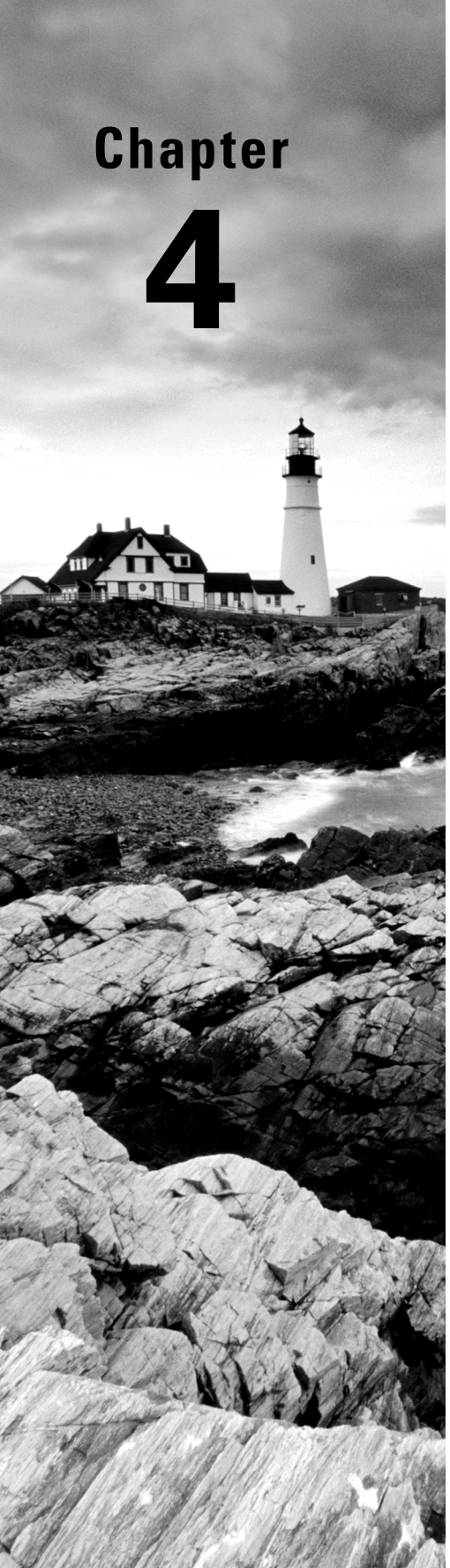


Chapter

4

Configure Windows Server 2012 R2

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configure file and share access**

- Create and configure shares
- Configure share permissions
- Configure offline files
- Configure NTFS permissions
- Configure access-based enumeration (ABE)
- Configure Volume Shadow Copy Service (VSS)
- Configure NTFS quotas
- Create and configure Work Folders

✓ **Configure print and document services**

- Configure the Easy Print print driver
- Configure Enterprise Print Management
- Configure drivers
- Configure printer pooling
- Configure print priorities
- Configure printer permissions

✓ **Configure servers for remote management**

- Configure WinRM
- Configure down-level server management
- Configure servers for day-to-day management tasks
- Configure multi-server management
- Configure Server Core
- Configure Windows Firewall
- Manage non-domain joined servers

This chapter explains how to set up your servers so that your network users have something to access. Before you can set up a server, you have to determine the purpose of it. Is it going to be a print server, a file storage server, a remote access server, or a domain controller?

After you have decided how the machine is going to help your network, you must implement your decision. In this chapter, I'll show you how to set up a print server and a file server. In addition, I will discuss how to set up permissions and security for these servers and how you can limit the amount of space your users can have on a server.

Microsoft Windows Server 2012 and Windows Server 2012 R2 are used for all of the server types in this chapter. Although other operating systems can be used, this chapter refers only to Windows Server 2012 and Windows Server 2012 R2.

Understanding File Servers

Before you configure a file server, you must understand what a file server actually does. *File servers* are machines on your network that store data files to share among network clients. The same machine can be a file server and another type of server. For example, a machine can both host network files and run Exchange Server 2013. Such a machine would have both file server and application server functions. (*Application servers* are machines that host applications used by network clients.)

Real World Scenario

Multiple Server Types on One Machine

More than ever, in today's world most IT departments have to worry about budgets. The problem is that the IT department often has the smallest budget in a company. You are typically stuck between a rock and a hard place because if your network is running well, people (including executives) forget about you. This makes it hard when you ask for anything that may impact the budget.

Because of the lack of funds, often you will leverage one machine to perform many server tasks. I have seen several companies where the IT department had to have the same machine running both as an application server and as a file server.

You must consider various factors before allowing a machine to run multiple server types. How many processors do you have? What are the processor speeds? How much RAM does the machine have? What is the hard drive speed? What type of applications will be hosted on the machine?

After you have gathered all of the information about the machine, then you can decide whether the machine can host multiple server types. Keep this one fact in mind, however—because of the requirements and demands on the computer system, it's always a good idea to host SQL Server on a dedicated machine.

When setting up a file server, one of the most important things you will do is to set up work and personal folders for your users. I have been consulting for many years, and one thing I always stress to all of my clients is to perform regular backups. After all, most organizations would not be able to recover after losing all of their data. Usually, companies back up only their servers, and this is why home folders are so important. *Home folders* are one of the most common file types on a file server; they are folders set up on the server for users to store information. Users have a location on the server to store their important data, and therefore that data will be backed up when the company does its regular backups.

Home folders are just one example of how to use work folders on a file server. I will be discussing other examples throughout this chapter.

Configuring File Servers

Now that you have an understanding of what a file server does, it's time to discuss how to configure these servers. Setting up a file server properly encompasses many steps. As always, one major concern is security. In the following sections, I will first describe how to share and publish online and offline files and folders. Then I will discuss the two types of security—shared permissions and NTFS security—that an administrator can set when sharing files or folders.

Sharing Folders

A file server is for sharing and storing data. To use one, you need to know how to set up a share, or a shared folder, on your server. A *shared folder* is exactly what it says; it's a folder that is shared on your network so that users can access the data within that folder. As an administrator, you have the ability to determine which users can access which files within a shared folder.

One of the main goals of Active Directory is to make resources easy to find. Active Directory also makes it easy to determine which files are available to users. That being said, I will explain how Active Directory manages to publish shared folders.

Making Active Directory Objects Available to Users

With Active Directory, a system administrator can control which objects users can see. The act of making an Active Directory object available is known as *publishing*. The two main publishable objects are Printer objects and Shared work folder objects. The reason I list Shared work folders here is because personal folders for users are not normally published in Active Directory. You publish an object in Active Directory because you want an easy way for everyone to find resources. Ordinarily, you don't want everyone accessing someone's home folder, and this is why you don't normally publish home folders.

The general process for creating server shares and shared printers has remained unchanged from previous versions of Windows. You create the various objects (printers or folders) and then enable them for sharing.

To make these resources available via Active Directory, however, there's an additional step: You must publish the resources. Once an object has been published in Active Directory, clients will be able to find it.

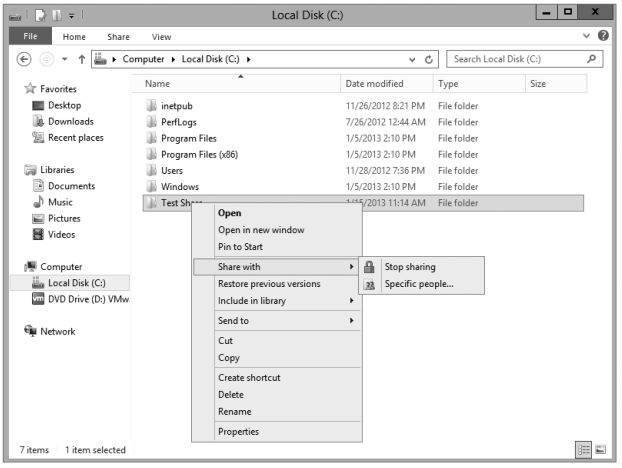
When you publish objects in Active Directory, you should know the server name and share name of the resource. This information, however, doesn't matter to your users. A system administrator can change the resource to which an object points without having to reconfigure or even notify clients. For example, if you move a share from one server to another, all you need to do is update the Shared Folder's object's properties to point to the new location. Active Directory clients still refer to the resource with the same path and name as they used before.

Exercise 4.1 will walk you through the steps for sharing and publishing a folder for use on your network.

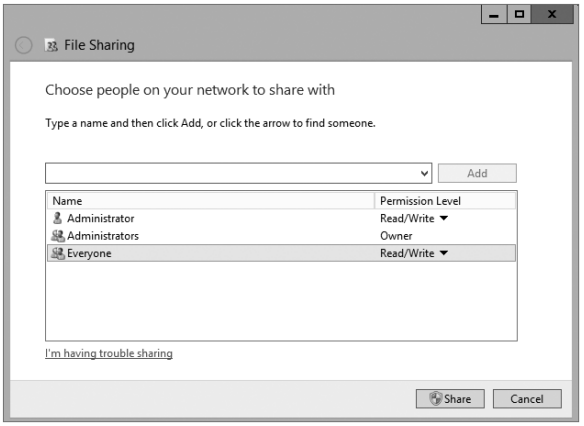
EXERCISE 4.1

Creating and Publishing a Shared Work Folder

1. Create a new folder in the root directory of your `C:` partition, and name it **`Test Share`**.
2. Right-click the `Test Share` folder, and choose Share With ➢ Specific People.



