

MCTS/MCITP Exam 648

Maintaining an Active Directory Environment

Exam objectives in this chapter:

- Backup and Recovery
- Offline Maintenance
- Monitoring Active Directory

Exam objectives review:

- ☒ Summary of Exam Objectives
- ☒ Exam Objectives Fast Track
- ☒ Exam Objectives Frequently Asked Questions
- ☒ Self Test
- ☒ Self Test Quick Answer Key

Introduction

Being able to implement a Windows Server 2008 Active Directory environment is only half the battle. You must also be able to maintain the environment to provide minimum downtime and optimum performance of your enterprise. Various solutions and strategies come into play as part of maintenance. Some can be seen as larger “disaster recovery” components, whereas others may simply be “tweaking” the environment to improve user experience.

In some situations, “maintenance” may fall somewhere in between—a user account is accidentally deleted, a file is accidentally deleted, or replication is underperforming or not performing at all! In this chapter, you will learn about the many maintenance and management tools offered as a part of Windows Server 2008, as well as some solutions to better improve your Windows Active Directory environment. These topics will be critical not only to your exam success, but also to your success as an IT professional. We will begin this section with a discussion of Windows Server Backup and how it has changed drastically from earlier versions of the Windows server product.

Backup and Recovery

Most people never think about backup and recovery until they need it. Microsoft has been shipping a simple backup solution with Windows since Windows NT 3.1 back in 1993. The technology used today has changed since then, but the needs are still the same. Administrators need the ability to effectively back up servers, data, and the system state while also having an easy way to restore when needed.

Windows Server 2008 does not support the old NTBackup.exe tool or its backup format. It now uses a backup feature called Windows Server Backup. This feature cannot read the old .bkf files. Therefore, it cannot restore any backups from NTBackup.exe. Windows Server Backup is primarily intended for use by small businesses and companies that do not have full-time or a highly technical IT staff.

Windows Server Backup uses the same backup technology found in Windows Vista, which is a block-level image. It uses .vhd image files just like those found in Microsoft Virtual Server. After the first full backup is complete, Windows Server Backup can be configured to automatically run incremental backups, therefore saving only the data that has changed and not the entire object over and over again. Restoration is also simplified in that an administrator no longer has to manually restore from multiple backups if an item was stored on an incremental backup. They can now restore items by choosing a backup to recover from and then select

the item(s) to restore. One thing that you cannot do in Windows Server Backup, however, is back up to tape. Tape is not a supported medium for Windows Server Backup. You can back up to disks, DVDs, and network shares.

New and Noteworthy ...

Windows Server Backup

Although you cannot use Windows Server Backup to recover files from a .bkf format, you can download a version of Windows Backup for Windows Server 2008. It is for use by administrators who need to recover data from backups taken using NTBackup. The downloadable version cannot be used to create additional backups on Windows Server 2008. To download NTBackup for Windows Server 2008 go to <http://go.microsoft.com/fwlink/?LinkId=82917>.

Using Windows Server Backup

Before using Windows Server Backup, you must install the feature. Just like many of the features within Windows Server 2008, Windows Server Backup is installed via a wizard through Server Manager. Installing the Windows Server Backup feature is easy and simple; just follow the steps in Exercise 5.1.

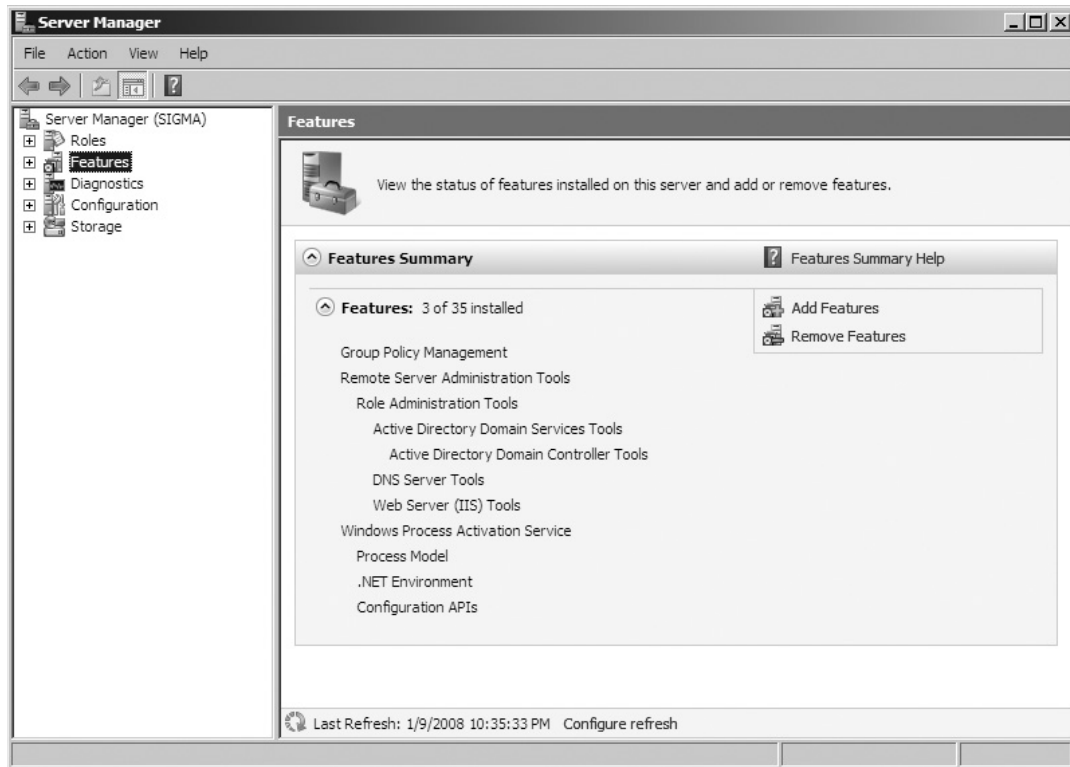
EXERCISE 5.1

INSTALLING WINDOWS SERVER BACKUP

1. Log on to Windows Server 2008 as an administrator (domain admin or local admin).
2. Click Start | Administrative Tools | Server Manager. Server Manager should come up.
3. In Server Manager, on the left window pane also known as the Console Tree, click on the top icon where it reads Server Manager <server name>. In our case, it reads Server Manager (SIGMA).

4. You'll now see a list of different options. Go to **Features** and click on it. Server Manager will show the different features installed on that particular server in the Details pane to the right of the console tree. Figure 5.1 is an example of what an administrator would see after doing this.

