Chapter 2

Administering File and Print Servers

File and print servers are sometimes the very reason organizations implement networks. For this reason, they are also often the very first servers to be put in place in a networked system. This is why they are the first specific server role examined in this book.

Administrative Activities

The administration of file and print servers is divided into three categories. These include File Services, Print Services and Cluster Services. Table 2-1 outlines the administrative activities that you must perform on an ongoing basis to ensure proper operation of the services you deliver to your user community. It also identifies the frequency of each task.

Procedure Number	Activity	Frequency
File Services		
FS-01	Available Free Space Verification	Daily
FS-02	Data Backup Management	Daily
FS-03	Shared Folder Management	Daily
FS-04	File Replication Service Event Log Verification	Daily
FS-05	Volume Shadow Copy Management	Weekly
FS-06	Distributed File System Management	Weekly
FS-07	Quota Management	Weekly
FS-08	Indexing Service Management	Weekly

Table 2-1. File and Print Service Administration Task List

Procedure Number	Activity	Frequency
FS-09	Data Disk Integrity Verification	Weekly
FS-10	Data Disk Defragmentation	Weekly
FS-11	File Access Audit Log Verification	Weekly
FS-12	Temporary File Cleanup	Weekly
FS-13	Security Parameter Verification	Weekly
FS-14	Encrypted Folder Management	Weekly
FS-15	Data Archiving	Monthly
FS-16	File Replication Service Management	Monthly
FS-17	Disk and Volume Management	Ad hoc
Print Services		
PS-01	Print Queue Management	Daily
PS-02	Printer Access Management	Weekly
PS-03	Printer Driver Management	Weekly
PS-04	Printer Sharing	Ad hoc
PS-05	Print Spooler Drive Management	Ad hoc
PS-06	Printer Location Tracking Management	Ad hoc
PS-07	Massive Printer Management	Ad hoc
PS-08	New Printer Model Evaluation	Ad hoc
Cluster Services		
CS-01	Clusters: Cluster State Verification	Daily
CS-02	Clusters: Print Queue Status Verification	Daily
CS-03	Clusters: Server Cluster Management	Weekly
CS-04	Clusters: Quorum State Verification	Weekly

Table 2-1. File and Print Service Administration Task List *(continued)*

You may not need to perform all of these activities because you don't use some of the services mentioned here. You may also use a different schedule. Remember to personalize the task list to adapt it to your environment.

File Service Administration

With Windows Server 2003, file service administration involves everything from formatting a new disk to integrating with the Active Directory to creating complex shared folder structures with the Distributed File Service. But, it is mainly focused on disks and the services Windows Server 2003 can support when dealing with storage.

Four main tools can be used to manage file servers:

- **Windows Explorer** because it gives access to both disks and shared folders.
- The **File Server Management** console because it is a single-purpose console that focuses on disks and shares.
- The `net share` command because it is a command-line tool that can be used to script sharing operations.
- The `diskpart` command because it is designed to manage disks, volumes, and partitions.

SCRIPT CENTER *The Microsoft TechNet Script Center includes a series of Windows Scripting Host (WSH) sample scripts that help you perform file and folder as well as disk and file system administration tasks. These scripts can be found at http://www.microsoft.com/technet/ treeview/default.asp?url=/technet/scriptcenter/filefolder/default.asp?frame=true and at http://www.microsoft.com/ technet/treeview/default.asp?url=/technet/scriptcenter/dfs/default.asp?frame=true. Because of this, script references will not be repeated in each file- or disk-related activity unless there is one specific script that addresses the task.*

FS-01: Available Free Space Verification

Activity Frequency: Daily

Checking for free space on a server requires a view of the actual disk drives located on the server. There are several

ways to do this, but the easiest is to simply open a Remote Desktop Connection (RDC) to the server whose drives you want to verify. If you haven't already done so, use **Procedure RA-01** to create an RDC link to each of the servers you want to verify or go to the Remote Desktop Web Connection page created in **Procedure RA-04**, and then proceed as follows:

1. Use the Global MMC Console to launch a **Remote Desktop** session to the server you want to verify and log in with your administrative credentials.
2. Use the **Windows Explorer** shortcut located in the **Quick Launch Area** to expand **My Computer**.
3. Click on the server's **data disks** and view available space by checking the **status bar** at the bottom of the Explorer window.
4. Note the available space for each data disk in your **Available Free Space Log**.
5. Close the **Explorer** when done.

Of course, if you have 500 servers, this procedure can become tedious. So you might prefer to use a more automated method. To do so, you can create a performance monitoring console that automatically tracks free disk space on all servers. This console will need access rights to performance counters on each server you monitor, so it is best to use the **Run As Shortcut** created in **Procedure GS-01** to launch the **Performance Monitoring Console** (**Start Menu | Administrative Tools | Performance**), and then proceed as follows:

1. Use the plus symbol (+) in the toolbar to add a counter.
2. In the **Select counters from computer** field, type in the name of the server you want to view.
3. Select **LogicalDisk** as the performance object and **% Free Space** as the counter.
4. Make sure you select the data disk drive(s) and click **Add**, and then **Close**.

5. When all the servers and disks are added, use **File | Save As** to place the console under your **My Documents** folder and name it **Free Disk Space.msc**. Use this console to view free space on all file servers from now on.

Finally, you can use a simple command-line tool to verify free disk space. It works on any system and can send its output to a text file. Use the following structure:

```
freedisk /S systemname /D drivename
```

where *systemname* is the DNS name of the remote server and *drivename* is either the drive or volume name you want to verify.

You can also use the `diruse` command from the Windows Server Support Tools to verify the amount of disk space used in each folder. To identify the space used on the C: drive, type:

```
diruse /m /* c:\ >filename.txt
```

This will include only top level folders, provide information in megabytes and pipe the information to a text file named *filename.txt*. In addition, you can use either local or remote folders (must be in UNC format).