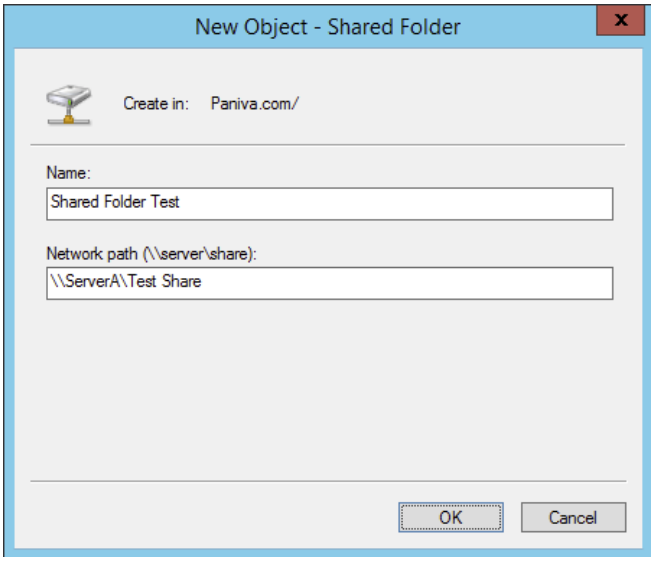
3. In the File Sharing dialog box, enter the names of users with whom you want to share this folder. In the upper box, enter **Everyone** and then click Add. Note that Everyone appears in the lower box. Click in the Permission Level column next to Everyone, and choose Read/Write from the drop-down menu. Then click Share.



4. You see a message that your folder has been shared. Click Done.

5. Open the Active Directory Users and Computers tool. Expand the current domain. Select New ➢ Shared Folder.

6. In the New Object – Shared Folder dialog box, type **Shared Folder Test** for the name of the folder. Then type the UNC path to the share (for example, **`\\serverA\Test Share`**). Click OK to create the share.



One of the main benefits of having all of your resource information in Active Directory is that you can easily find the information that you're seeking using the Find dialog box. When setting up objects in Active Directory, I recommend you always enter as much information as possible for the objects you're creating. The extra effort will pay off when your users start doing searches for these objects. The more information you enter, the more users can search to find the appropriate resource they need.

Access-Based Enumeration

Access-Based Enumeration (ABE) is a feature included with Windows Server 2012/2012 R2. ABE allows your domain users to list only the files and folders to which they have access when browsing content on the file server.

ABE helps eliminate domain users' issues that are caused by users connecting to file servers and seeing large numbers of files and folders the user cannot connect. ABE allows users only to see files and folders to which they have access.

Knowing that ABE is working on the Windows Server helps you set up your permissions properly. If you need to give a user the ability to see files and folders that they might not be able to change, you need to allow them at least to read or view the directories. As an administrator, it's important that you understand that Access-Based Enumeration is working on the server and what you need to do to get a user around it when needed.

Configuring Offline Files

If you have been in this industry long enough, you have seen a major change in end-user computers. Years ago, only a few select users had laptops. They were big and bulky, and they weighed almost as much as today's desktop computers.

The pendulum has swung in the opposite direction. It probably seems like every one of your end users now has a laptop. As an IT administrator, this gives you a whole new set of challenges and problems to address.

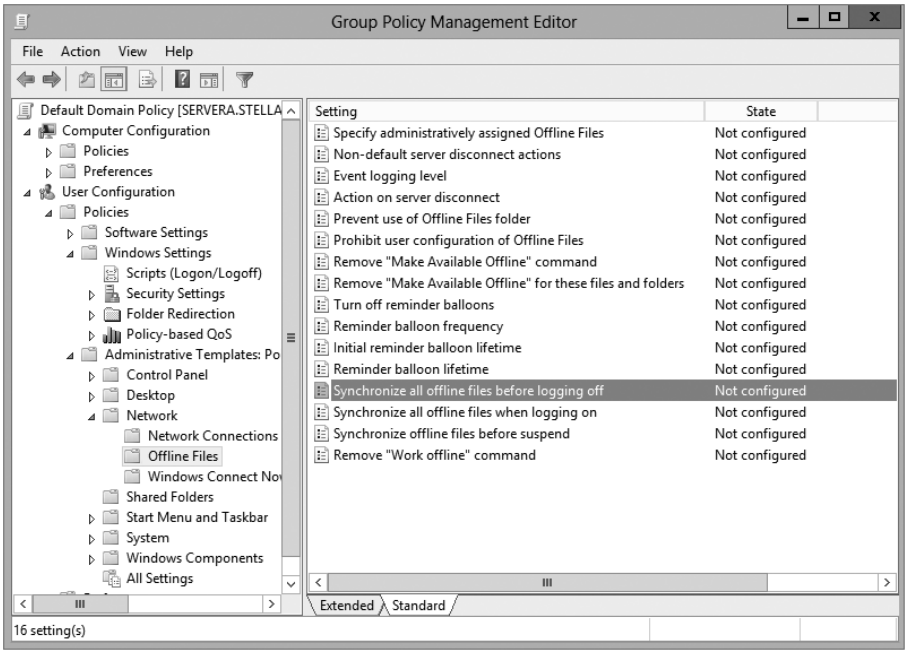
One challenge that you have to address is how users can work on files while outside of the office. If you have a user who wants to work at home, how do you give them the files they need to get their work done?

The answer is *offline folders*. These folders contain data that can be worked on by users while outside the office. An IT administrator can set up offline folders through the use of *Group Policy objects (GPOs)*.

When you decide to make folders available for offline use, these folders need to synchronize with the laptops so that all of the data matches between both systems. As an administrator, one decision that you will need to make is when the offline folders will

be synchronized. There are three synchronization options that you can set in a GPO (see Figure 4.1).

FIGURE 4.1 Synchronization options in a GPO



You can set up any combination of these options:

- When you select Synchronize All Offline Files Before Logging Off, offline folders are synchronized when the user logs off the network.
- When you select Synchronize All Offline Files When Logging On, offline folders are synchronized when the user logs on to the network.
- When you select Synchronize Offline Files Before Suspend, offline folders are synchronized before the user does a system suspend.

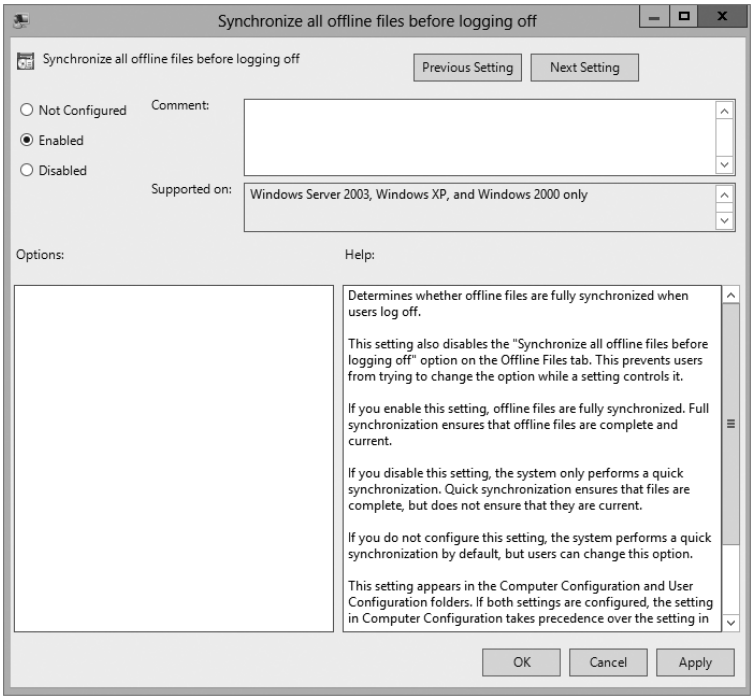
In Exercise 4.2, I will show you the steps necessary to configure offline folder options by using a GPO. This exercise uses the Group Policy Management Console (GPMC). If your GPMC is not installed, use the Server Manager MMC (under Features) to install it.

Group Policy objects will be covered in full detail in Chapter 6 "Manage GPOs."

EXERCISE 4.2

Configuring Offline Folder Options

1. Open the Group Policy Management Console.
2. In the left pane, expand your forest and then your domain. Under your domain name, there should be a default domain policy.
3. Right-click the default domain policy and choose Edit.
4. In the User Configuration section, expand Policies ➢ Administrative Templates ➢ Network and then click Offline Files.
5. Right-click Synchronize All Offline Files Before Logging Off and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.



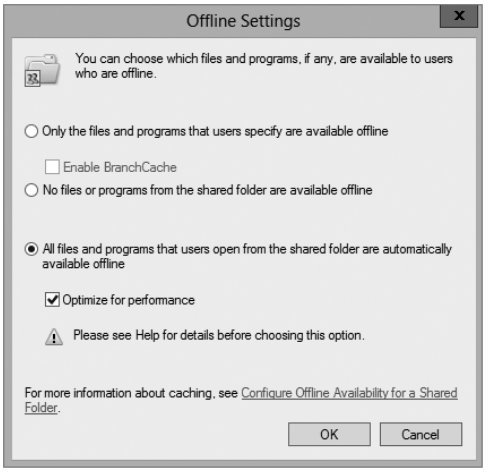
6. Right-click Synchronize All Offline Files When Logging On and choose Edit. The GPO setting dialog box appears. Choose the Enabled option and click OK.
7. Right-click Synchronize Offline Files Before Suspend and choose Edit. The GPO setting dialog box appears. Choose the Enabled option. In the Action drop-down box, make sure Quick is selected. Click OK.
8. Close the GPMC.

Now that you have set up a GPO for synchronization, it's time to share a folder for offline usage. In Exercise 4.3, you will set up a folder for offline access. You must complete Exercise 4.1 before doing this exercise.