Figure 5.1 The List of Features Installed



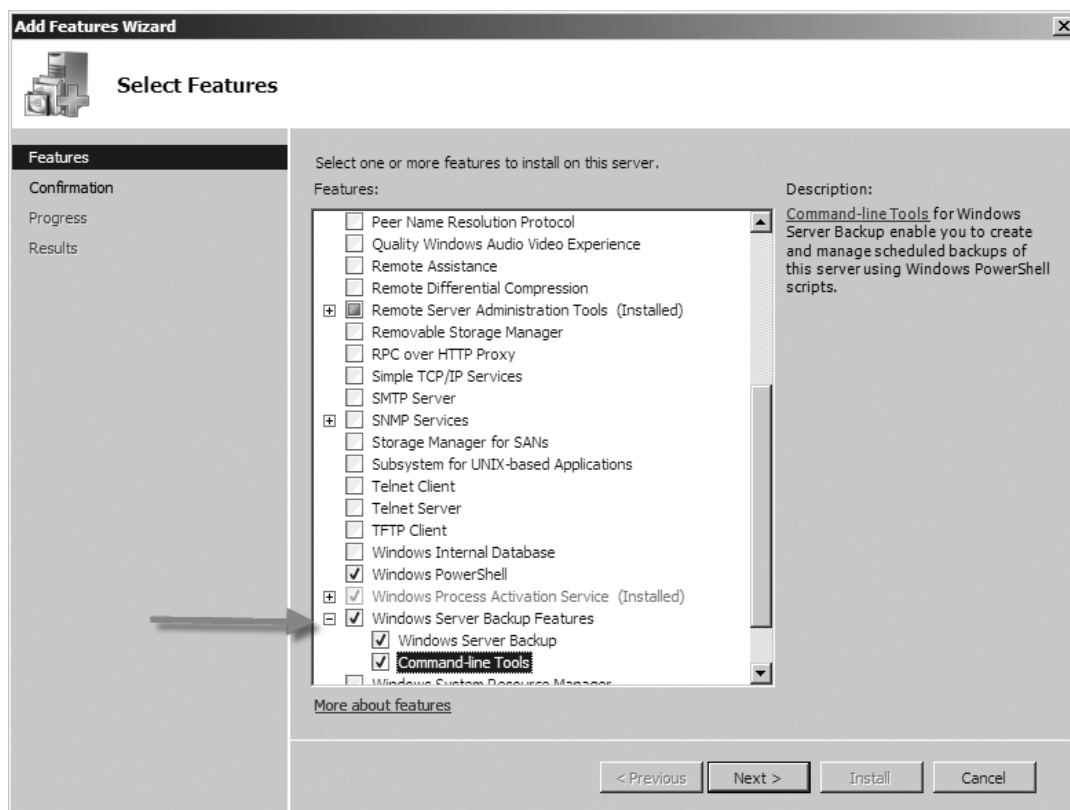
5. In the console tree, right-click **Features** and choose **Add Features**. You will now come to the **Select Features** window via the **Add Features Wizard**. Scroll down the list to where you see **Windows Server Backup Features** and put a check beside it and click **Next**. In Figure 5.2, you'll notice that you are installing the **Windows Server Backup** and the **Command-line Tools**.

Head of the Class...

Command-Line Tools

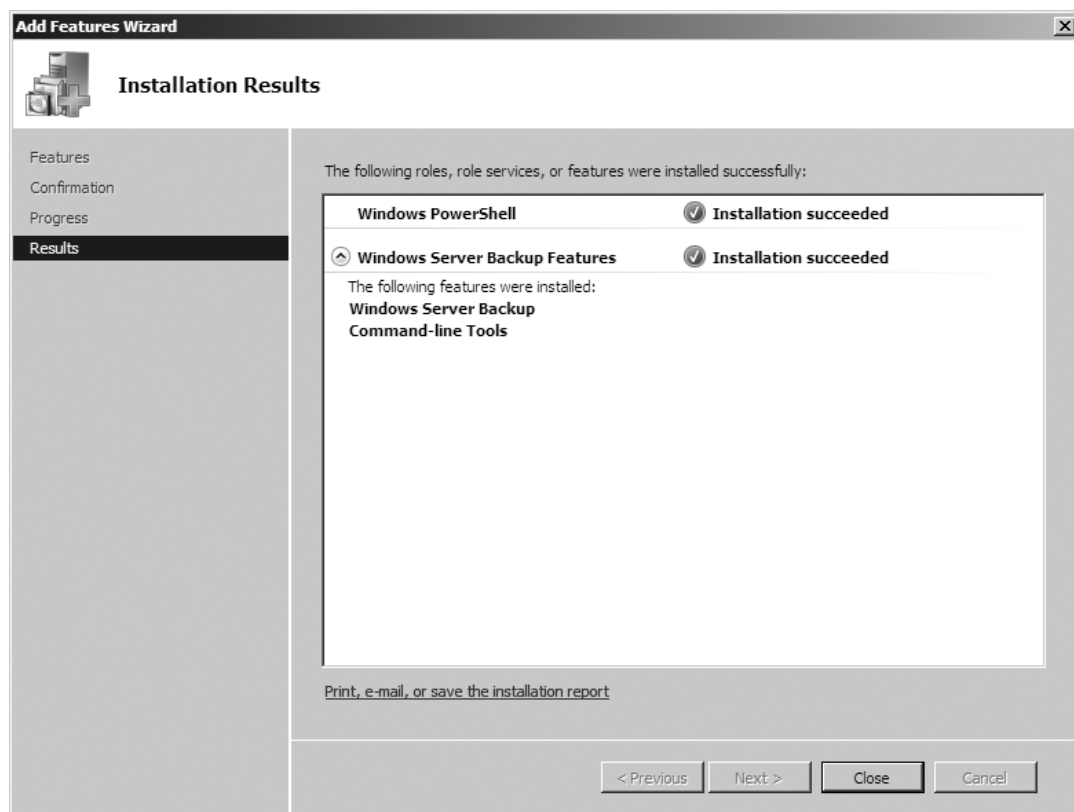
If you want to install the **Command-line Tools** with the **Windows Server Backup Features**, you must also install the **Windows PowerShell**. The Windows PowerShell is a command-line and scripting language that allows IT professionals to better control system administration and automation. It is built on top of the .NET Framework and uses cmdlets (command lets), which is a single-function command-line tool built into the shell.