SCRIPT CENTER *The Microsoft TechNet Script Center includes a script that helps you identify the free space on a disk. This script can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/dfs/ScrDFS10.asp?frame=true.*

FS-02: Data Backup Management

Activity Frequency: Daily

Windows Server 2003 offers a lot more functionality in this area, especially with the Volume Shadow Copy service. But, even though data backups are a lot easier to do with WS03, you should still take the time to make sure they have been performed properly. To do so, you need to view the backup log on each file server.

Use **Procedure BR-02** to review your data backup logs. If you find errors, determine if it is a critical file (data backup errors are on files in data drives only) and use the Windows Explorer to see why the file wasn't backed up.

FS-03: Shared Folder Management

Activity Frequency: Daily

Shared Folder Management refers to two main activities: the creation of new folders and the creation of new file shares. This may or may not be a daily activity for you; it all depends on your environment and the number of users you support. If you set it up right, this activity should be very straightforward.

SECURITY SCAN *You will need to set security permissions on these folders. Remember that NTFS permissions are final permissions. This means you should concentrate on these permissions first. This process is illustrated in Figure 2-1.*

To create new folders:

1. Use the Global MMC Console to open a **Remote Desktop Connection** to the appropriate server.
2. Launch the **Windows Explorer** (**Quick Launch Area** | **Windows Explorer**) and select the **D: drive** (all data should be on D: drive).
3. Locate the folder level where you want to create the new folder in the left pane. Right-click in the right pane of the Explorer, select **New, Folder** and type in the **name of the folder**. Choose a name that can double as folder and share name. Press ENTER when done. Repeat for each folder you require.
4. Apply appropriate NTFS security settings for each folder. To do so, right-click on each **folder name** and select **Properties**. Move to the **Security** tab. Add the **appropriate groups** and assign **appropriate security settings** to each group.

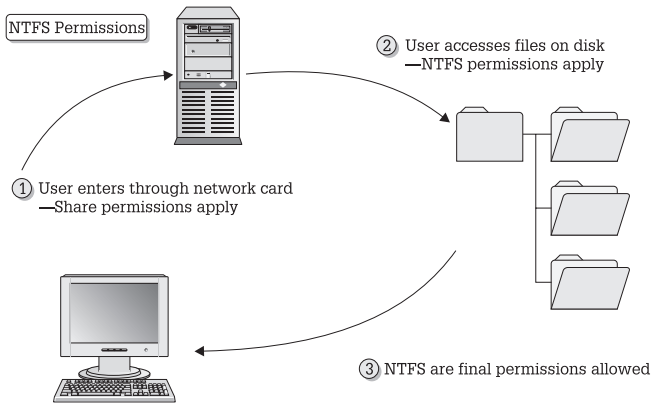


Figure 2-1. The file access security process

SECURITY SCAN *You should modify security settings on root folders because these settings are inherited whenever you create subfolders. This way, you will only need to fine-tune subfolder settings from then on.*

You can share folders in three ways: the *Windows Explorer*, the *File Server Management* console or the net share command. To share folders with the Explorer (since you just used it to create a folder):

1. Locate the folder you want —to share, right-click on it and select **Sharing**.
2. Identify the **name for the share**—if possible, the name of the folder—and type in a **description**.
3. Now set share permissions. If you set NTFS permissions properly, you can set share permissions to **Authenticated Users: Change**. Do so by clicking **Add**, locating **Authenticated Users** and checking the **Change** setting. Remove **Everyone** from the share security settings. Close the dialog box.

SECURITY SCAN *Remember that, by default, all shares are set to **Everyone: Read**. It is important to verify security settings every time you create a new shared folder.*

4. Next, set **Offline Settings**. By default all shares are set to allow users to determine if they want offline copies. Use the **Offline Settings** button to select the appropriate setting for this share.
5. Click **OK** when done. Repeat for each new share.

You're almost done. Now, the only thing left is to make the shares available to users. This is done through Active Directory.

To publish a share in Active Directory:

1. Open a Remote Desktop Connection on a **domain controller** and open the **Active Directory Users and Computers** console.
2. Locate the organizational unit you want to use to publish shared folders or create a **new organizational unit** and name it appropriately.
3. Now, move to the right pane and right-click to select **New, Shared Folder** from the context menu.
4. Type in the **name of the share** and the **path to the shared folder** (using Universal Naming Convention format or \\servername\sharename). Click **OK** when done. Repeat for each share you need to publish.

Once the shares are created, you will need to add a description and keywords to each. Folder descriptions are useful since they will help users identify the purpose of the shared folder. Keywords are also useful because users can search for shared folders by keyword instead of share name.

1. To enter both, view the **Properties** of each shared folder in AD.
2. Add complete descriptions to each share and identify its **Manager**.

3. To add keywords, click the **Keywords** button. Type the **keyword** and click **Add.** Click **OK** when done.
4. Close the dialog box when done. Repeat for each share you publish in AD.

TIP *Do not publish hidden shares (using the Share$ name format) because they will no longer be hidden. Any share that is published in AD will be visible to users.*

Your shares are now ready for access by users.

FS-04: File Replication Service Event Log Verification

Activity Frequency: Daily

The File Replication Service (FRS) is at the core of both the Distributed File System and Active Directory operations. Its proper operation must be verified daily. The best way to do this is to use the Global MMC Console you created in **Procedure GS-17** and follow much the same steps as outlined in **Procedure GS-03**.

1. Launch the **Global MMC Console** (**Quick Launch Area | Global MMC Console**).
2. Connect to the appropriate server (**Action | Connect to another computer**) and either type in the server name (\\servername) or use the **Browse** button to locate it. Click **OK** when done.
3. Move to the **FRS Event Log** (**System Tools | Event Viewer | File Replication Service**).
4. Identify any errors or warnings. Take appropriate action if either appears.