EXERCISE 4.3

Configuring a Shared Network Folder for Offline Access

1. Right-click the `Test Share` folder that you created in Exercise 4.1 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button.
3. When the Advanced Sharing dialog box appears, click the Caching button.
4. When the Offline Settings dialog box appears, choose the All Files And Programs That Users Open From The Shares Will Be Automatically Available Offline option. Click OK.



5. Click OK twice more to close the Properties dialog box.

Volume Shadow Copy Services

Windows includes a feature that allows you to create a point-in-time image of one or more volumes. The *Volume Shadow Copy Service (VSS)* is the feature within Windows that allows an administrator take an image (shadow copy) of one or more volumes. Shadow copies have the ability to provide both file system and application.

Shadow copies allow an administrator to back up shared folders to a remote location. Shadow copies are designed to help recover files that were accidentally deleted, that were overwritten, or that have become corrupt. One major advantage to shadow copies is that

open files can be backed up. This means that even if users are currently working on files in a shared folder that has shadow copies enabled, the shadow copies will continue to function.

Once administrators have configured and enabled shadow copies (using the Computer Management snap-in), network users can restore earlier versions of files. After the initial shadow copy of the shared folder is created, only changes are copied and not the entire file.

You can enable shadow copies of entire volumes.

The following are some of the settings that you can configure when setting up shadow copies:

Schedule You have the ability to set the schedule of the shadow copies. You can set this schedule to run daily, weekly, monthly, once, at system startup, at logon, or when the system is idle. You can also set the time at which the shadow copy will run.

Storage Locations An administrator needs to set the location of the shadow copy backup. If you are on a network, it is a good idea to place the shadow copy on a network drive.

Maximum Size You can set a maximum size on your shadow copies, or you can specify that they have no size limit. One of the predetermined settings is 64 shadow copies per volume.

In Exercise 4.4, you'll set up a volume to make shadow copies every Monday at 7 a.m. To set up the shadow copies, you will use the Computer Management MMC snap-in.

EXERCISE 4.4

Configuring a Shadow Copy on a Volume

1. Open Computer Management by pressing the Windows key and selecting Administrative Tools ➢ Computer Management.
2. Expand Storage and then right-click Disk Management. Choose All Tasks ➢ Configure Shadow Copies.
3. When the Shadow Copies dialog box appears, click the Settings button.
4. When the Settings windows appears, click the Schedule button.
5. In the Schedule window, set the schedule task to weekly and the start time for 7 a.m. Uncheck all of the days-of-the-week boxes except Mon. Click OK.
6. When the Settings window reappears, click OK.
7. If the Enable button is enabled, click it. Then click OK.
8. Exit the Computer Management MMC.

To recover a previous version of a file from a shadow copy, you use the `\\server_name\share_name` path. The operating system determines how you will gain access to the shared folders and shadow copies. Shadow copies are built into Windows XP (SP1), Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2. If you are using a different Microsoft operating system, you need to download the Shadow Copy Client Pack from the Microsoft download center.

VssAdmin Command

Another way to create, configure, and manage shadow copies is by using the `vssadmin.exe` command-line utility. The `vssadmin.exe` command allows you to create, delete, list, and resize shadow copies and shadow storage.

One area where the VSS is very important is during backups. When you back up open files, the VSS copies the data and helps back up open files. For example, when you are backing up a Microsoft Exchange server using a Unitrends backup server, the VSS Exchange writer is used. To see if the VSS writers are functioning properly, you can open a command prompt (with administrative privileges) and type in the following statement:

```
VSSAdmin list writers
```

This command will show you all the different VSS service writers and how those VSS writers are functioning properly.

Table 4.1 describes the `vssadmin.exe` command and the different commands associated with the `vssadmin` utility.

TABLE 4.1 `Vssadmin.exe` commands

Command	Description
Add ShadowStorage	Adds a new volume shadow copy storage association
Create Shadow	Creates a new volume shadow copy
Delete Shadows	Deletes volume shadow copies
Delete ShadowStorage	Deletes the volume shadow copy storage associations
List Providers	Lists registered volume shadow copy providers
List Shadows	Lists existing volume shadow copies
List ShadowStorage	Lists volume shadow copy storage associations
List Volumes	Lists volumes eligible for shadow copies
List Writers	Lists subscribed volume shadow copy writers
Resize ShadowStorage	Resizes a volume shadow copy storage association
Revert Shadow	Reverts a volume to a shadow copy
Query Reverts	Queries the progress of in-progress revert operations

Configuring Permissions

You have gone through the steps necessary to set up a shared folder, publish it to Active Directory, and set it up for offline access. Now you will see how you can protect these files and folders by using permissions.

You can secure folders using permissions in two ways, and you can secure files in one way. You can set up permissions and security through NTFS or through sharing.

Understanding NTFS

NTFS is an option that you have when you are formatting a hard drive. You can format a hard drive for a Microsoft operating system in three ways.

- File Allocation Table (FAT) is supported on older operating systems only (Server 2003, Server 2000, XP, and so on).
- FAT32 is supported in Windows Server 2012 R2.
- NTFS is supported in Windows Server 2012 R2.

NTFS has many advantages over FAT and FAT32. They include the following:

Compression Compression helps compact files or folders to allow for more efficient use of hard drive space. For example, a file that usually takes up 20MB of space might use only 13MB after compression. To enable compression, just open the Advanced Attributes dialog box for a folder and check the Compress Contents To Save Disk Space box (see Figure 4.2).

FIGURE 4.2 Setting up compression on a folder

Quotas *Quotas* allow you to limit how much hard drive space users can have on a server. Quotas are discussed in greater detail in the section "Configuring Disk Quotas."

Encryption *Encrypting File System (EFS)* allows a user or administrator to secure files or folders by using encryption. Encryption employs the user's security identification

(SID) number to secure the file or folder. To implement encryption, open the Advanced Attributes dialog box for a folder and check the Encrypt Contents To Secure Data box (see Figure 4.3).

FIGURE 4.3 Setting up encryption on a folder

If files are encrypted using EFS and an administrator has to unencrypt the files, there are two ways to do this. First, you can log in using the user's account (the account that encrypted the files) and unencrypt the files. Second, you can become a recovery agent and manually unencrypt the files.

If you use EFS, it's best not to delete users immediately when they leave a company. Administrators have the ability to recover encrypted files, but it is much easier to gain access to the user's encrypted files by logging in as the user who left the company and unchecking the encryption box.

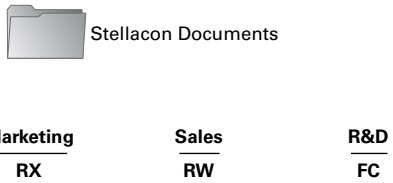
Security One of the biggest advantages of NTFS is security. Security is one of the most important aspects of an IT administrator's job. An advantage of NTFS security is that the security can be placed on individual files and folders. It does not matter whether you are local to the share (in front of the machine where the data is stored) or remote to the share (coming across the network to access the data); the security is always in place with NTFS.

The default security permission is `Users = Read` on new folders or shares.

NTFS security is *additive*. In other words, if you are a member of three groups (Marketing, Sales, and R&D) and these three groups have different security settings, you get the highest level of permissions. For example, let's say you have a user by the name of wpanek who belongs to all three groups (Marketing, Sales, and R&D).

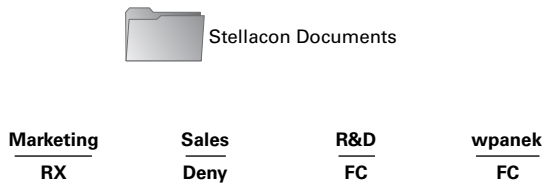
Figure 4.4 shows this user's permissions. The Marketing group has Read and Execute permissions to the `Stellacon Documents` folder. The Sales group has Read and Write, and the R&D group has Full Control. Since wpanek is a member of all three groups, wpanek would get Full Control (the highest level).

FIGURE 4.4 Security settings on the `Stellacon Documents` folder



The only time this does not apply is with the Deny permission. Deny overrides any other group setting. Taking the same example, if Sales has Deny permission for the `Stellacon Documents` folder, the user wpanek would be denied access to that folder. The only way around this Deny is if you added wpanek directly to the folder and gave him individual permissions (see Figure 4.5). Individual permissions override a group Deny. In this example, the individual right of wpanek would override the Sales group's Deny. The user's security permission for the `Stellacon Documents` folder would be Full Control.

FIGURE 4.5 Individual permissions



Give users only the permissions necessary to do their jobs. Do not give them higher levels than they need.

Understanding Shared Permissions

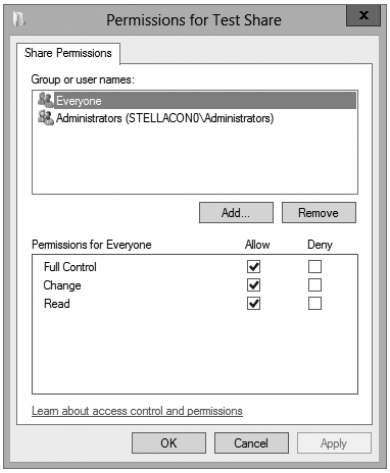
When you set up a folder to be shared, you have the ability to assign that folder's permissions. *Shared permissions* can be placed only on the folder and not on individual files. Files have the ability to inherit their permissions from the parent folder.

Shared folder permissions are in effect only when users are remote to the shared data. In other words, if computer A shares a folder called `Downloads` and assigns that folder shared permissions, those permissions would apply only if you connected to that share from a machine other than computer A. If you were sitting in front of computer A, the shared permissions would not apply.