Figure 5.2 Selecting Windows Server Backup Features

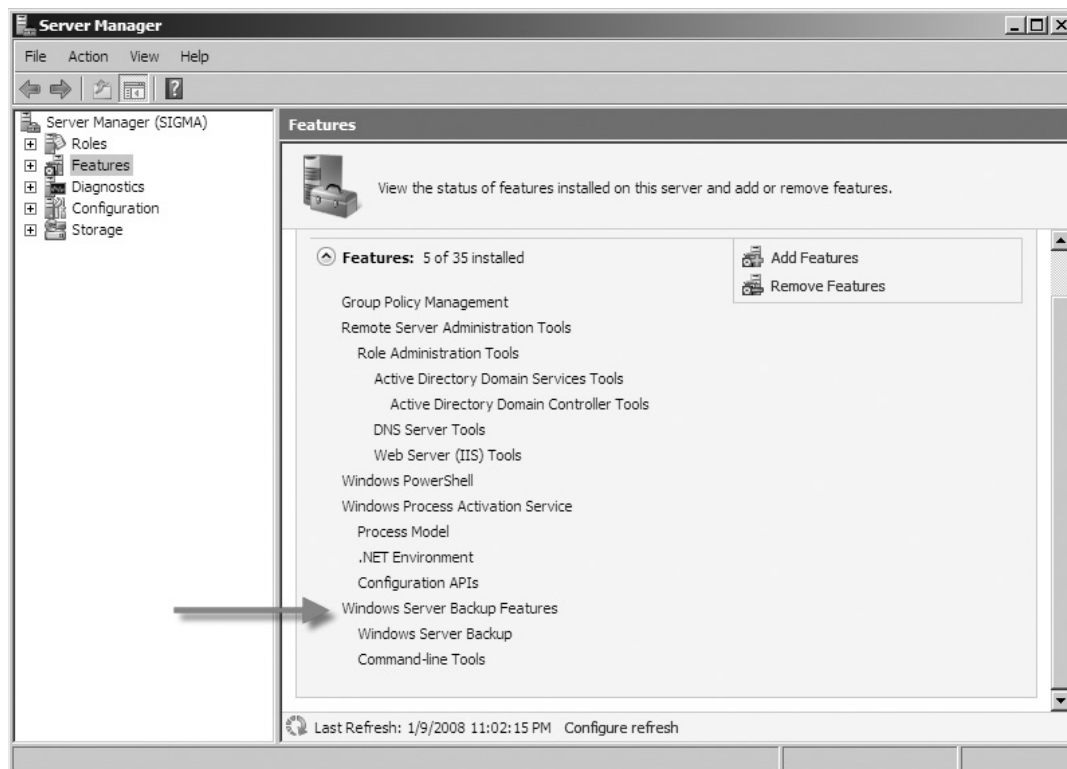


6. Now you will come to the **Confirm Installation Selections** screen. Once you've verified that the feature(s) you plan to install are shown in the confirmation list, click **Install**.
7. Once the installation has completed, you will come to the **Installation Results** screen, as shown in Figure 5.3. Notice that we installed the **Windows PowerShell** and the **Windows Server Backup Features** successfully. Once the installation is complete, click on **Close**.

Figure 5.3 Installation Results

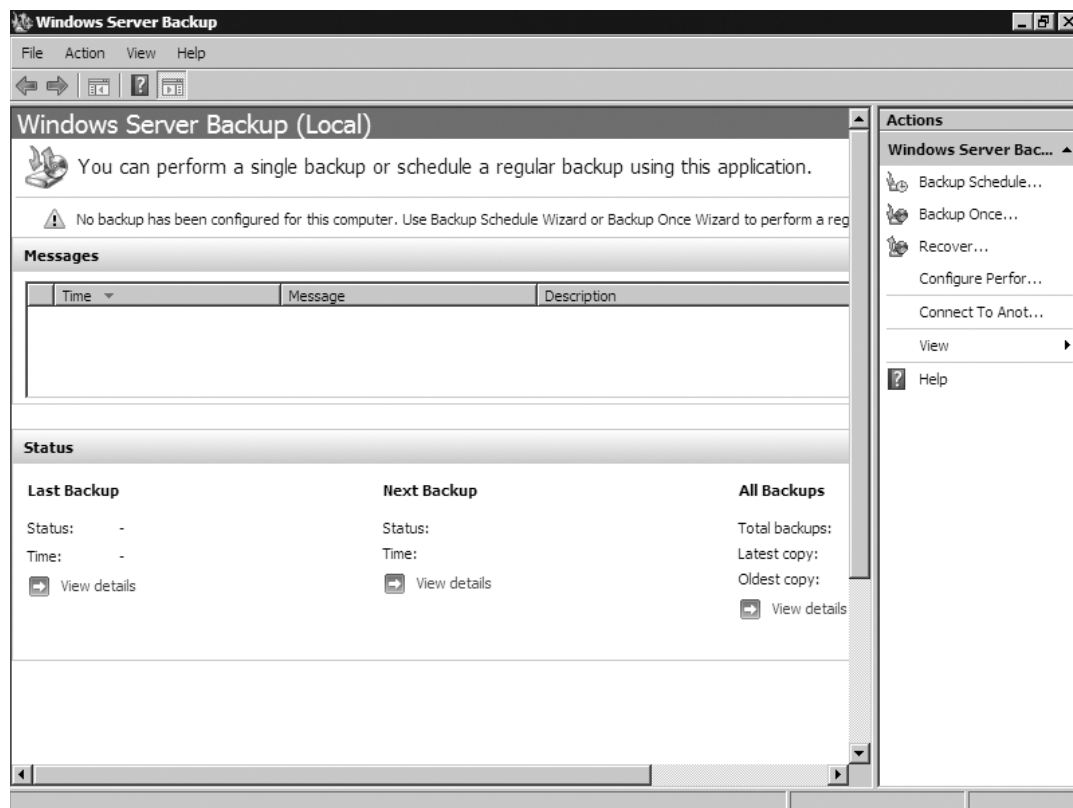


8. Back in Server Manager, you will see the list of features installed, and in the list you will see Windows Server Backup Features, just as you see in Figure 5.4.

Figure 5.4 The List of Features Installed

To use the newly installed Windows Server Backup, simply click **Start | Administrative Tools | Windows Server Backup**. As you can see in Figure 5.5, Windows Server Backup's interface is pretty straightforward. Information about backups and messages is shown in the left pane, and options such as the following are shown in the right pane:

- Backup Schedule
- Backup Once
- Recover
- Configure Performance Settings
- Connect To Another Computer

Figure 5.5 Windows Server Backup

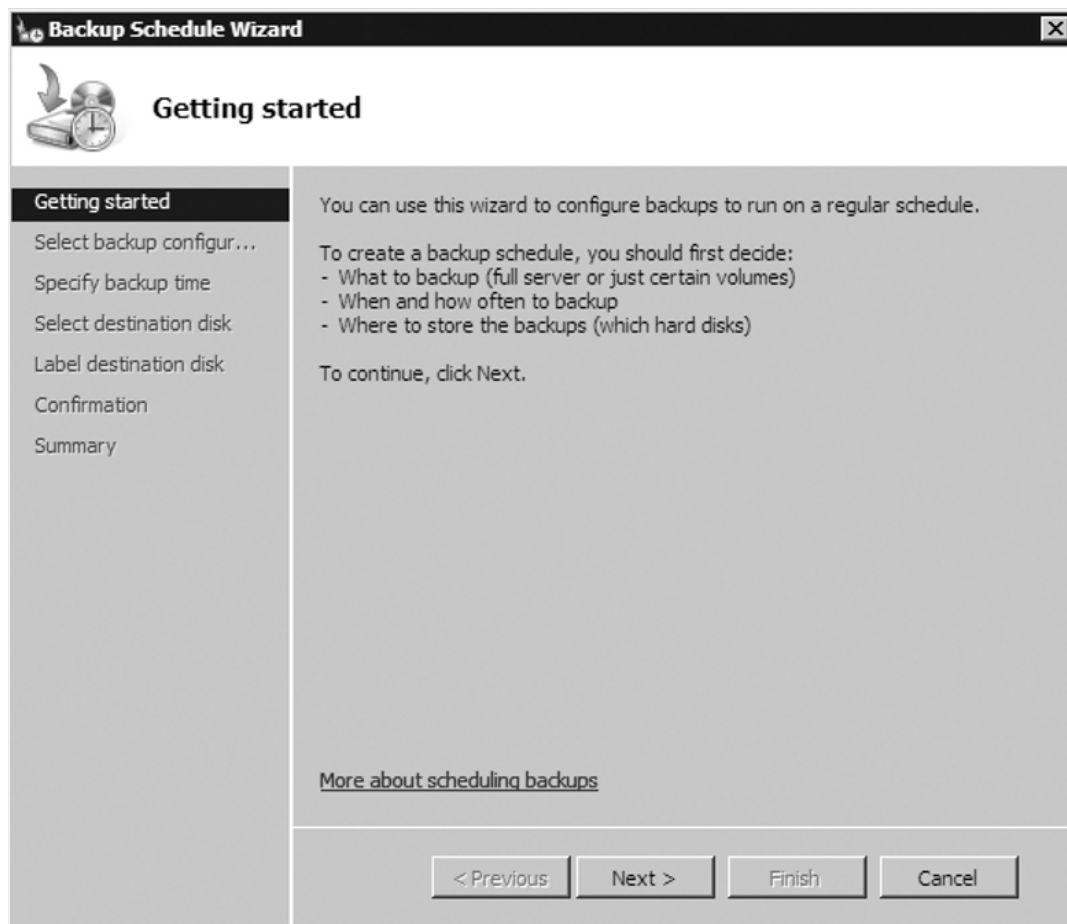
Scheduling a Backup

Windows Server Backup allows administrators and operators with sufficient rights to schedule backups to take place at certain times on a regular basis. In scheduling a backup, you need to decide what you want to back up, how often and when the backup(s) are to take place, and where to store the backup(s). To schedule a backup, follow the steps in Exercise 5.2.