Make note of any corrective action you need to take. Use **Procedure GS-06** to log the different events you investigate each day.

FS-05: Volume Shadow Copy Management

Activity Frequency: Weekly

The Volume Shadow Copy service (VSC) is a very useful tool for system administrators because it provides users with the ability to restore their own files. It also provides the ability to create backups from copies or snapshots of production data letting you back up data without affecting production environments.

Shadow copies are a feature of disk drives. To verify the status of VSC:

1. Use the **Global MMC Console** to open a **Remote Desktop Connection** to the appropriate server and then open the **Windows Explorer** (**Quick Launch Area | Windows Explorer**).
2. Navigate to the data drive (drive D:) and right-click on it to select **Properties**.
3. Move to the **Shadow Copies** tab and click **Settings**.
4. In the Settings dialog box, click **Details**. This will display a dialog box outlining the volume shadow copies are located on, the amount of available space on the volume, and the amount of space used by VSC. Verify that enough space is available for the shadow copies and click **OK** to close the dialog box.

TIP *Shadow copies should be located on a dedicated volume. This makes sure the VSC service does not interfere with production service levels.*

5. Verify the **Maximum size** allocated to the VSC service and modify it if required.
6. You should also check the VSC schedule. Click **Schedule**, verify that everything is as it should be and click **OK** when done. The default schedule is usually appropriate for most environments.

7. Close the **Properties** dialog box when done, by clicking **OK**.

You should make sure that VSC Restores work properly. To verify VSC restores:

1. On your own computer, launch the **Windows Explorer** (**Quick Launch Area** | **Windows Explorer**).
2. Locate a shared folder you have access to and select a test file within this folder. Right-click on it to view its **Properties**.
3. Move to the **Previous Versions** tab and select the version of the file you want to restore and click **Restore**. It will give you a warning about overwriting newer versions. Click **OK** to proceed.
4. Close the Properties dialog box when done.

The file should be located in the folder you selected. While VSC does not replace backups, it offers user self-service for short-term file recoveries.

TIP *To be able to access previous versions of files, you must have deployed the Previous Versions Client to Windows XP PCs. The Previous Versions client is a Windows Installer file named TWCLI32.MSI. It is located in the %SystemRoot%\System32\Clients folder. Locate the appropriate version (32 or 64-bit) and deploy it to all users of Windows XP machines. In fact, it should be part of the basic build of all client systems.*

You can also use the `vssadmin` command-line tool to manage Volume Shadow Copies. For example, to list the shadow copies currently on a volume, type:

```
vssadmin list shadows
```

You can also pipe this command to a text file to capture the information more rapidly. The `vssadmin` command is very useful. It lists shadow copies, lists volumes eligible for shadow copies, creates and deletes shadow copies and more. For more information, simply type `vssadmin` at the command prompt.

FS-06: Distributed File System Management

Activity Frequency: Weekly

The Distributed File System (DFS) is one of Windows Server 2003's most powerful file services. It provides fully redundant file share access in either stand-alone or domain-based mode. Figure 2-2 illustrates the DFS creation process in either mode.

Use the DFS console to ensure the proper operation of this service.

1. Launch the **DFS console** (**Start Menu | Administrative Tools | Distributed File System**).
2. If the DFS root you want to manage is not visible, use the Action menu to connect to your DFS roots (**Action | Show Root**), locate the root you want to manage, select it and click **OK**.
3. To make sure the DFS share is operating properly, right-click on the **DFS share name** and select **Check status** from the context menu.
4. All root targets should show a status of *online*. If not, verify why the targets are not online and repair them (the server may be down).

TIP *DFS depends heavily on the Remote Procedure Call service. Make sure this service is up and running. Also, domain-based DFS roots must have synchronized clocks (to support replication and location of the root targets). Make sure all systems are synchronized with the PDC Emulator (this is normally the default in an Active Directory domain).*

The DFS console can also be used to modify the DFS configuration, add new targets, add new links, configure replication and so on.

Stand-alone DFS roots tend to be applied more often in server clusters. If you use server clusters and stand-alone

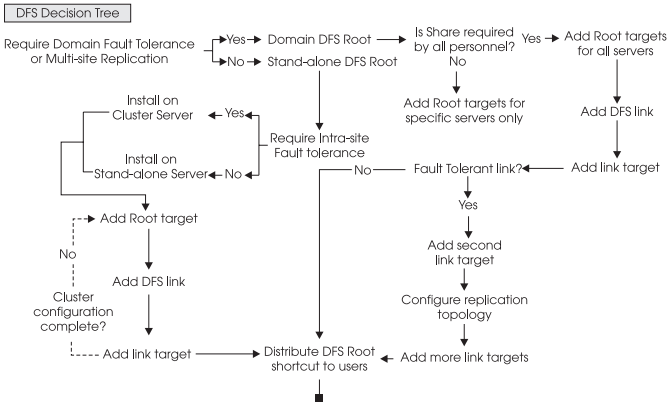


Figure 2-2. The DFS creation process

DFS roots, you will have the opportunity to reuse this procedure.

SCRIPT CENTER *The Microsoft TechNet Script Center includes several scripts that help you identify work with DFS. These scripts can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/dfs/default.asp?frame=true.*

FS-07: Quota Management

Activity Frequency: Weekly

The Windows Server 2003 Quota Service is also a feature of disk drives. To verify quota status:

1. Use the **Global MMC Console** to open a **Remote Desktop Connection** to the appropriate server and then open the **Windows Explorer** (**Quick Launch Area | Windows Explorer**).
2. Navigate to the data drive (drive D:) and right-click on it to select **Properties**.
3. Move to the **Quota** tab and click **Quota Entries**.

4. View all quota entries and verify how your users are making use of shared disk space.
5. You can view a user's individual settings by right-clicking on the user and selecting **Properties**. Close the Quota Entries window when done.