Like NTFS permissions (discussed in the previous section), shared permissions are additive, so users receive the highest level of permissions granted by the groups of which they are members.

Also, as with NTFS permissions, the Deny permission (see Figure 4.6) overrides any group permission, and an individual permission overrides a group Deny.

FIGURE 4.6 Setting up permissions on a shared folder



The default shared permission is `Administrators = Full Control`. The shared permissions going from lowest to highest are Read, Change, Full Control, and Deny. Table 4.2 compares the two different types of permissions and security.

TABLE 4.2 NTFS security vs. shared permissions

Description	NTFS	Shared
Folder-level security.	Yes	Yes
File-level security.	Yes	No
In effect when local to the data.	Yes	No
In effect when remote to the data.	Yes	Yes
Permissions are additive.	Yes	Yes
Group Deny overrides all other group settings.	Yes	Yes
Individual settings override group settings.	Yes	Yes

How NTFS Security and Shared Permissions Work Together

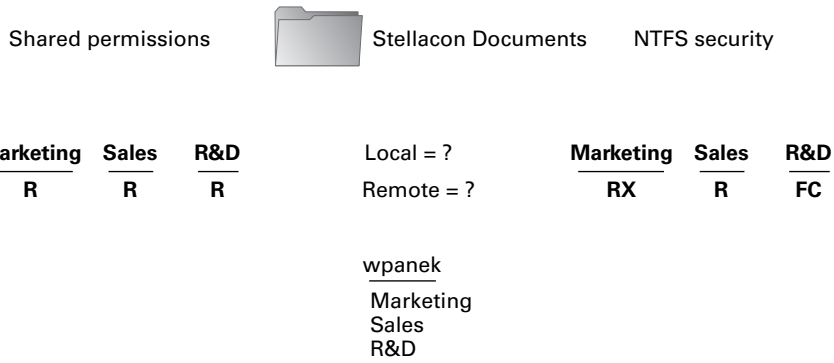
When you set up a shared folder, you need to set up shared permissions on that folder. If you're using NTFS, you will also need to set up NTFS security on the folder. Since both shared permissions and NTFS security are in effect when the user is remote, what happens when the two conflict?

These are the two basic rules of thumb:

- The local permission is the NTFS permission.
- The remote permission is the more restrictive set of permissions between NTFS and shared.

This is easy to do as long as you do it in steps. Let's look at Figure 4.7 and walk through the process of figuring out what wpanek has for rights.

FIGURE 4.7 NTFS security and shared permissions example



As you can see, wpanek belongs to three groups (Marketing, Sales, and R&D), and all three groups have settings for the `Stellacon Documents` folder. In the figure, you will notice that there are two questions: Remote = ? and Local = ? That's what you need to figure out—what are wpanek's effective permissions when he is sitting at the computer that shares the folder, and what are his effective permissions when he connects to the folder from another computer (remotely)? To figure this out, follow these steps:

1. Add up the permissions on each side separately.

   Remember, permissions and security are *additive*. You get the highest permission. So, if you look at each side, the highest shared permission is the Read permission. The NTFS security side should add up to equal Full Control. Thus, now you have Read permission on shared and Full Control on NTFS.
2. Determine the local permissions.

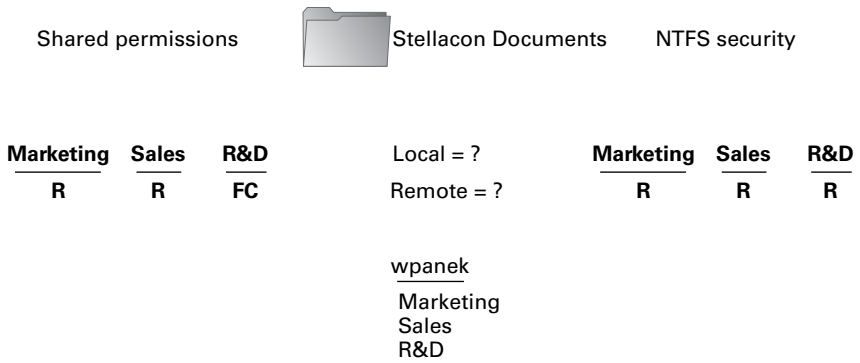
   Shared permissions do not apply when you are local to the data. Only NTFS would apply. Thus, the local permission would be Full Control.

3. Determine the remote permissions.

   Remember, the remote permission is the most restrictive set of permissions between NTFS and shared. Since Read is more restrictive than Full Control, the remote permission would be Read.

Let's try another. Look at Figure 4.8, and see whether you can come up with wpanek's local and remote permissions.

FIGURE 4.8 NTFS security and shared permissions



Your answer should match the following:

Local = Read

Remote = Read

Remember, first you add up each side to get the highest level of rights. NTFS would be Read, and shared would be Full Control. The local permission is always just NTFS (shared does not apply to local permissions), and remote permission is whichever permission (NTFS or shared) is the most restrictive (which would be Read on the NTFS side).

Exercise 4.5 walks you through the process of setting both NTFS and shared permissions. You must complete Exercise 4.1 before doing this exercise.

EXERCISE 4.5

Configuring Shared and NTFS Settings

1. Right-click the `Test Share` folder you created in Exercise 4.1 and choose Properties.
2. Click the Sharing tab and then click the Advanced Sharing button. (You will set the shared permissions first.)
3. Click the Permissions button. Click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Sales group.) Once you find your group, click OK.

EXERCISE 4.5 *(continued)*

4. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Full Control and click OK. (All of the other Allow check boxes will automatically become checked.)
5. On the Advanced Sharing page, click OK. Now click the Security tab. (This allows you to set the NTFS security settings.)
6. Click the Edit button. That takes you to the Permissions page. Now click the Add button. When the Select User page appears, choose a group from Active Directory. (I used the Everyone group.) Once you find your group, choose OK.
7. The Permissions dialog box appears. With your group highlighted, click the Allow check box next to Modify, and click OK. (All of the check boxes below Modify will automatically become checked.)
8. Click Close.

Configuring Disk Quotas

In this chapter so far, you have seen how to set up a share and publish it to Active Directory. You've also learned how to set up permissions and security and how NTFS and shared permissions work with each other. It's time to learn how to limit users' hard drive space on the servers.

Disk quotas give administrators the ability to limit how much storage space a user can have on a hard drive. As mentioned earlier in this chapter, disk quotas are an advantage of using NTFS over FAT32. If you decide to use FAT32 on a volume or partition, quotas will not be available.

You have a few options available to you when you set up disk quotas. You can set up disk quotas based on volume or on users.

A good rule of thumb is to set up an umbrella quota policy that covers the entire volume and then let individual users exceed the umbrella as needed.

Setting Quotas by Volume One way to set up disk quotas is by setting the quota by volume, on a per-volume basis. This means that if you have a hard drive with `C:`, `D:`, and `E:` volumes, you would have to set up three individual quotas—one for each volume. This is your umbrella. This is where you set up an entire disk quota based on the volume for all users.

Setting Quotas by User You have the ability to set up quotas on volumes by user. Here is where you would individually let users have independent quotas that exceed your umbrella quota.

Specifying Quota Entries You use quota entries to configure the volume and user quotas. You do this on the Quotas tab of the volume's Properties dialog box. (See Exercise 4.6.)

Creating Quota Templates Quota templates are predefined ways to set up quotas. Templates allow you to set up disk quotas without needing to create a disk quota from scratch. One advantage of using a template is that when you want to set up disk quotas on multiple volumes (`C:`, `D:`, and `E:`) on the same hard drive, you do not need to re-create the quota on each volume.

Exercise 4.6 will show you how to set up an umbrella quota for all users and then have an individual account in your Active Directory exceed this quota.

EXERCISE 4.6

Configuring Disk Quotas

1. Open Windows Explorer.
2. Right-click the local disk (`C:`) and choose Properties.
3. Click the Quotas tab.
4. Check the Enable Quota Management check box. Also check the Deny Disk Space To Users Exceeding Quota Limit box.
5. Click the Limit Disk Space To option and enter **1000MB** in the box.
6. Enter **750MB** in the Set Warning Level To boxes.
7. Click the Apply button. If a warning box appears, click OK. This warning is just informing you that the disk may need to be rescanned for the quota.
8. Now that you have set up an umbrella quota to cover everyone, you'll set up a quota that exceeds the umbrella. Click the Quota Entries button.
9. The Quotas Entries for (`C:`) window appears. You will see some users already listed. These are users who are already using space on the volume. Click the Quota menu at the top and choose New Quota Entry.

   Notice the N/A entry in the Percent Used column. This belongs to the administrator account, which by default has no limit.
10. On the Select User page, choose a user that you want to allow to exceed the quota (for this example, I used the wpanek account). Click OK.
11. This opens the Add New Quota Entry dialog box. Click the Do Not Limit Disk Usage option and click OK.
12. You will notice that the new user has no limit. Close the disk quota tool.

Configuring Print Services

One of the most important components on a network is the printer. Printers today are almost as important as the computers themselves. Think about your network. What would your network be like without a printer? Even small networks or home networks have a printer today.

How many printers do you want on your network? It is not feasible to put a printer on every user's desk. What if some users need black and white while others need color? Do you give each user two printers? What if they need laser printing for reports but ink-jets will work fine for every other type of print job? These are all questions that you must answer before buying any printers for your networks.

This is also where network printers and print servers come into play. *Network printers* are printers that can be directly connected to the network through some form of network interface card. These printers usually have settings that can be configured for your network needs. For example, if your network uses DHCP, you can set the printer to be a DHCP client.