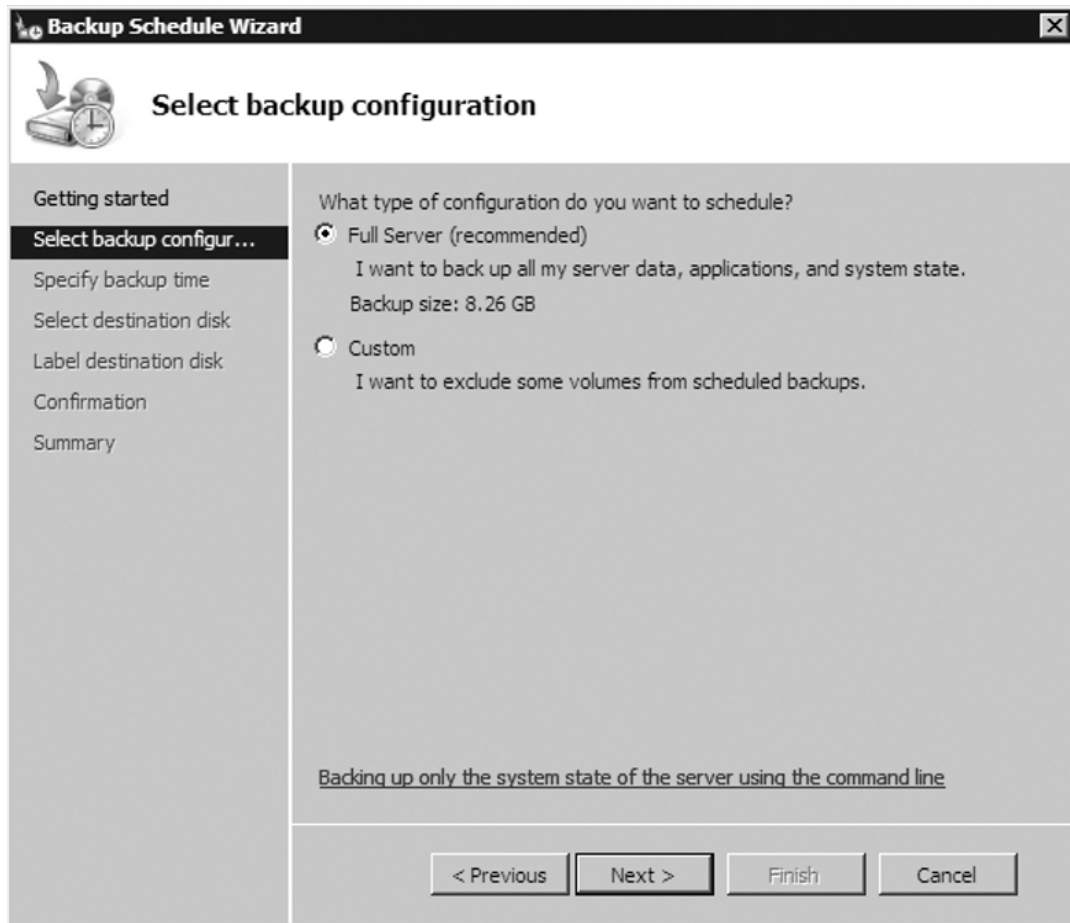
EXERCISE 5.2

SCHEDULING A BACKUP

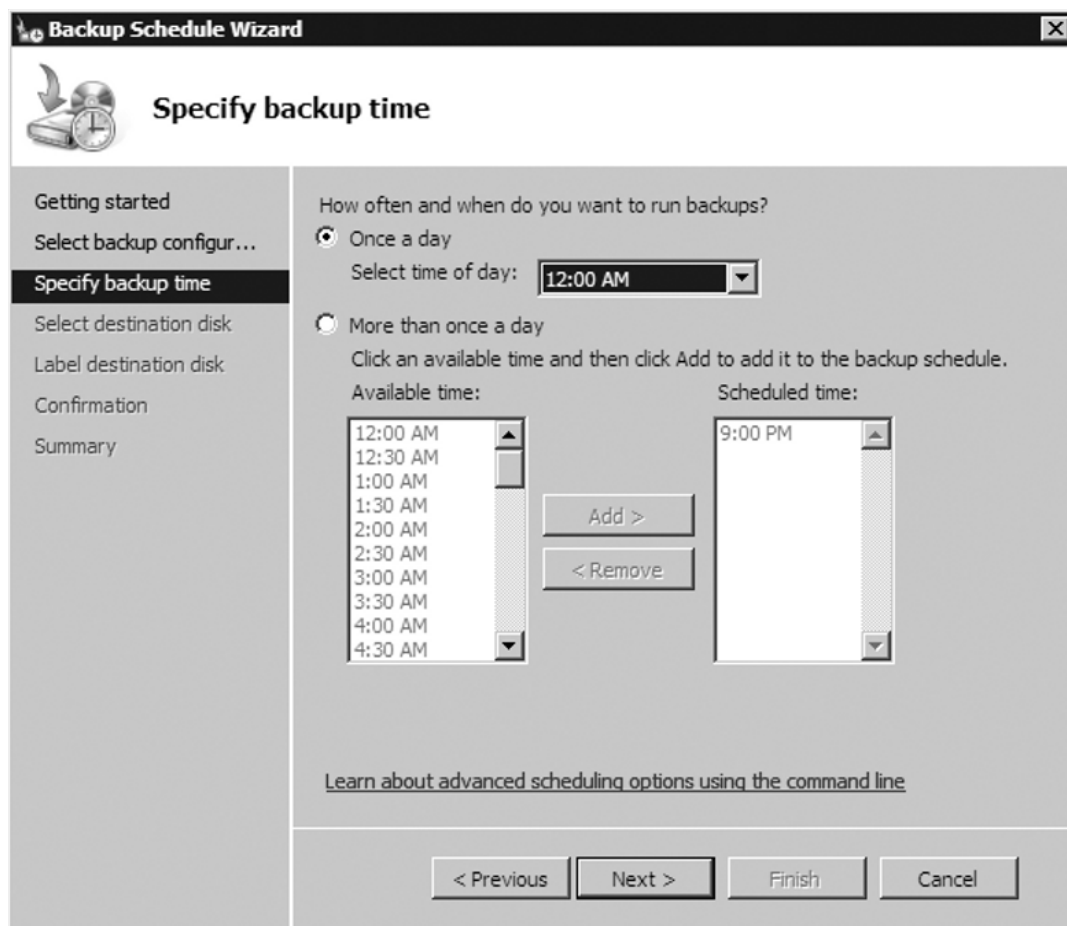
1. In **Windows Server Backup** go to the **Actions** pane and select **Backup Schedule**. This will kick off the **Backup Schedule Wizard** which you see in Figure 5.6.