You can also import quota settings from another volume. If you need to do so (replacing a volume, moving data to a new volume), make sure you export the settings (**Quota | Export**) from the source volume before you import them (**Quota | Import**) into the destination volume.

SCRIPT CENTER *The Microsoft TechNet Script Center includes several scripts that help you identify work with quotas. These scripts can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/dfs/default.asp?frame=true.*

FS-08: Indexing Service Management

Activity Frequency: Weekly

The WS03 Indexing Service will index documents in the following formats:

- Text, HTML, Office 95 and later, Internet Mail and News, and any other document for which a filter is available

For example, Adobe Corporation provides an indexing filter for documents in the PDF format. This filter can be found at http://download.adobe.com/pub/adobe/acrobat/win/all/ifilter50.exe.

In addition each drive must be marked for indexing and the Indexing Service must be turned on. Drive marking is performed in the **Properties** dialog box for the drive under the **General** tab. This setting is turned on by default on all drives. Since data is located only on specific drives, you should uncheck it for system drives.

To verify that the Indexing Service is turned on, use the Global MMC Console (**Procedure GS-17**) to view the

service status (**Services and Applications | Services**). Make sure it is set to automatic startup.

To verify that the Indexing Service is working properly, search for a document you know is on the drive (**Start Menu | Search**).

FS-09: Data Disk Integrity Verification

Activity Frequency: Weekly

Because data is stored on drives and drives tend to be the major point of failure on any given system, it is important to verify that the volumes you use are regularly scanned for integrity.

To scan a disk for integrity, use the following command:

```
chkdsk volume: /f
```

where *volume:* is the name of the drive or volume you want checked. This command can be set as a **Scheduled Task** (see **Procedure GS-19**).

You can also perform this command through the graphical interface. Use **Windows Explorer** to locate the disk drive you want to verify, right-click on it, select **Properties**, move to the **Tools** tab and click **Check Now**.

TIP *This command can only be run in real-time on nonsystem volumes. Since CheckDisk needs exclusive access to a volume during verification, it can only run at server startup on system volumes.*

SCRIPT CENTER *The Microsoft TechNet Script Center includes two scripts that help you work with disk verifications. The first lets you run Chkdsk on a volume and the second tells you the status of Chkdks on a volume. These scripts can be found at http:// www.microsoft.com/ technet/treeview/default.asp?url=/ technet/scriptcenter/dfs/ScrDFS34.asp?frame=true and http:// www.microsoft.com/technet/treeview/ default.asp?url=/technet/scriptcenter/dfs/ scrdfs36.asp?frame=true.*

FS-10: Data Disk Defragmentation

Activity Frequency: Weekly

It is also important to defragment drives on a regular basis to improve performance and data access speeds.

To defragment a disk, use the following command:

```
defrag volume /v >filename.txt
```

where *volume* is the name of the drive or volume you want to defragment. Using the /v switch enables the verbose mode which can be piped into the file of your choice. This command can also be set as a **Scheduled Task** (see **Procedure GS-19**).

You can also perform this command through the graphical interface. Use **Windows Explorer** to locate the disk drive you want to verify, right-click on it, select **Properties**, move to the **Tools** tab and click **Defragment Now**.

FS-11: File Access Audit Log Verification

Activity Frequency: Weekly

One of the foremost responsibilities of a file system administrator is to make sure people access only those files they are allowed to. Therefore it is essential to enable file access auditing on data drives, especially if the data is either sensitive, confidential or secret.

File access auditing is enabled through Group Policy and must be specifically applied to the objects you want to audit. Use the following procedure:

1. Use the **Global MMC Console** to view the **Group Policy Management Console** (**Start Menu | Global MMC Console**).
2. Move to the **Group Policy Object** container (**GPMC | Forest | Domains | Domainname | Group Policy Objects**) and locate the GPO you want to modify. This policy may apply at the domain level or could

be focused on an organizational unit that stores all of the file servers. Right-click on the policy and select **Edit**.

3. Turn on the object access audit policy (**Computer Configuration | Windows Settings | Security Settings | Local Policy | Audit Policy**).
4. Next you must identify the folders you want to audit (**Computer Configuration | Windows Settings | Security Settings | File System**). To do so, you must use the **Add file** command, locate the folder you want to audit, click the **Advanced** button, move to the **Audit** tab, click **Add**, locate the group you want to audit (Everyone), and identify the events you want to audit for this group.

This is one of the rare opportunities where the Everyone group applies, because in fact you do not want to audit only Authenticated Users, but everyone who has access to the system.

5. Close all dialog boxes and the Group Policy Editor when done.
6. Use the **Global MMC Console** to view the results of the audit under **System Tools | Event Viewer | Security**.

TIP *Auditing object access creates a lot of entries. Be careful what you choose to audit and make sure your Security Event Log is set to an appropriate file size (**System Tools | Event Viewer | Security | Properties**).*

FS-12: Temporary File Cleanup

Activity Frequency: Weekly

Applications need to create temporary files to ensure that users do not lose their data as they work. These temporary files are normally removed when the application closes. Unfortunately, not all applications are so well behaved.

Thus, you must verify data disks for temporary or corrupt files to delete them on a regular basis.

You can do this interactively using the Disk Cleanup utility. Use the following procedure to do so:

1. Launch **Disk Cleanup** (**Start Menu | All Programs | Accessories | System Tools | Disk Cleanup**).
2. Select the disk you want to clean up and click **OK**. (No disk selection is offered when the system has only one drive.) Disk Cleanup scans the computer for files that can be deleted.
3. Select the files to clean up or compress and click **OK**.
4. Click **Yes** to confirm the operation.

You can also do this by creating a global script that regularly scans drives and removes all temporary or corrupt files. This script should be run at times when few users are logged on even though it will operate properly when users have active temporary files on the volume because active files are locked and cannot be deleted.