Print servers are servers that have a connected printer, where the server handles all printing issues. This is an excellent solution for printers that cannot directly connect to the network. Once the printer is connected to the network (through the use of a NIC or a server), the end user just connects to the printer and prints. To the end user, there is no real difference between the two options.

Before an end user can print to a network printer, an administrator must connect, set up, share, and publish the printer for use. An administrator must also set the permissions on the printer to allow users to print to that printer. The following sections will discuss these items in detail.

Creating and Publishing Printers

Once your printer is installed, you must share the printer and then publish the printer to Active Directory before users can print to it. Printers can be published easily within Active Directory. This makes them available to users in your domain.

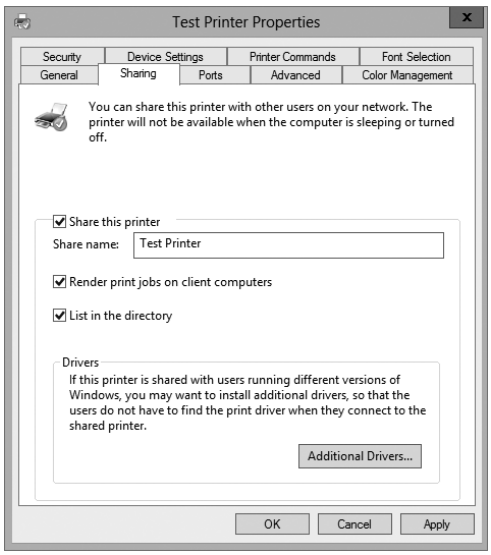
Exercise 4.7 walks you through the steps you need to take to share and publish a Printer object by having you create and share a printer. To complete the printer installation, you need access to the Windows Server 2012 installation media (via the hard disk, a network share, or the CD/DVD drive). If you do not have a printer for this exercise, just choose one from the list and continue the exercise.

EXERCISE 4.7

Creating and Publishing a Printer

1. Press the Windows key and select ➢ Control Panel ➢ Devices and Printers ➢ Add Printer. This starts the Add Printer Wizard.

2. On the Add Printer page, click the link The Printer That I Want Isn't Listed.
3. Choose Add A Local Printer and click Next.
4. On the Choose A Printer Port page, select Use An Existing Port. From the drop-down list beside that option, make sure LPT1: (Printer Port) is selected. Click Next.
5. On the Install The Printer Driver page, select Generic for the manufacturer, and for the printer, highlight Generic/Text Only. Click Next.
6. If a driver page appears, choose Use The Driver That Is Currently Installed and click Next.
7. On the Type A Printer Name page, enter **Text Printer**. Uncheck the Set As The Default Printer box and then click Next.
8. The Installing Printer page appears. After the system is finished, the Printer Sharing page appears. Make sure the Share This Printer So That Others On Your Network Can Find And Use It box is selected, and accept the default share name of Text Printer.
9. In the Location section, type **Building 203**, and in the Comment section, add the following comment: **This is a text-only printer**. Click Next.
10. On the You've Successfully Added Text Printer page, click Finish.
11. Next you need to verify that the printer will be listed in Active Directory. Right-click the Text Printer icon, and select Text Printer Properties.
12. Next select the Sharing tab and make sure that the List In The Directory box is checked. Click OK to accept the settings.



13. Close the printer Properties box, and close Devices And Printers.

Note that when you create and share a printer this way, an Active Directory Printer object is not displayed within the Active Directory Users and Computers tool.

Configuring Printers

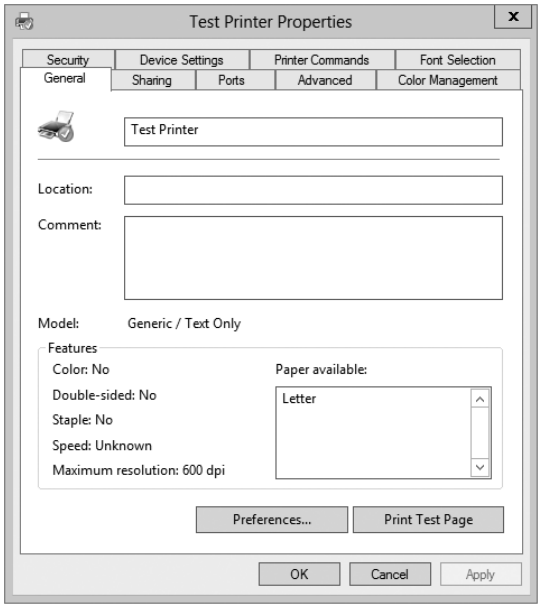
The printer has now been installed and published to Active Directory. It's time to set all of the different configuration options. To get to the options, right-click the Printer object and choose Properties.

The following are just some of the tabs you can configure:

The General Tab The General tab (see Figure 4.9) allows you to set some basic printer attributes.

- The field at the top of the dialog box contains the display name of the Printer object.
- The Location field should contain text that helps users physically locate the printer. This allows users to search for printers based on location (location-aware printing).
- The Comment field allows an administrator to put in any additional information, such as the printer type.
- The Printing Preferences button takes you to controls that allow you to change the layout and paper type of the printer.

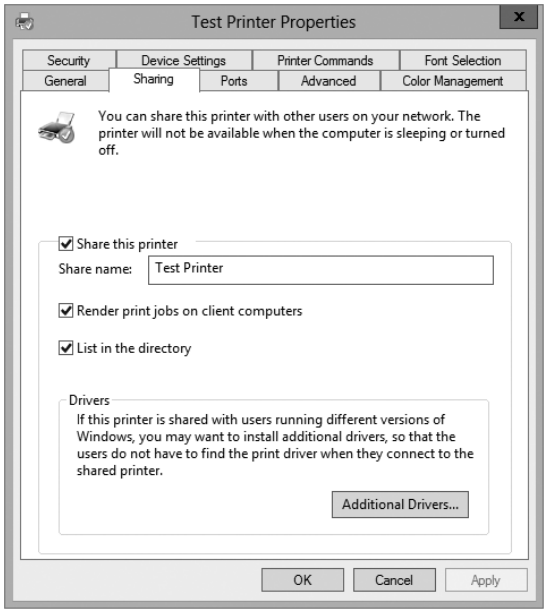
FIGURE 4.9 The General tab of the printer's Properties dialog box



The Sharing Tab The Sharing tab (see Figure 4.10) allows you to configure your printer for sharing on your network. This is what allows users to use a network printer (if they have the proper permissions on the printer).

- The Share This Printer check box allows you to share the printer on the network.
- Share Name is the name your users will see on the network.
- When Render Print Jobs On Client Computers is checked, the client computer caches the print job until the printer is ready to print. If unchecked, the print server will cache the entire job before it prints to the printer.
- When List In The Directory is checked, users can search the directory for the printer.
- The Additional Drivers button allows you to load additional drivers for your clients. It is especially useful for giving access to drivers for older client systems. One advantage of a print server is that the server will automatically download drivers to client computers.

FIGURE 4.10 The Sharing tab of the printer's Properties dialog box

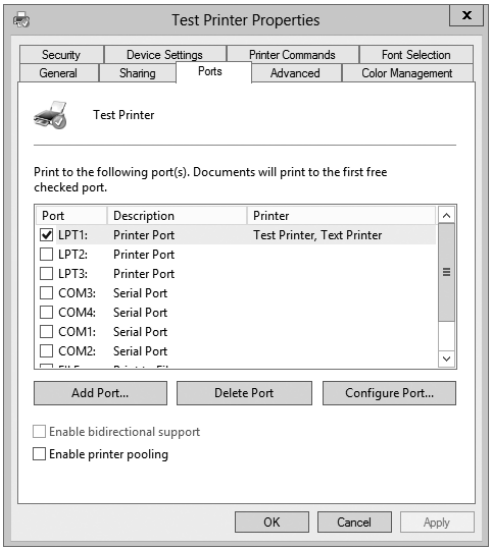


The Ports Tab The Ports tab (see Figure 4.11) allows you to configure the port to which your printer is connected. You can add ports or configure existing ports.

- The Port check boxes allow you to choose to which port your printer is connected. Options are the printer port, serial port, local port, and print to file port.
- The Add Port button allows you to add a custom port (for example, a TCP/IP port).

- The Delete Port button allows you to remove a port from the Port list.
- The Configure Port button gives you settings to configure an existing port. For example, if you use TCP/IP, this button allows you to change the TCP/IP options.
- Enable Bidirectional Support allows your printer and computer to communicate back and forth. If this check box is disabled, your printer cannot support two-way communications.
- A *printer pool* allows two or more identical printers to share the print load. When a document is sent to the printer pool, the first available printer receives the print job and prints it. Enable Printer Pooling allows a large department or organization to get print jobs done faster. Users do not have to wait for one printer to get their print job. You should follow these rules when setting up a printer pool:
  - All printers in the pool need to be the same model and type.
  - All printers in the pool should be in the same physical location. Print jobs will be printed to the first available printer. If these printers are located all over the company, it may take a user too long to find their print job.