Figure 5.6 The Backup Schedule Wizard's Getting Started Screen

2. Next you're asked what type of configuration you want to schedule. You can select **Full Server** or you can select **Custom**, as shown in Figure 5.7. The full server configuration will back up all data, applications, and system state. Selecting Custom, though, allows you to select which items you would prefer to back up. For our example, we will choose to conduct a **Full Server** backup. After you have made your decision just click **Next**.

Figure 5.7 Selecting Backup Configuration

3. The next thing we need to do in scheduling our backup is decide how often we want to conduct a backup and what time(s) to run it. In Figure 5.8, you see we have decided to kick off our backup once a day at midnight. After deciding when and how often backups are to take place, click **Next** to continue.

Figure 5.8 Specifying the Backup Time

4. Now we need to tell Windows Server Backup where we want to store the backup. For scheduled backups, we have to use a locally attached drive. This can be a DVD drive, a USB flash drive, or even an externally attached drive. It cannot be a network drive. Although Windows Server Backup does allow you to back up to a network drive, you are not allowed to schedule a job that does. On our system, we have a second drive listed as volume E. We will have our scheduled backup job use this as the destination; to continue we just click **Next**. You'll notice a pop-up from Windows Server Backup, letting you know that it will reformat the destination drive you selected and that it will only be dedicated to backing up files and will not show up in Windows Explorer.

To continue, just click **Yes**. Figure 5.9 shows that we have chosen the E drive as our destination disk and Figure 5.10 informs us that the destination drive will be reformatted, among other things.

Figure 5.9 Selecting the Destination Disk

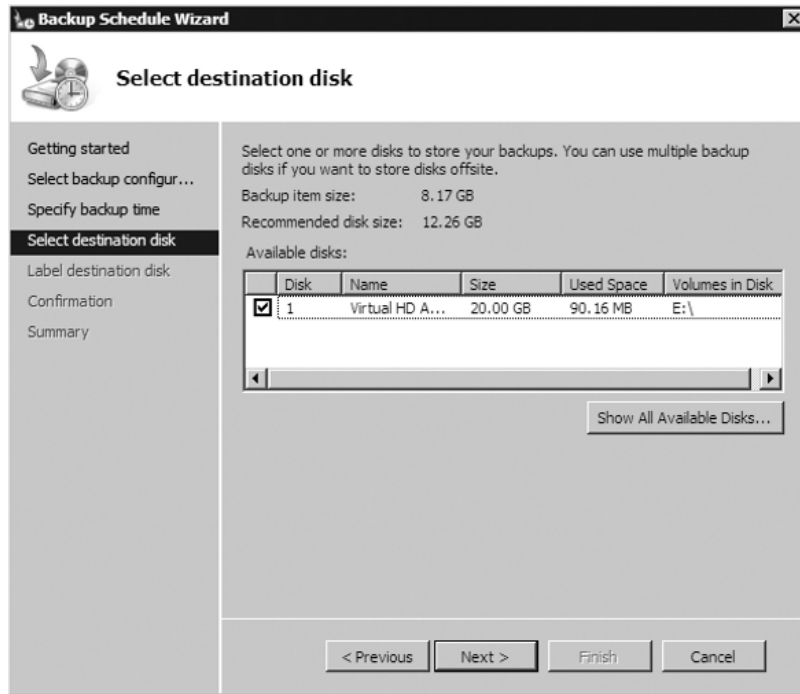
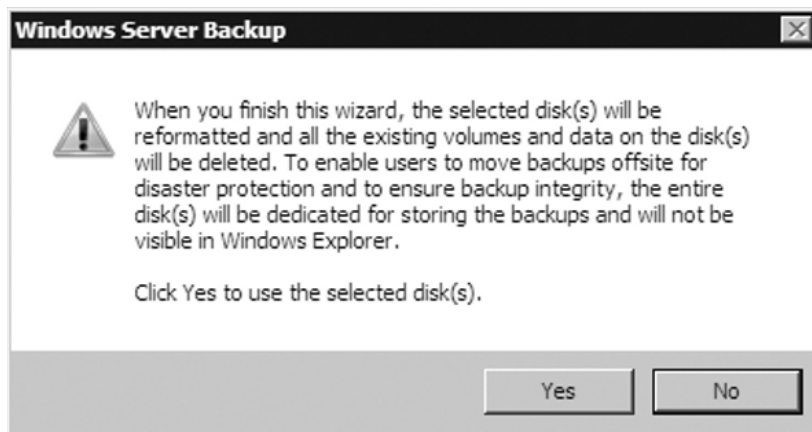
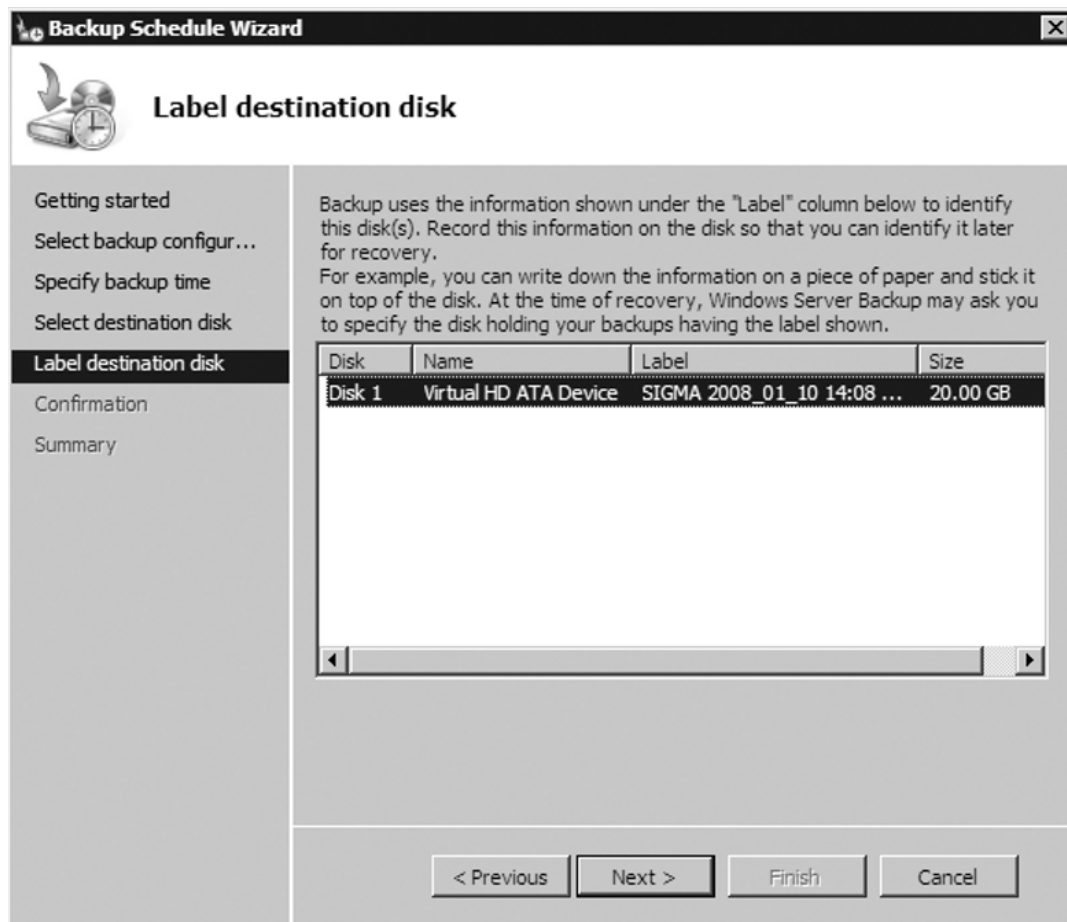


Figure 5.10 The Destination Drive Will Be Reformatted



5. Windows Server Backup will now label the destination disk. The default name will be in the form of **<server name> year_month_date <military time>**. As you see in Figure 5.11, our label will be **SIGMA 2008_01_10 14:08**. After confirming this, you can click **Next**.