The script should delete the following file types:

- *.tmp
- ~*.*

Use the following commands in your script:

```
del volume:*.tmp /s /q >filename.txt
del volume:~*.* /s /q /a:h >filename.txt
```

where *volume:* is the name of the data drive. The `/s` and `/q` switches respectively mean including files located in subdirectories and don't ask for confirmation and the `/a:h` switch ensures that you delete only temporary files because they are normally hidden from users (some users may use the tilde (~) in their filenames). Finally, piping the information into a file (*filename.txt*) gives you a complete listing of all deleted files.

FS-13: Security Parameter Verification

Activity Frequency: Weekly

Security is always a concern in a networked data environment. Therefore, it is necessary to verify that security settings are appropriate on data and system drives.

The best way to verify security settings is to use the Security Configuration Manager in analysis mode. It compares an existing security implementation to a baseline security template and outlines the differences. This means that you must keep track of all the changes you make to security settings on data drives and you must update your baseline security template on a regular basis.

To analyze a computer and compare it to a given security policy in graphical mode, use **Procedure GS-20**. If you need to perform this verification on several systems, you should do so via a command line. The command to use is:

```
secedit /analyze /db filename.sdb /log filename.log
```

In addition, the `/verbose` switch can be used to create a log file that is highly detailed. If no log file is specified, secedit will automatically log all information to the scesrv.log file in the %windir%\security\logs folder. To configure a computer instead of analyzing it, replace the `/analyze` switch with `/configure`.

TIP *This command must be run locally. If you create scripts to run this command, make sure you design them to run locally on each file server.*

You can also verify and modify file and folder security settings with the `cacls` and `xcacls` commands. These commands are very useful for adding and removing security descriptors to and from files and folders without modifying existing security parameters. Use the `/?` switch with both commands for more information.

FS-14: Encrypted Folder Management

Activity Frequency: Weekly

File encryption is used to protect confidential information. Shared folder encryption is new to WS03.

To encrypt data in shared folders, the file servers must be trusted for delegation within Active Directory. This is a property of the server's computer account within the directory (**Server Name | Properties | Delegation | Trust this computer for delegation to any service (Kerberos only)**).

In addition, folders can only contain one of two values: compression or encryption. If a folder is not available for encryption, it is because its compression value is set.

Finally, encryption settings are applied through a folder's properties (**Properties | General tab | Advanced**) and encrypted files and folders are displayed in green in the Windows Explorer.

FS-15: Data Archiving

Activity Frequency: Monthly

Windows Server 2003 does not really include any special tool for archiving data, though it does include support for archival technology such as remote offline storage. You can use NT Backup to perform a backup of selected data for archival purposes, then remove the data from the network to create additional free space, but this is not necessarily an easy task. To archive data based on creation/modification date in Windows Server 2003, you must launch **Windows Backup** (**Start Menu | All Programs | Accessories | Backup**), move to the **Backup** tab, expand your data disk in the selection window, view each of the folders in the drive and sort files by date (click on the **Modified** title in the right pane) and select all of

the oldest files, then run the backup. You'll also need to print the backup report to identify which files to delete.

It is much simpler to create special archive-shared folders and ask users to place data that can be archived into these special shares. Then, on a regular basis, back them up and delete the folder's contents.

FS-16: File Replication Service Management

Activity Frequency: Monthly

Procedure FS-04 identifies that you must regularly check the FRS Event Log to make sure there are no replication errors. You also have to make sure the FRS replication rules are set properly and meet your network configuration's capabilities for replication, though this is done less often.

The items to verify are the following:

- Replication topology and schedule
- Files excluded from replication and replication priority

FRS is managed from the DFS console (Start Menu | Administrative Tools | Distributed File System).

1. If you don't see your DFS roots, use the **Action** menu to connect to them (**Action | Show Root**), and then locate the root you want to manage, select it and click **OK**.
2. Expand the DFS share name in the left pane to display the DFS links. Right-click on a link and select **Show replication information**.
3. Review the replication status for each DFS link.

FRS uses four different replication topologies: ring, hub and spoke, full mesh, and custom. You can change the replication mode by right-clicking on the DFS share name and selecting **Configure replication**.

TIP *FRS supports automatic replication on domain-based DFS roots. To do so, it requires a staging folder where it stores temporary files. You should also verify that the disk hosting this folder (FRS-Staging) has enough space to support the automatic replication process. You can use* ***Procedure FS-01*** *to do so.*

In addition, you can use SONAR, a Resource Kit tool that is designed to monitor both FRS Replica Set members and their status. SONAR runs as a command-line tool. It must first be installed on a system:

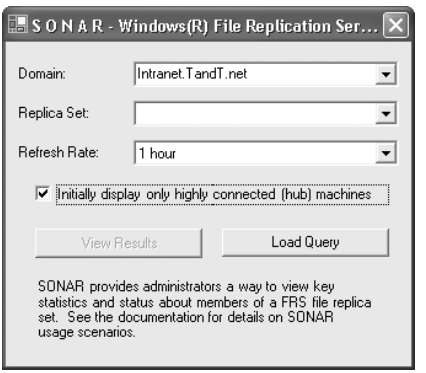
1. Locate **SONAR.exe** on the Resource Kit CD (or search for SONAR at www.microsoft.com/download) and use the following command:

   ```
   sonar /i
   ```

2. Once SONAR is installed, all you need to do is start it:

   ```
   sonar /s
   ```

3. This opens a dialog box that lets you select the **Domain**, and the **Replica Set**, and the Refresh Rate, and identify if you want to view only Hub data or all data.



4. To view the results, click **View Results**.

5. To stop SONAR, use **File | Exit**. **Save** your changes if you have made any.

Alternatively, you can store all the parameters in a file and launch SONAR with the configuration stored in this file. Type `sonar /?` for more information.

