoring that machine to its initial state once the primary server is available.

  1. Ensure that VFM is installed and properly configured on both the primary and standby server machines.

  2. Run the 'MSSQL$VFM' service as a local system for security purposes.

  3. Export the VFM configuration on the standby server in order to have a baseline configuration to return to following failover/failback activities.

The following sections explain how to set up manual or automated backups for VFM configuration files.

11 AUTOMATING BACKUPS OF VFM CONFIGURATION FILES

To automate backups of VFM configuration files on the primary and standby server:

1. On the Tools menu, click **Options**.

2. Under System Options, click **Application Snapshot Options**.

3. Select the **Automatically snapshot the application** option.

4. Type a local destination where you want to save the configuration files in the edit box labeled **Snapshot save location**.

   It is important to specify a local path on the machine to save the configuration files.

5. Enter the number of snapshots to retain in the **Number of snapshots to keep** box.

6. (Optional) Type the UNC path of the batch file that you want to run before and after the snapshot process.

7. Enter how frequently you want to back up the files and click **OK**.

8. Create a replication policy to copy the application snapshots from the local server to the remote machine hosting the standby server on a scheduled basis.

12 MANUALLY BACKING UP VFM CONFIGURATION FILES

Use the following method when you have access to the VFM client and the VFM server is running on the machine from which the configuration is to be exported:

1. On the Tools menu, click **Take Application snapshot now**.
2. Enter a local destination path where you want to save the configuration files. It is important that you specify a local path to save the configuration files.
3. Click **OK**.
4. Create a replication policy to copy the application snapshots from the local server to the remote machine hosting the standby server.

Use the following method when you do not have access to the VFM client or the VFM server is not running.

1. Close the VFM console.
2. On the machine from which the VFM configuration is to be exported, start a command prompt and change to the VFM installation directory where the export batch file is located (typically C:\Program Files\Brocade\Tapestry VFM\Tools\Export).
3. At the command prompt, type `export <directory name>, where <directory name>` is the local path to the folder in which you want to save the VFM configuration files.
4. Press **Enter** and respond to the prompts.
5. Copy the application snapshot manually (using Windows Explorer) to the machine hosting the standby server.
6. Once the export is completed, on the server to which you intend to import the configuration files:
   - Close the VFM console.
   - Start a command prompt and change to the VFM installation directory where the export batch file is located (typically C:\Program Files\Brocade\Tapestry VFM\Tools\Export).
   - At the command prompt, type `import <directory name>, where <directory name>` is the local path to the folder where the VFM configuration files were saved.
   - Press **Enter** and respond to the prompts that follow.
7. Open the VFM console on the standby (secondary) server and verify that the configuration has been properly imported.

NetApp™

www.netapp.com