Figure 5.11 Labeling the Destination Disk

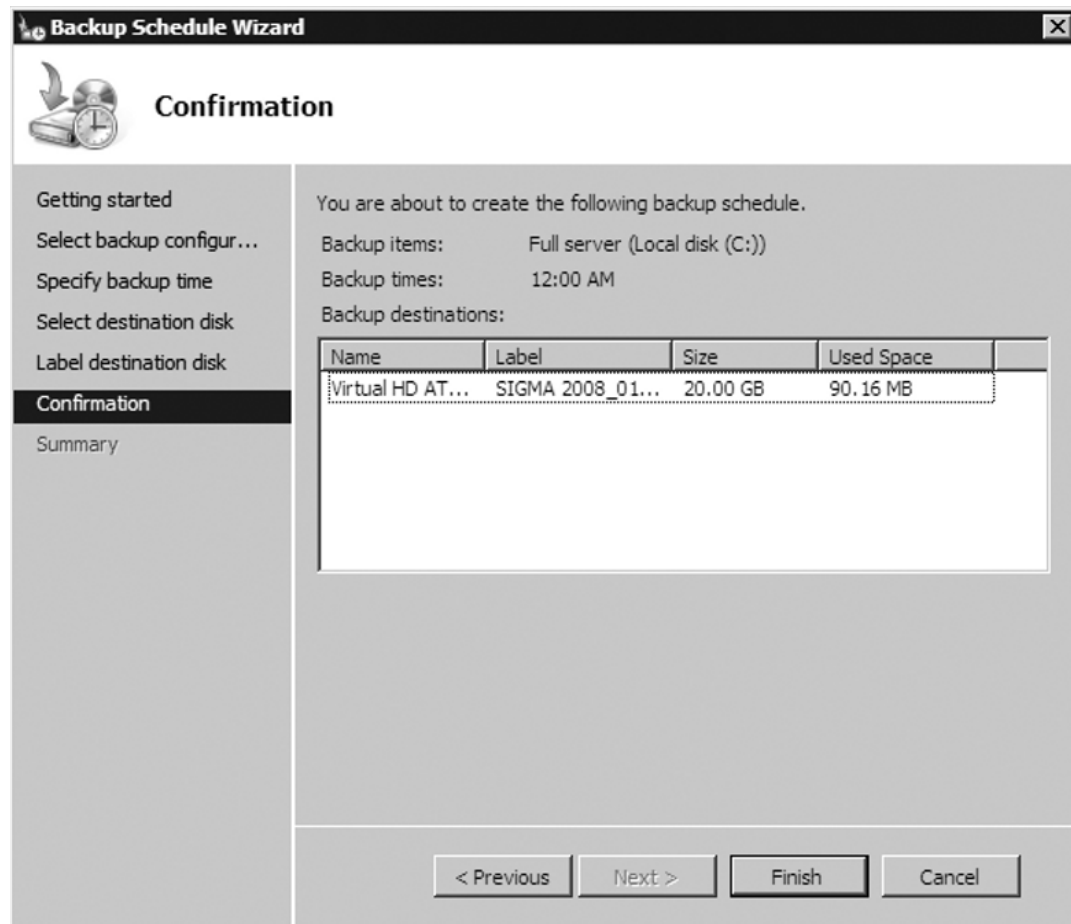


EXAM WARNING

It is highly recommended that administrators and backup operators alike write the label name on the destination drive. During recovery Windows Server Backup may specify a disk holding backups with a specific label name.

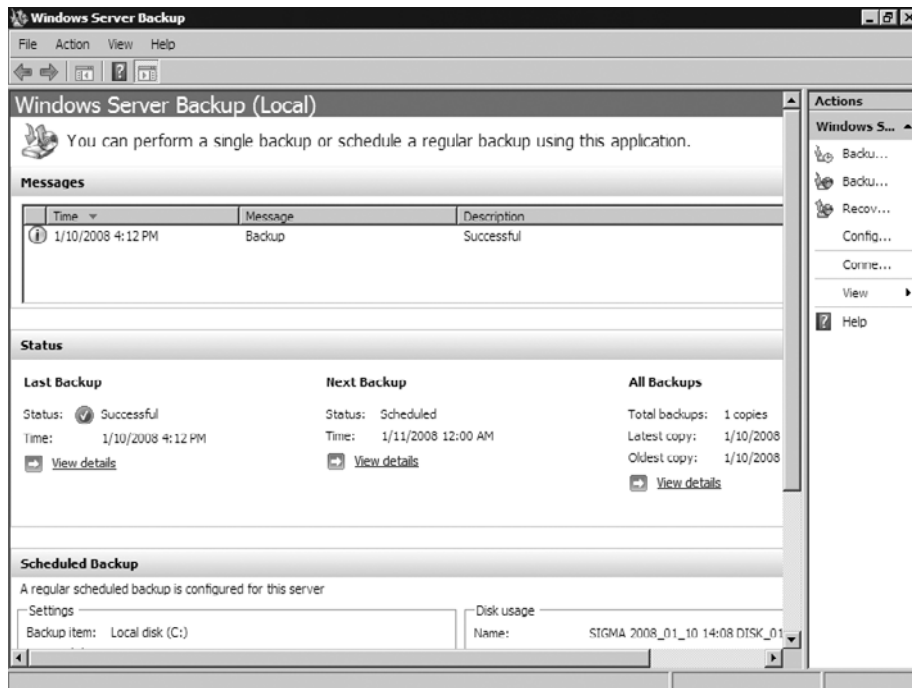
6. The final step in scheduling a backup is to confirm your selections. The **Confirmation** screen will show you what you have chosen at the backup items, times, and the destination, as you see in Figure 5.12. After you've confirmed your choices, click **Finish**.

Figure 5.12 The Backup Schedule Confirmation



Now that we have a scheduled backup, we can just wait for it to kick off at midnight. In Figure 5.13, you'll notice in Windows Server Backup we went ahead and ran a full backup. You'll see under **Messages** and **Status** that we have conducted a successful backup. We did this by going into the **Actions** pane and selecting **Backup Once**. This gave us a chance to test the backup configuration.

Figure 5.13 A Successful Backup



As you've seen, we've gone through installing Windows Server Backup, and gone over the media it supports, how to schedule a backup, and how to immediately start one. What we have not covered, which you will be tested on, is how to use the *wbadmin* command.

Wbadmin.exe is the command-line utility that comes with Windows Server Backup. It can be used to perform backups and restores from the command line or via batch files and scripts. Table 5.1 is a list of the commands supported by *wbadmin.exe*.