SCRIPT CENTER *The Microsoft TechNet Script Center includes a script that helps you monitor FRS replication. This script can be found at http://www.microsoft.com/ technet/treeview/default.asp?url=/technet/scriptcenter/monitor/ScrMon22.asp?frame=true.*

FS-17: Disk and Volume Management

Activity Frequency: Ad Hoc

Managing file servers also means managing disks, volumes and partitions. The best way to do this is to use the `diskpart` command-line tool. This tool includes its own command interpreter. To launch this command interpreter, open a command prompt and type `diskpart`, then press ENTER. The command interpreter starts and lists a new `diskpart` prompt.

Before you can use this command interpreter, you must `list`, then `select` either a disk, volume or partition to give it focus. The object that has focus will display an asterisk. Use the following command structure within the diskpart command interpreter:

```
list disk (or volume, or partition)
select disk number (or volume label or
partition number)
```

where *number* or *label* are the disk, volume or partition number or, in the case of a volume, its label (such as C, D, E, and so on).

Once an object has focus, you can use the `diskpart` command environment to perform a multitude of management activities on disk objects such as activation, deactivation, extension, creation, deletion, repair, and more.

You can also script `diskpart` activities by creating a simple text-based script file and using the following command:

```
diskpart /s scriptname.txt >logfile.txt
```

By adding *logfile.txt* to the command, you can redirect the script's output to a logfile you can view at a later date.

`Diskpart` is especially useful if you use WS03's built-in RAID functions.

Print Service Administration

With Windows Server 2003, print service administration involves everything from installing appropriate printer drivers to managing large clusters of print servers supporting massive user communities. In fact, Microsoft has tested a two-server cluster configuration supporting over 3,000 print queues.

WS03 works with Version 3 print drivers—drivers that are designed to integrate more properly with the operating system to provide better fault tolerance. One of the great advantages of these print drivers is that when the printer driver fails, it does not require a server restart but only a print spooler restart. In fact, WS03 can automatically restart the print spooler on a failure making the failure transparent to the majority of the users connected to the printer. The only user who will notice the failure is the one whose job caused the print spooler to fail.

This is because Windows 2000 and 2003 drivers are user-mode drivers as opposed to kernel-mode. Kernel-mode drivers are Version 2 drivers and were used in Windows NT. But a faulty kernel-mode driver can crash the entire kernel—or rather, the entire server. To provide better reliability, Windows 2000 and 2003 drivers were moved to user-mode. In Windows Server 2003, a default Group Policy blocks the use of Version 2 drivers.

TIP *Each printer in WS03 includes a special Troubleshooting topic under the Help menu. This provides you with a series of wizards that help debug printing problems.*

In addition, a default Group Policy blocks remote printer management on new print servers. This policy must be

activated before you can manage print servers from the comfort of your desk. You must make sure the Group Policy affecting print servers has the following setting:

- Allow Print Spooler to Accept Client Connections = enabled (**Computer Configuration | Administrative Templates | Printers**)

This will allow you to manage the print server remotely even if no printers are shared on it yet. This policy is automatically activated when you share a printer on a server.

SECURITY SCAN *WS03 supports printer management through a browser, but this requires the installation of Internet Information Server on the print server. In most cases, you should choose not to install IIS on your print servers because IIS can make print server management more complex and WS03 supports several other remote print server management methods.*

SCRIPT CENTER *The Microsoft TechNet Script Center includes a series of scripts that help you manage printing in Windows. These scripts can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/printing/default.asp?frame=true. Because of this, script references will not be repeated in each print-related activity unless there is one specific script that addresses the task.*

PS-01: Print Queue Management

Activity Frequency: Daily

Because printing is a function everyone uses on a daily basis, you should perform a proactive print queue verification on a daily basis. To verify printer status:

1. Launch the **Windows Explorer** (**Quick Launch Area | Windows Explorer**).
2. Navigate to **My Network Places**, locate the print server you need to verify and click **Printers and Faxes**.

3. Click on each printer to view its status. Repair its status if required.
4. In this case, you may have to delete or pause jobs, and then restart the print queue. All of these commands are under the **File** menu.

You can also use the command line to manage print queues:

```
net print \\servername\sharedprintername
```

where `\\`*servername*`\`*sharedprintername* is the UNC name for the printer. Typing this command lists the details of the print queue. You can also use three switches—`/delete, /hold,and /release`—to control print jobs. You must provide the job number to do so. For example:

```
net print \\servername\sharedprintername 10 /delete
```

PS-02: Printer Access Management

Activity Frequency: Weekly

Printer access is controlled through access rights. As always, assigning appropriate and controlled rights is an important aspect of a system administrator's job.

There are three basic rights that can be assigned to shared printers (**Printer | Properties | Security tab**):

- Print
- Manage Printers
- Manage Documents

These rights control who can do what on a printer. By default, everyone can use a printer once it is shared, but this can be changed. If, for example, you have a brand new color printer that will be reserved for managers only, you need to change its default security settings, removing Everyone and assigning a Managers group the Print right. Anyone with Print rights can manage their own documents on the printer.

By default, Print Operators, Server Operators and Administrators have complete control over shared printers. This means they can manage documents and stop and start printer queues. You must be a member of one of these groups to perform print management activities.

PS-03: Printer Driver Management

Activity Frequency: Weekly

As mentioned earlier, WS03 uses Version 3 printer drivers. These may not be available for every one of your printers. If this is the case, you will need to monitor printers more closely because Version 2 drivers can halt a server when they fail.

This is the reason why you should regularly monitor the printer manufacturer's web site for new, updated printer drivers for Windows Server 2003. Then, as soon as a Version 3 printer driver is available, modify the shared printer to improve reliability. Make sure the printer driver includes Windows Server 2003 certification. This will guarantee the printer driver's compatibility with WS03.