FIGURE 4.11 The Ports tab of the printer's Properties dialog box



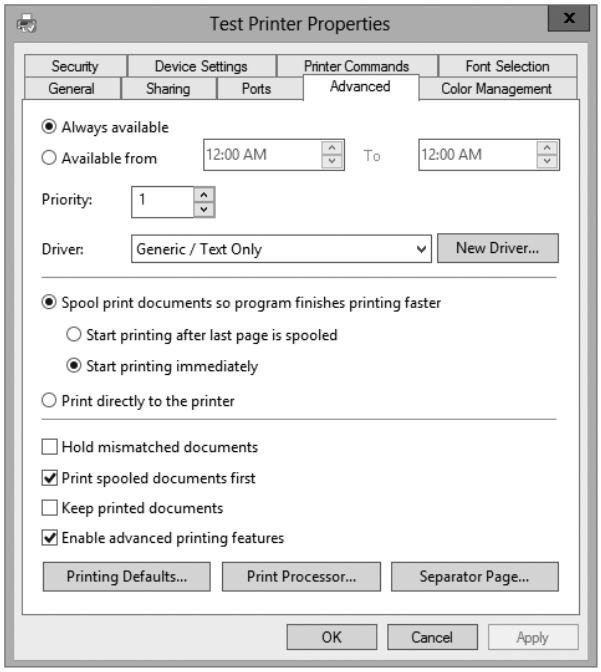
The Advanced Tab The Advanced tab (see Figure 4.12) is where you can set availability, priority, and many other options.

- The availability controls let you set the hours when this printer can be used. You can set it to be always available or available only between the hours you set.
- If multiple print shares are set up to go to the same printer, you can specify a printer priority with the Priority field for each share. The higher the number, the faster a print job sent to that share will access the printer. The highest priority is 99, and the default

(lowest) is 1. If two users send jobs to the same printer at the same time, one with a 99 priority and the other with a 1 priority, the 99 priority would print first.

- Driver is the default printer driver that the printer is using.
- The print spooling controls let you decide how the print job will spool. You can choose to have the entire job spool first before printing (this ensures that the entire job is received by the print queue before printing), to start printing immediately while the job is still spooling, or to print directly to the printer without spooling. (The last option requires a printer with a large amount of RAM on the motherboard.)
- Hold Mismatched Documents allows the spooler to hold any print jobs that don't match the setup for the print device.
- Print Spooled Documents First allows a completely spooled printer job to be printed first even if it has a lower priority number than a job that is still spooling.
- Usually, after a print job has been printed, the print queue deletes the print job. If you check the Keep Printed Documents box, the print queue will not delete the print job after it is printed.
- Enable Advanced Printing Features allows you to set some advanced features such as the Page Order and Pages Per Sheet settings.

FIGURE 4.12 Advanced tab of the printer's Properties dialog box

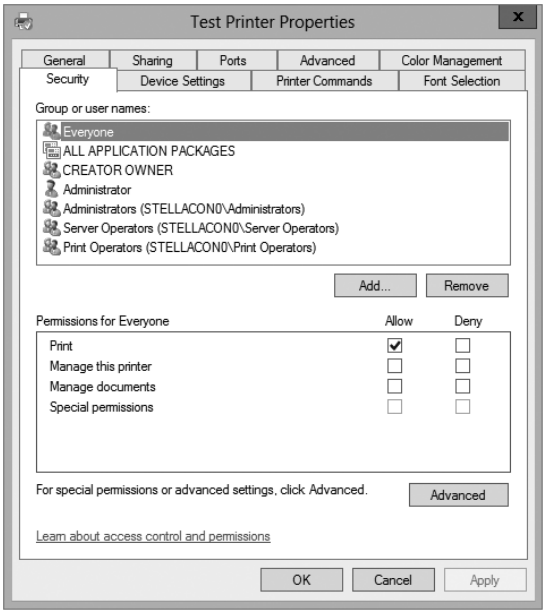


The Color Management Tab This tab allows you to adjust the color of your printing jobs.

The Security Tab The Security tab (see Figure 4.13) is where you can set the permissions for your printer. This allows users to print, manage printers, manage documents, and take advantage of special permissions.

- The Add button allows you to add users and groups to the printer.
- The Remove button allows you to remove users and groups from the printer.
- The following controls, available in the Permissions For Everyone box, apply to everyone on your network:
    - Print gives everyone the right to print to this printer.
    - Manage Printers gives everyone the right to manage this printer, including deleting print jobs, setting priorities, setting availability, and so on.
    - Manage Documents gives everyone the right to manage print jobs.
    - Special Permissions allows you to set unique permissions such as Print, Manage Printers, Read permissions, Change permissions, and Take Ownership.

FIGURE 4.13 Security tab of the printer's Properties dialog box



Migrating Print Servers

In a network environment, an administrator may find it necessary to replace older print servers or to consolidate multiple print servers into one. To do this print server migration or

replacement, you can use the Printer Migration Wizard or the `Printbrm.exe` command-line tool. These two utilities allow you to export print queues, printer settings, printer ports, and language monitors. These utilities then allow you to import these settings on another print server running Windows Server 2012 R2.

Printer Pooling

In a large organization, one issue that you may run into when you print a document to a print device is that you may have to wait a while for that document to print. If you have hundreds of print jobs being sent to a print device, it could take time until your print job appears on the print device. This is where printer pools can help.

A *printer pool* allows an administrator to associates multiple printers (identical print devices) with a single set of printer software. When you send a print job to a device, the print job will print to the first available device in the printer pool. This allows print jobs to print faster to multiple devices. For this to work, you must make sure that all devices are in the same physical area. You do not want a user traveling all over the company looking for their print job because they don't know which device printed the job.

To set up a printer to print to multiple devices, follow these steps:

1. Open Devices and Printers.
2. Right-click the printer you are using and then click Printer Properties.
3. On the Ports tab, select the Enable Printer Pooling check box.
4. Click each port where the printers you want to pool are connected.

Easy Print Driver

One printer configuration that is a little different from normal is when you are setting up a printer for a Remote Desktop server. However, Microsoft has included a feature to help. That feature is called the *Easy Print Driver*.

Remote Desktop Services gives you the ability to do printer redirection. What this means is Remote Desktop can route printing jobs from a server to a printer that is attached to a client computer. On an RD Session Host server, an administrator has the ability to use the Remote Desktop Easy Print printer driver to help simplify printer configuration.

The RD Session Host server first tries to use the Remote Desktop Easy Print driver, and if the RD client computer does not support this driver, the server looks for a matching printer driver on the server.

Configuring Remote Management

As an administrator, sometimes you might need to manage a server remotely. There are a few different tools you can use to do this task. You can use remote administration to help configure services on a Windows Server 2012 R2 system. The following sections cover Windows Remote Management and Windows PowerShell.

Windows PowerShell does not always have to be used remotely. For example, you can use Windows PowerShell when configuring a Windows Server 2012 R2 Server Core installation locally.

Windows Remote Management

The *Windows Remote Management (WinRM) utility* is Microsoft's version of the WS-Management protocol, an industry-standard protocol that allows different vendors' operating systems and hardware to work together. There are three main ways to access the WinRM utility:

- WinRM command-line tool
- WinRM scripting objects
- Windows Remote Shell command-line tool

The WinRM utility allows you to execute commands remotely and obtain management data from local and remote computers. You can use the WinRM utility on both Windows-based operating systems and non-Windows-based operating systems.

When using the WinRM utility, you can use the `-machine` switch to indicate the remote machine to which you are connecting. When connecting to a machine, you can connect using the localhost name, the NetBIOS name, the fully qualified domain name (FQDN), or the IP address of the remote machine. The following is an example of a WinRM command using a FQDN name on the secure port 443:

```
winrm get -machine:server.stellacon.local -port:443
```

Table 4.3 shows the command-line WinRM commands and descriptions of what each command does.

TABLE 4.3 WinRM commands and descriptions

Command	Description
`WinRM g` or `WinRM get`	Retrieves management information
`WinRM s` or `WinRM set`	Modifies management information
`WinRM c` or `WinRM create`	Creates a new instance on the managed resources
`WinRM d` or `WinRM delete`	Removes an instance from a managed resource
`WinRM e` or `WinRM enumerate`	Lists all instances of a managed resource
`WinRM i` or `WinRM invoke`	Executes a method on a managed resource
`WinRM id` or `WinRM identity`	Determines whether a WS-Management implementation is running on a remote machine

`WinRM quickconfig`	Configures a machine to accept WS-Management commands from a remote machine
`WinRM configSDDL`	Modifies an existing security descriptor for a Uniform Resource Identifier (URI)
`WinRM helpmsg`	Displays error messages for an error code

Now that you have looked at WinRM, let's take a look at how to use the Windows PowerShell utility.

Windows PowerShell

Windows PowerShell is a task-based, command-line scripting utility that allows you to execute commands locally or remotely on a Windows Server 2012 R2 machine. It was specifically designed for system administrators to allow for local or remote administration.

Microsoft asks a lot of questions on the exam about Windows PowerShell. Therefore, I will be discussing PowerShell throughout this book because of its importance on all of the Windows Server 2012 R2 exams.

Most operating system shells, including `Cmd.exe` and the SH, KSH, CSH, and BASH Unix shells, work by running a command or utility in a new process and then presenting the results to the user as text. These system shells also have commands that are built into the shell and execute in the shell process. In most system shells, because there are only a few built-in commands, many utilities have been created over the years to complete tasks.

Windows PowerShell contains an interactive prompt and a scripting environment that can be used independently or in combination. Unlike the previously mentioned system shells, which accept and return text, Windows PowerShell is built using the *.NET Framework common language runtime (CLR)* and the .NET Framework. Because of this, Windows PowerShell accepts and returns .NET Framework objects. This important change in the shell allows you to use entirely new tools and methods to manage and configure Windows.

Windows PowerShell introduced the concept of using cmdlets (pronounced "command-lets"). Cmdlets are simple, single-function command-line tools built into the shell. Administrators can use the cmdlets independently, or they can combine these tools to execute complex tasks and harness the true power of PowerShell. Windows PowerShell includes more than a hundred core cmdlets, but the true advantage of PowerShell is that anyone can write their own cmdlets and share them with other users.