Table 5.1 The *wbadmin.exe* Command

Command	Description
<i>wbadmin enable backup</i>	Enables or configures scheduled daily backups
<i>wbadmin disable backup</i>	Disables running scheduled daily backups
<i>wbadmin start backup</i>	Runs a backup job

Continued

Table 5.1 Continued. The wbadmin.exe Command

Command	Description
<i>wbadmin stop job</i>	Stops a running backup or recovery job
<i>wbadmin get versions</i>	Reports information about the available backups
<i>wbadmin get items</i>	Lists the items included in a backup based on parameters you specify
<i>wbadmin start recovery</i>	Runs a recovery of the volumes, applications, or files and folders specified
<i>wbadmin get status</i>	Gives the status of a backup or recovery job
<i>wbadmin get disks</i>	Lists disks that are currently online
<i>wbadmin start systemstaterecovery</i>	Recovers the system state from a backup
<i>wbadmin start systemrecovery</i>	Runs a full system recovery. Available only if you are using the Windows Recovery environment.
<i>wbadmin start recovery</i>	Runs a recovery
<i>wbadmin restore catalog</i>	Recovers a catalog that has been corrupted. Helpful in times if the recovery from the backup catalog has been corrupted.
<i>wbadmin delete catalog</i>	Deletes a catalog that has been corrupted
<i>wbadmin start systemstatebackup</i>	Runs a system state backup
<i>wbadmin delete systemstatebackup</i>	Deletes a system state backup(s)

Backing Up to Removable Media

Windows Server 2008, WBS can back up to removable media such as DVD and USB-based flash drives. Although the wizard-driven GUI interface cannot back up to removable media, wbadmin.exe can. One of the big advantages of being able to back up to removable media is that you can easily take it offsite. One disadvantage to using removable media with WBS is that recovery can be done only at the volume level. It cannot be done by recovering individual files or folders that can

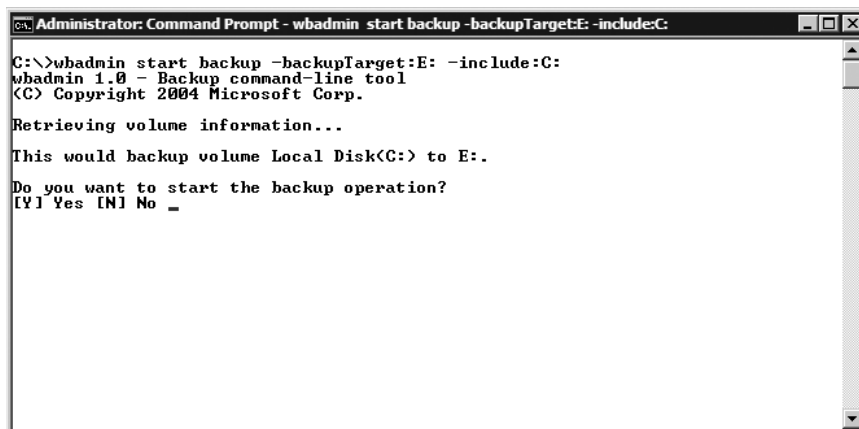
be done only via the GUI which does not support removable media. So, how do we back up to removable media? That's a good question. In Exercise 5.3, we will back up a server to DVDs.

EXERCISE 5.3

BACKING UP TO DVD

1. Make sure your system has a DVD burner either attached to it or internal to the server.
2. Log on as either the Administrator or a member of the Backup Operators.
3. Put a blank DVD in the DVD burner.
4. Open a command prompt (**Start | Command Prompt**); at the prompt type **wbadmin start backup -backupTarget:E: -include:C:** and then press **Enter**. You should see a screen similar to that shown in Figure 5.14 (if your DVD drive is another drive letter instead of E, use that drive letter for the *backupTarget* argument).

Figure 5.14 Backing Up the Server to DVD



5. At the **Do you want to start the backup operation?** prompt, type **Y** for yes and press **Enter**.
6. Now you are told to insert new media, which in this case is a DVD, which we will label as **SIPOC 2008_01_14 23:19 DVD_01**, as shown in Figure 5.15. The naming standard is **<server name>**

<year_month_date> <time (in military time)> <type of media number of media just used>. So, take the first DVD out, write down the proper label, and put in a newly blank DVD and type C to continue. For our example, we are also asked to submit a third DVD. The second DVD will have the name **SIPOC 2008_01_14 23:19 DVD_02** and any additional DVDs will have the same name except for the DVD_##.

Figure 5.15 Labeling the First DVD and Continuing

```
Administrator: Command Prompt - wbadmin start backup -backupTarget:E: -include:C:
C:\>wbadmin start backup -backupTarget:E: -include:C:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Retrieving volume information...

This would backup volume Local Disk(C:) to E:.

Do you want to start the backup operation?
[Y] Yes [N] No y

Backup to E: is starting.

Creating the shadow copy of volumes requested for backup.
Creating the shadow copy of volumes requested for backup.
Creating the shadow copy of volumes requested for backup.
Creating the shadow copy of volumes requested for backup.

Label new media as SIPOC 2008_01_14 23:19 DVD_01. This information will be used
to identify this
backup media in a recovery.

Insert the new media into drive E:. To continue, click [C] after inserting new
media. To exit, click [E].
[C] Continue [E] Exit
```

7. Once the backup is complete, you will get a summary by wbadmin similar to the one in Figure 5.16. After you're finished with the backup, just take the last DVD out of the DVD burner.

Figure 5.16 The Completed Backup

```
Administrator: Command Prompt
media. To exit, click [E].
[C] Continue [E] Exit c

Formatting media...
Formatting media...
Running backup of volume Local Disk(C:), copied (98%).
Running backup of volume Local Disk(C:), copied (98%).
Running backup of volume Local Disk(C:), copied (99%).
Running backup of volume Local Disk(C:), copied (99%).
Running backup of volume Local Disk(C:), copied (99%).
Running backup of volume Local Disk(C:), copied (99%).
Running backup of volume Local Disk(C:), copied (100%).
Verification 4% complete...
Verification 21% complete...
Verification 42% complete...
Verification 76% complete...
Verification 100% complete...
Backup completed successfully.

Summary of backup:

Backup of volume Local Disk(C:) completed successfully.

C:\>
```

Head of the Class...

Unformatted DVDs

If a DVD is unformatted, Windows Server 2008 will automatically format it during the backup.

Backing Up System State Data

The components that make up the system state in Windows Server 2008 depend on the role(s) that are installed on a server and which volumes host the critical files that the operating system and the installed roles use. The system state for all servers at a minimum includes the Registry, the COM+ Class Registration database, system files, boot files, and files under Windows Resource Protection (WRP). WRP is the new name for what was known as Windows File Protection under Windows Server 2003 and earlier. Servers that are domain controllers (DCs) also include the Active Directory Domain Services database and the System Volume (SYSVOL) directory. Other servers, depending on their roles, may also include the Active Directory Certificate Services database, cluster service information, and the Internet Information Server (IIS) metadirectory.

Backing up the System State in Windows Server 2008 creates a point-in-time snapshot that you can use to restore a server to a previous working state. It does this using the Volume Shadow Copy Service (VSS). VSS helps to prevent inadvertent data loss. It creates “shadow” copies of files and/or folders stored on network file shares set up at predetermined time intervals. It is essentially a previous version of the file or folder at a specific point in time.

Without a copy of the System State, recovery of a crashed server would be impossible. The System State is always backed up when full backups are invoked, whether through the WBS Wizard or *wbadmin*. To back up the System State by itself you must use the *wbadmin* command, though, and it cannot be scheduled unless you create a script that forces it to. In Exercise 5.4, we will back up the system state to our E drive.