WS03 includes a default policy that bars Version 2 drivers from being installed (**Disallow installation of printers using kernel-mode drivers** under **Computer Configuration | Administrative Templates | Printers**). If you need to use kernel-mode drivers because you are using older printers, you must disable this policy setting.

TIP *If you deactivate this setting, make it one of your primary objectives to enable it again as soon as possible to improve print server reliability.*

Finally, user-mode printer drivers allow users to set their own printer preferences, but these preferences are derived from the printer properties you set. Make sure you set appropriate properties. For example, if the printer is capable of double-sided printing, set it to print double-sided by default.

PS-04: Printer Sharing

Activity Frequency: Ad hoc

Printer sharing is the main focus of print server management. Whenever you share printers in Windows Server 2003, you initiate a process that will eventually publish the printer in Active Directory. Users will be able to search the directory for printers based on name, properties, and printer type. Make sure you enter as much detail as possible when preparing a printer for shared use.

To share a printer:

1. Right-click on the printer you want to share and select **Sharing**.
2. Click **Share this printer**, assign a standard **Share name** to the printer and make sure that the **List in the directory** box is checked.
3. If you need to support client systems other than Windows 2000, XP, or 2003, then click **Additional Drivers**.
4. In the Additional Drivers dialog box, check the other Windows systems you need to support, then click **OK**. WS03 will ask you to provide the location of the additional drivers. Identify this location and click **OK**. Click **OK** once again to close the Additional Drivers dialog box.
5. Move to the **Advanced** tab and set spooling properties. Select **Start printing after last page is spooled** and **Print spooled documents first**. Other settings can remain at the default setting.
6. Move to the **Configuration** tab and ensure the device is properly configured. Then move to **Device Settings** and apply default printer settings such as duplex printing, stapling, and paper type in each paper tray.
7. If you need to modify the security settings on the printer share, use **Procedure PS-01**. Click **OK** to close the printer **Properties** dialog box when done.

PS-05: Print Spooler Drive Management

Activity Frequency Ad hoc

Large print servers need to spool a lot of print jobs. This means a lot of disk activity. The best way to provide fast and reliable printing is to dedicate a disk drive (or partition) to print spooling. This means that you need to prepare a special drive and assign the spooling to this drive:

1. In Windows Explorer, open **Printers and Faxes**. Select **Server Properties** from the **File** menu (or use the right mouse button anywhere in the right pane to select **Server Properties** from the context menu).
2. Move to the **Advanced** tab and type in the location for printer spooling. For example, this could be E:\Spool\Printers if E: was your dedicated spooling drive. Click **OK** when done.

Use **Procedure FS-01** on a regular basis to make sure there is enough free space on the print spooler drive.

PS-06: Printer Location Tracking Management

Activity Frequency: Ad hoc

Windows Server 2003 supports Printer Location Tracking. This component is based on the Active Directory site topology designed for your network. One of the key elements of the site topology is the subnet. Each subnet includes a name and a description. It can also include location information. Location information is stored in hierarchical form in the subnet properties under the Location tab. Each level is separated by a slash. You can use up to 256 levels in a location name, though the entire location name cannot be more than 260 characters long. Each part of the name can include up to 32 characters. For example, a printer located in the northeast corner of the first floor of the headquarters building could be identified as HQ/First Floor/Northeast Corner.

To enable Printer Location Tracking in your domain, you need the following elements:

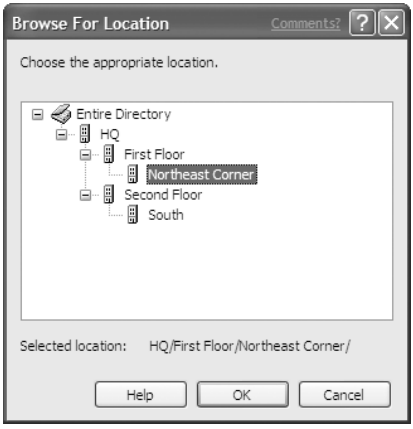
- Subnets and subnet locations entered into Active Directory Sites and Services
- A printer location naming convention
- Location Tracking GPO enabled
- Location settings for all printers
- Location settings for all PCs and servers

To turn Printer Location Tracking on, you must enable the **Pre-populate printer search location** text setting under **Computer Configuration | Administrative Templates | Printers**. This setting enables the Browse button in the Location tab for printer and computer properties within the directory. It also enables this button in the Search Printers tool. Apply this setting in a Group Policy that covers every machine in your network.

Printer location settings are set through the **General** tab of the **Property** dialog box. You can either type or click **Browse** to enter the location. Be as specific as you can.

TIP *You have to perform the same operation on all computer objects in the directory. Open the* ***Property*** *dialog box and use the* ***Location*** *tab to either type or click* ***Browse*** *to enter the location.*

Now, whenever users use the Search tool to locate a printer, printer location will automatically be entered in the location field enabling your user community to find printers near them without having to know your location-naming strategy.



PS-07: Massive Printer Management

Activity Frequency: Ad hoc

WS03 offers a series of Windows Scripting Host scripts to perform local and remote print server management. These include:

- **Prncnfg.vbs** manages printer configurations.
- **Prndrvr.vbs** manages printer drivers.
- **Prnjobs.vbs** manages print jobs.
- **Prnmngr.vbs** manages printers or printer connections.
- **Prnport.vbs** manages TCP/IP printer ports.
- **Prnqctl.vbs** manages print queues.

Each of these commands uses the following command structure:

```
cscript printcommand.vbs
```

where *printcommand* is the name of the script you want to use. Used without switches these commands automatically display help information. These commands are great tools for remote printer management and administration or for scripting operations that affect multiple printers at once.