Administrators often automate the management of their multicomputer environments by running sequences of long-running tasks, or *workflows*, which can affect multiple managed computers or devices at the same time. Windows PowerShell can help administrators accomplish workflows in a more effective way. Windows PowerShell includes some of the following advantages:

Windows PowerShell Scripting Syntax Administrators can use Windows PowerShell scripting expertise to create script-based tasks by using the extensible Windows PowerShell language. Windows PowerShell script-based tasks are easy to create, and IT members can share them easily by entering them into an email or publishing them on a web page.

Day-to-Day Management tasks Windows PowerShell allows administrators to configure and maintain servers. PowerShell allows you to pre-create scripts or use ready-to-use scripts to handle day-to-day tasks. This way, an administrator can just run a script to complete server configurations or management.

Multiserver Management Administrators can concurrently apply workflow tasks to hundreds of managed servers and computers. Windows PowerShell includes common parameters to set workflows automatically, such as `PSComputerName`, to enable multicomputer administrative scenarios.

Single Task to Manage Complex, End-to-End Processes Administrators can combine related scripts or commands that act upon an entire scenario into a single workflow. The status of activities within the workflow can be viewed at any time.

Automated Failure Recovery Using Windows PowerShell allows workflows to survive both planned and unplanned interruptions, such as computer restarts. Administrators have the ability to suspend workflow operations and then restart or resume the workflow from the exact point at which it was suspended. Administrators can then create checkpoints as part of their workflow process so that they can resume the workflow from the last persisted task (or checkpoint) instead of restarting the workflow from the beginning.

Activity Retries Administrators can create workflows that also specify activities that must rerun if the activity does not get completed on one or more managed computers (for example, if a target node was not online at the time the activity was running).

Connect and Disconnect Administrators can connect and disconnect from the node that is executing the workflow, but the workflow will continue to run.

Configuring Non-Domain Servers Another advantage of PowerShell is the ability to configure non-domain servers from a Windows Server 2012 R2 server (domain member). When you are running commands on the non-domain machine, you must have access to the non-domain machine's system administrator account. Another way to configure a non-domain server is to connect through remote desktop into the non-domain server and then configure the machine or run PowerShell commands while connected through remote desktop.

Task Scheduling Workflow tasks have the ability to be scheduled and started when specific conditions are met. This is also true for any other Windows PowerShell cmdlet or script.

Table 4.4 defines a few of the cmdlets available in Windows PowerShell. Again, there are hundreds of cmdlets, and the ones listed in the table are just some of the more common ones. You can retrieve a list of all the cmdlets starting here:

`http://technet.microsoft.com/en-us/scriptcenter/dd772285.aspx`

TABLE 4.4 Windows PowerShell cmdlets

Cmdlet	Definition
`Clear-History`	Deletes entries from the command history
`Invoke-command`	Runs commands on local or remote computers
`Start-job`	Starts a Windows PowerShell background job
`Stop-job`	Stops a Windows PowerShell background job
`Remove-job`	Deletes a Windows PowerShell background job
`Import-Module`	Adds modules to the current session
`Receive-job`	Gets the results of a Windows PowerShell background job
`Format-table`	Shows the results in a table format
`Out-file`	Sends the job results to a file
`Get-Date`	Gets the date and time
`Set-Date`	Sets the system time and date on a computer
`Get-event`	Gets an event in the event queue
`New-event`	Creates a new event
`Trace-command`	Configures and starts a trace of a command on a machine
`Get-WindowsFeature`	Gets a list of available and installed roles and features on the local server
`Get-WindowsFeature -ServerName`	Gets a list of available and installed roles and features on a remote server
`Get-Help Install-WindowsFeature`	Gets the syntax and accepted parameters for the `Install-WindowsFeature` cmdlet
`Uninstall-WindowsFeature`	Removes a role or feature
`Get-NetIPAddress`	Gets information about IP address configuration
`Set-NetIPAddress`	Modifies IP address configuration properties of an existing IP address
`Set-NetIPv4Protocol`	Modifies information about the IPv4 protocol configuration

Windows PowerShell Commands

I will show you Windows PowerShell commands throughout this book. If I show you how to install a role or feature in Server Manager, I will also include the Windows PowerShell equivalent.

Another advantage of Windows PowerShell is that it allows you to gain access to a file system on a computer and to access the registry, digital certificate stores, and other data stores.

Complete Exercise 4.8 to start the Windows PowerShell utility in the Windows Server 2012 R2 Server Core machine installed in the previous exercise.

EXERCISE 4.8

Starting the Windows PowerShell Utility

1. Type **`Start PowerShell`** at the Windows Server 2012 R2 Server Core command prompt.
2. When the Windows PowerShell utility starts, type **`Help`** and press Enter. This will show you the Windows PowerShell syntax and some of the commands included in Windows PowerShell.
3. At the Windows PowerShell command prompt, type **`Get-Date`**. This will show you the system's date and time.
4. At the Windows command prompt, type **`Help *`**. This will show you all of the cmdlets you can use.
5. Close the Windows PowerShell utility by typing **`Exit`**.

Configuring Down-Level Servers

As an administrator, sometimes you might have to configure a Windows Server 2008 R2 server from a Windows Server 2012 R2 machine. This is referred to as configuring a *down-level server.*

When you install Windows Server 2012 R2, Server Manager can be used to configure and manage a down-level server as long as that down-level server is running one of the following operating systems:

- Windows Server 2008 R2 SP1 (either full server or a Server Core installation)
- Windows Server 2008 SP2 (full server only)

To be able to configure the Windows Server 2008/2008 R2 servers remotely, you must first install Windows Management Framework 3.0 (WMF 3.0) and all of its prerequisites on the Windows Server 2008/2008 R2 servers. No special configuration is required on the Windows Server 2012 R2 server.

If you need to install WMF 3.0 on a Windows Server 2008 R2 Server Core installation, you can do this by using the Deployment Image Servicing and Management (DISM) commands. The command names that you would use for these features are as follows:

- MicrosoftWindowsPowerShell
- MicrosoftWindowsPowerShell-WOW64
- NetFx2-ServerCore
- NetFx2-ServerCore-WOW64

To run these commands, you would run the following in Server Core:

```
Dism /online /enable-feature: <Feature Name>
```

It is important to remember that Dism is case-sensitive in the command shown here.

Configuring Server Core

When configuring servers remotely, an administrator may have to configure a Server Core system. Let's take a look at some of the Server Core commands that can be used to do some basic server configurations.

When configuring Server Core, you may need to set the system for a static TCP/IP address. Use the following Windows PowerShell commands:

- `Get-NetIPConfiguration` allows you to view your current network configuration.
- `Get-NetIPAddress` allows you to view the IP addresses you are currently using.

If you want to set your static TCP/IP address, do the following:

1. In Windows PowerShell, run `Get-NetIPInterface`.
2. Write down the number shown in the `IfIndex` column of the output for the IP interface or the `InterfaceDescription` string for the network adapter you want to change.
3. In Windows PowerShell, run `New-NetIPAddress -InterfaceIndex 10 -IPAddress -192.168.15.2 -PrefixLength 24 -DefaultGateway -192.168.15.1`.
   - `InterfaceIndex` is the value of `IfIndex` from step 2 (in this example, `10`).

- `IPAddress` is the static IP address you intend to set (in this example, `192.168.15.2`).
- `PrefixLength` is the prefix length (another form of subnet mask) for the IP address you intend to set (in this example, `24`).
- `DefaultGateway` is the default gateway (in this example, `192.168.15.1`).

4. In Windows PowerShell, run `Set-DNSClientServerAddress -InterfaceIndex 10 -ServerAddresses 192.168.15.4`.
   - `InterfaceIndex` is the value of `IfIndex` from step 2.
   - `ServerAddresses` is the IP address of your DNS server.
5. To add multiple DNS servers, run `Set-DNSClientServerAddress -InterfaceIndex 10 -ServerAddresses 192.168.15.4,192.168.15.5`.
   - In this example, `192.168.15.4` and `192.168.15.5` are both IP addresses of DNS servers.

Another Server Core task that you may need to configure is setting the server name. In PowerShell, run the following command to rename the server: `Rename-Computer`.

As an administrator, you may also want to run PowerShell commands on one system to run on another system. You can enable Windows PowerShell Remoting by using the `Enable-PSRemoting` command.

Configuring the Windows Firewall

The final item to examine is configuring Windows Firewall remotely. Microsoft Server 2012 R2 Windows Firewall will be discussed in full detail in Chapter 6, but since I am discussing remote administration, let's look at the commands needed to configure Windows Firewall remotely.

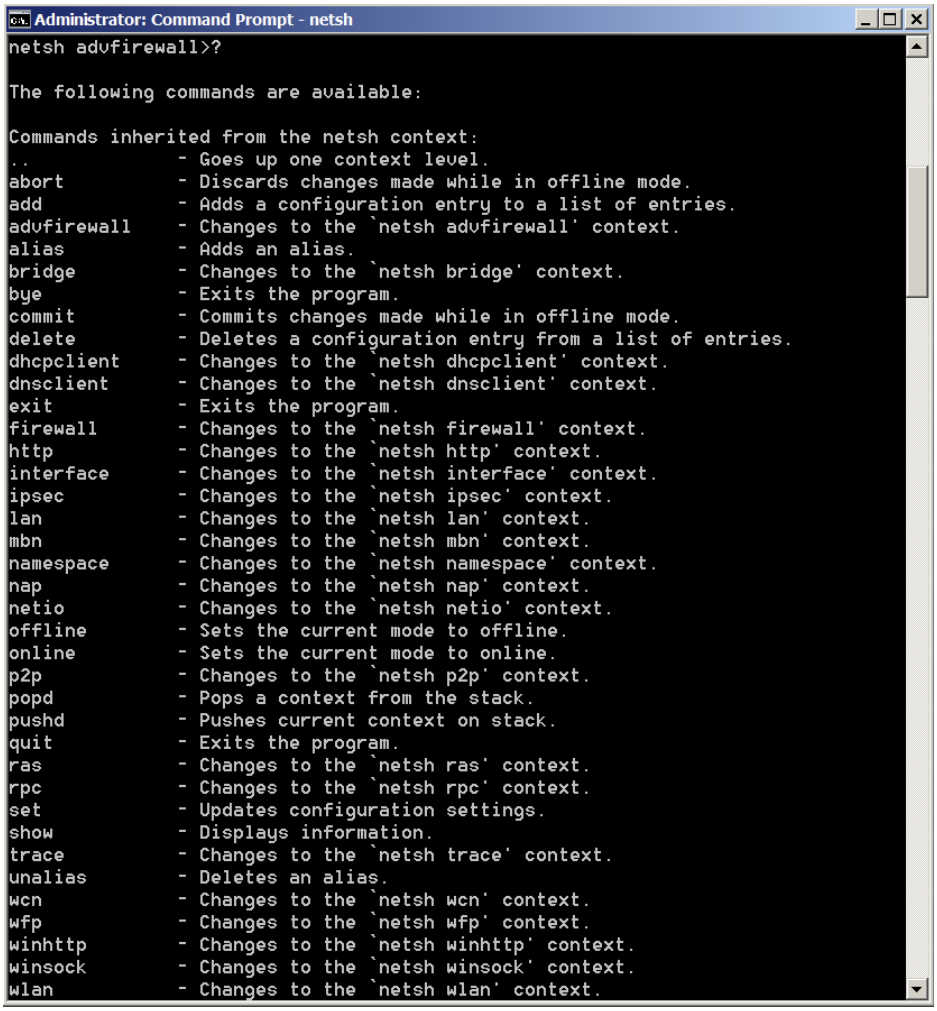
`Netsh advfirewall` is a command-line (with Administrator privileges) tool for Windows Firewall with Advanced Security that helps with the creation, administration, and monitoring of Windows Firewall and IPsec settings and provides an alternative to console-based management.

To enter into the `netsh advfirewall` prompt, you must first type **`netsh`**. After you enter the `netsh` prompt, you then type **`advfirewall`**, which will bring you to the `netsh advfirewall` prompt. When you enter `netsh advfirewall`, it enters you into a `netsh advfirewall` prompt that looks like the following:

```
netsh advfirewall> prompt
```

Once you are at the `netsh firewall` prompt, you can use the question mark to get a list of all available options (`netsh advfirewall>?`). Figure 4.14 shows you the list of available options.

FIGURE 4.14 Netsh advfirewall options



Summary

In this chapter, I discussed file servers and how they can be effective on your network. I also discussed sharing folders for users to access, and then I discussed how to publish those shared folders to Active Directory.

You learned about NTFS security versus shared folder permissions and how to limit users' hard drive space by setting up disk quotas. The chapter also covered the Encrypting File System (EFS) and how users can encrypt and compress files.

I talked about print servers and configuring printers. I talked about how to share and publish printers within Active Directory as well as print permissions, printer priorities, and print pooling.

You then took a look at remote configuration and a few tools that allow you to configure servers.

- Windows Remote Management lets you configure a server remotely from another machine.
- PowerShell is an important tool in the Windows Server 2012 R2 arsenal. Microsoft has been moving the industry toward PowerShell, and there will be many questions on the exam about PowerShell.
- `Netsh` allows you to configure Windows Firewall remotely.

Exam Essentials

Learn How Resources Can Be Published A design goal for Active Directory was to make network resources easier for users to find. With that in mind, you should understand how using published printers and shared folders can simplify network resource management.

Know How to Configure Offline Folders Offline folders give you the opportunity to set up folders so that users can work on the data while outside the office and later synchronize it with a master copy. You can set up GPOs to help with offline folder synchronization.

Know How to Configure NTFS Security One of the major advantages of using NTFS over FAT32 is access to additional security features. NTFS allows you to put security at the file and folder layers. NTFS security is in effect whether the user is remote or local to the computer with the data.

Know How to Configure Shared Permissions Shared permissions allow you to determine the access a user will receive when connecting to a shared folder. Shared permissions are allowed only at the folder layer and are in effect only when the user is remote to the computer with the shared data.

Understand How NTFS and Shared Permissions Work Together NTFS and shared permissions are individually additive—you get the highest level of security and permissions within each type. NTFS is always in effect, and it is the only security available locally. Shared permissions are in effect only when connecting remotely to access the shared data. When the two types of permissions meet, the most restrictive set of permissions applies.

Know How to Configure Disk Quotas Disk quotas allow an organization to determine the amount of disk space that users can have on a volume of a server. An administrator can set up disk quotas based on volumes or by users. Each volume must have its own separate set of disk quotas.

Know How to Configure Printing I discussed network printers versus print servers. Understand that when you create a printer, you want to publish the printer within Active Directory so that your users can find it throughout the domain. Understand the different printer permissions and how to install print drivers.

Understand Windows PowerShell Understanding Windows PowerShell is not only important for the exam; it will also allow you to configure Server Core more efficiently. Windows PowerShell is a command-line utility that allows you run single cmdlets as well as run complex tasks to exploit the full power from PowerShell.

Review Questions

1. The company for which you work has a multilevel administrative team that is segmented by departments and locations. There are four major locations, and you are in the Northeast group. You have been assigned to the administrative group that is responsible for creating and maintaining network shares for files and printers in your region. The last place you worked had a large Windows Server 2003 network, where you had a much wider range of responsibilities. You are excited about the chance to learn more about Windows Server 2012 R2.

   For your first task, you have been given a list of file and printer shares that need to be created for the users in your region. You ask how to create them in Windows Server 2012 R2, and you are told that the process of creating a share is the same as with Windows Server 2003. You create the shares and use `NETUSE` to test them. Everything appears to work fine, so you send out a message that the shares are available. The next day, you start receiving calls from users who say they cannot see any of the resources you created. What is the most likely reason for the calls from the users?

   A. You forgot to enable NetBIOS for the shares.

   B. You need to force replication for the shares to appear in the directory.

   C. You need to publish the shares in the directory.

   D. The shares will appear within the normal replication period.

2. You want to publish a printer to Active Directory. Where would you click in order to accomplish this task?

   A. The Sharing tab

   B. The Advanced tab

   C. The Device Settings tab

   D. The Printing Preferences button

3. A system administrator creates a local Printer object, but it doesn't show up in Active Directory when a user executes a search for all printers. Which of the following are possible reasons for this? (Choose all that apply.)

   A. The printer was not shared.

   B. The printer is offline.

   C. The client does not have permission to view the printer.

   D. The printer is malfunctioning.

4. You are the network administrator for a midsize coffee bean distributor. Your company's network has four Windows 2012 R2 servers, and all of the clients are running either Windows 8 or Windows 7. Most of your end users use laptops to do their work, and many of them work away from the office. What should you configure to help them work on documents when away from the office?

A. Online file access

B. Offline file access

C. Share permissions

D. NTFS permissions

5. Your company has decided to implement a Windows 2012 R2 server. The company IT manager who came before you always used FAT32 as the system partition. Your company wants to know whether it should move to NTFS. Which of the following are some advantages of NTFS? (Choose all that apply.)

A. Security

B. Quotas

C. Compression

D. Encryption

6. Will, the IT manager for your company, has been asked to give Moe the rights to read and change documents in the `Stellacon Documents` folder. The following table shows the current permissions on the shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Tylor	Read	Change

Moe is a member of the Sales and Finance groups. When Moe accesses the `Stellacon Documents` folder, he can read all of the files, but the system won't let him change or delete files. What do you need to do to give Moe the minimum amount of rights to do his job?

A. Give Sales Full Control to shared permissions.

B. Give Moe Full Control to NTFS security.

C. Give Finance Change to shared permissions.

D. Give Finance Modify to NTFS security.

E. Give Moe Modify to NTFS security.

7. You are the administrator of your network, which consists of two Windows Server 2012 R2 systems. One of the servers is a domain controller, and the other server is a file server for data storage. The hard drive of the file server is starting to fill up. You do not have the ability to install another hard drive, so you decide to limit the amount of space everyone gets on the hard drive. What do you need to implement to solve your problem?

A. Disk spacing

B. Disk quotas

C. Disk hardening

D. Disk limitations

8. You are the IT manager for your company. You have been asked to give the Admin group the rights to read, change, and assign permissions to documents in the `Stellacon Documents` folder. The following table shows the current permissions on the `Stellacon Documents` shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Admin	Change	Change

What do you need to do to give the Admin group the rights to do their job? (Choose all that apply.)

A. Give Sales Full Control to shared permissions.

B. Give Full Control to NTFS security.

C. Give Admin Full Control to shared permissions.

D. Give Finance Modify to NTFS security.

E. Give Admin Full Control to NTFS security.

9. You have been asked to configure a Windows Server 2012 R2 Datacenter Server Core machine. Which remote configuration applications can you use to configure this server from your machine? (Choose all that apply.)

A. Windows Remote Management

B. Command prompt

C. Windows PowerShell

D. Microsoft Remote Admin (MRA)

10. You have been hired by a small company to implement new Windows Server 2012 R2 systems. The company wants you to set up a server for users' home folder locations. What type of server would you be setting up?

A. PDC server

B. Web server

C. Exchange server

D. File server