TIP *You can also perform massive printer modifications with the Microsoft Print Migrator. Search for Print Migrator at http://www.microsoft.com/download for more information.*

PS-08: New Printer Model Evaluation

Activity Frequency: Ad hoc

Once in a while, you will also need to evaluate new printers. To enforce reliability and simplify your administration overhead, you should make sure all new printers meet the following criteria:

- Printer includes Version 3 digitally signed driver
- Printer driver has "Designed for Windows Server 2003" certification
- Printer is listed on the Microsoft Hardware Compatibility List (HCL) web site (http://www.microsoft.com/hcl/) or includes a certified driver
- Printer includes direct network connectivity
- Printer includes special features

TIP *You may also decide that you do not need to acquire PostScript printers (except in special cases such as for desktop publishing or graphics teams) because the Windows Unidriver rivals PostScript capabilities at lower cost.*

Cluster Services Management

One of Windows Server 2003's main strengths is its capability to support server clusters. WS03 can support server clusters including between two and eight nodes, but it depends on the WS03 edition you use: the Enterprise Edition supports between two and four node clusters and the Datacenter Edition supports between two and eight node clusters. Neither the Web or Standard Editions support server clustering (though they do support Network Load Balancing clusters).

Cluster verification is very important because the very nature of clusters is to provide high availability. This is only possible if it is operating properly. If one node of a two-node cluster is not functioning properly, you no longer have a redundant solution.

There are two cluster administration tools:

- The Cluster Administration console (Start Menu | Administrative Tools | Cluster Administration)
- The `cluster` command-line tool

The latter, the `cluster` command, provides all of the functionality required for cluster administration and can also be scripted. Typing `cluster /?` at the command line provides comprehensive help on this tool.

CS-01: Clusters: Cluster State Verification

Activity Frequency: Daily

Cluster services depend upon heartbeat detection to make sure each of the nodes is up and running. If the heartbeat of a node is not detected by the cluster service, it will automatically failover resources to other nodes.

Thus the first thing you should do when verifying the state of your clusters is make sure that each of the nodes

is operating properly. Use the following command to do so:

```
ping nodename or nodeipaddress
```

where *nodename* is the node's DNS name or *nodeipaddress* is the physical IP address for the node.

If the nodes do not respond, there may be a problem. Verify the node status with a **Remote Desktop Connection**. You can easily script this procedure and pipe the entire process into a text file (using the `>filename.txt` switch) and simply review the results in your text file.

CS-02: Clusters: Print Queue Status Verification

Activity Frequency: Daily

Server clusters are also very useful as Print Servers because they provide automatic failover on printer failure. But to do so, all printers must use drivers that are updated to meet Windows Server 2003's requirements. Use **Procedure PS-03** to make sure you are using proper print drivers on the server cluster.

Cluster print queues operate the same way as normal print queues except that they provide failover capabilities. To verify the status of the cluster print queues, use **Procedure PS-01**.

CS-03: Clusters: Server Cluster Management

Activity Frequency: Weekly

As mentioned earlier, cluster management is normally performed with either the **Cluster Administrator** console (**Start Menu | Administrative Tools | Cluster Administrator**) or the `cluster` command-line tool. Basically, you must verify that all of the cluster's nodes are operating properly and continue to be configured properly. You use these tools to add or remove nodes,

add quorum sets (shared disk storage), and configure majority node set (independent disk storage) replication.

The Cluster Administrator console is the easiest tool to use to add or remove cluster nodes because it includes a comprehensive series of wizards to perform most of the complex clustering tasks. To perform server cluster management:

- Launch the **Cluster Administrator** console. If you haven't already done so, use the **Open Connection to Cluster** dialog box to connect to a server cluster.
- Click on the **Cluster name** and view its status.
- Click on each **Cluster node** and view its status.
- If you have a new application to add to this cluster, right-click on the **Cluster name** and select **Configure Application**.
- This starts the **New Virtual Server** wizard. Provide it with appropriate answers and select the appropriate application type.

Applications can include file shares, print spoolers, DHCP, WINS, Distributed Transaction Coordinator, Message Queuing, Volume Shadow Copies, generic applications, and so on. Each specific application type will change the wizard's behavior and you will be asked appropriate questions for the application type.

You should also verify the System Event Log for events that are generated by the cluster service. These events are from the **ClusSvc** source. Use **Procedure GS-03** to check the System log in the Event Viewer. You can sort events by type simply by clicking on the **Category** column head.

CS-04: Clusters: Quorum State Verification

Activity Frequency: Weekly

A quorum is a collection of disks that are shared between cluster members. In WS03, quorums can be of two types: single disk units that are shared between all cluster

members or a majority node set. The latter, the majority node set, includes independent disk units for each member of a cluster and can be separated on a geographic basis. The majority node set removes the single point of failure from a server cluster but must rely on replication to operate properly.

The cluster service maintains a Quorum Log and it is through this log that it manages quorum operations. This log file is called **quolog.log** and is located under the **\MSCS** folder of the quorum (%Systemroot%\Cluster*quorumguid*\MSCS).

TIP *The Quorum Log is not a regular text file. Do not attempt to modify it.*

Use **Procedure CS-03** to view the quorum's state. Locate the quorum resource under **Clustername | Nodename | Active Resources**, right-click on the quorum name and select **Properties**. This will display the quorum's status under the **General** tab. You can also use the context menu to test failures (**Initiate Failure**) or to take the quorum resource offline (**Take Offline**).

TIP *Be careful with these operations. Make sure there are no users on the resource before either failure simulations or quorum resource dismounts.*

You can also use the cluster /quorum command to view available quorums. As usual, you can pipe this command to a text file using the >filename.txt switch and you can use this command in a script to automate the procedure.

TIP *Remember to look in Windows Server 2003's Help and Support Center to find out more information. It includes a special troubleshooting section that is really useful. Just select* ***Troubleshooting Strategies*** *from the H&SC home page.*