EXERCISE 5.4

PERFORMING A SYSTEM STATE BACKUP

1. Log on to a Windows Server 2008 server and open a command prompt (**Start | Command Prompt**).
2. In the command prompt, type `wbadmin.exe Start SystemStateBackup -backuptarget:E:.`
3. We are told that This would backup the system state from volume(s) Local Disk (C:) to E:. Do you want to start the backup operation? Type Y for yes.

Next, `wbadmin` creates the shadow copy of the C drive. After it does this it identifies the system state files to back up. Once it has completed its search for system state files, it begins the backup. Figure 5.17 shows that we have finished performing a system state backup.

Figure 5.17 The System State Backup Is Complete

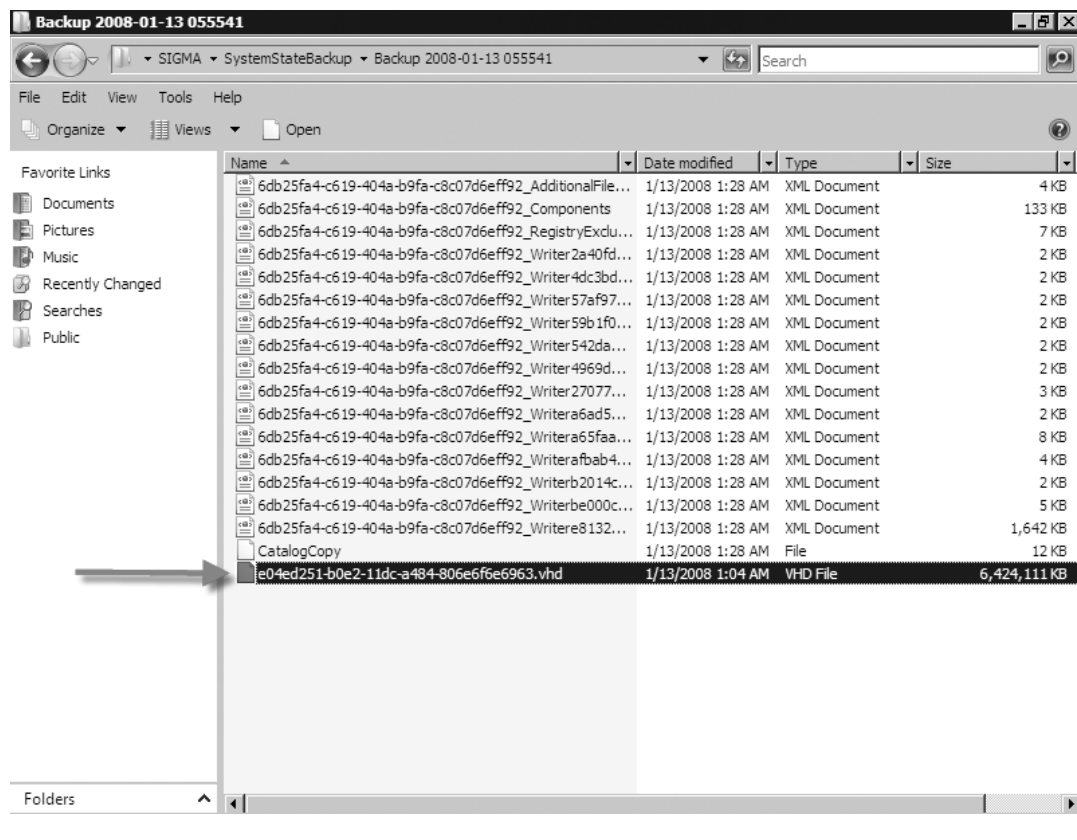
```

Administrator: Command Prompt
Backup of files reported by 'System Writer' completed
Backup of files reported by 'SPSearch USS Writer' completed
Backup of files reported by 'IIS Config Writer' completed
Overall progress - 98% <Currently backing up files reported by 'Registry Writer'
>
Backup of files reported by 'Registry Writer' completed
Backup of files reported by 'COM+ REGDB Writer' completed
Backup of files reported by 'NTDS' completed
Backup of files reported by 'WMI Writer' completed
Backup of files reported by 'DFS Replication service writer' completed
Backup of files reported by 'IIS Metabase Writer' completed
Overall progress - 99% <Currently backing up additional system state files>

Summary of backup:
-----
Backup of system state completed successfully [1/13/2008 1:29 AM]
Log of files successfully backed up
'C:\Windows\Logs\WindowsServerBackup\SystemStateBackup 13-01-2008 00-55-41.log'

C:\Users\Administrator>

```


Figure 5.19 The System State VHD File**EXAM WARNING**

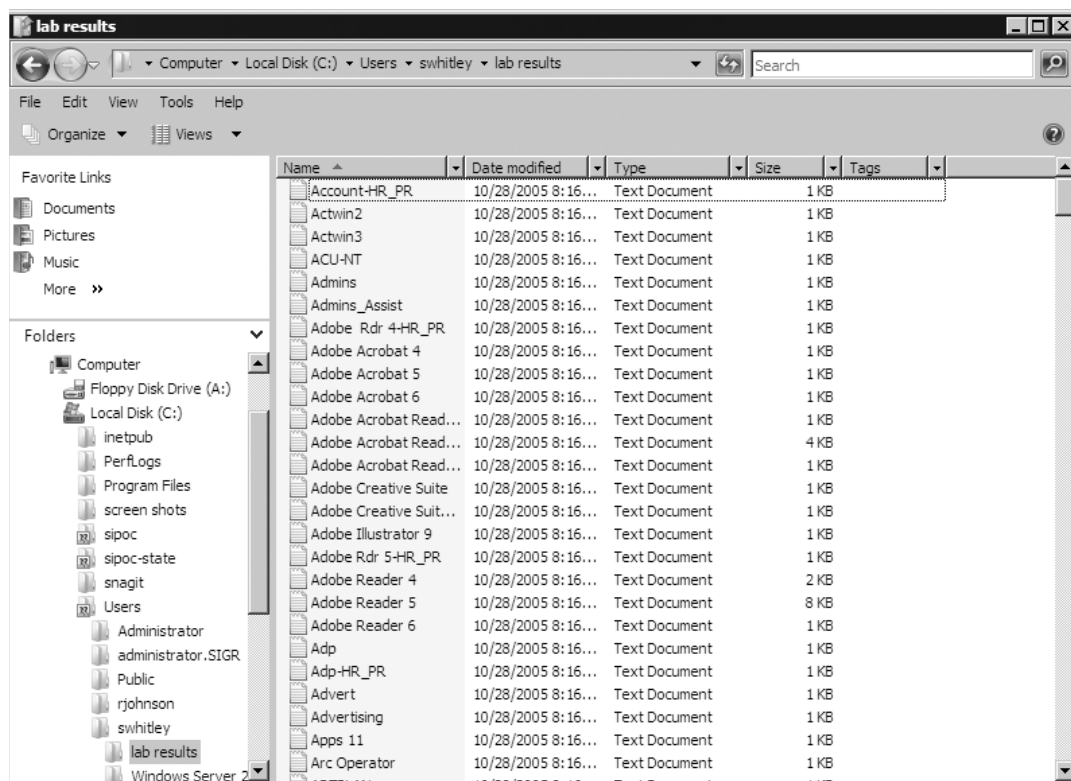
System state backups must have local drives as targets. They are not supported on DVDs, removable media, or remote/network drives. You can back up to a local drive and then copy the **SystemStateBackup** directory to another drive or device once the system state backup has been completed.

Backing Up Key Files

Windows Server Backup does not allow you to back up specific files or directories. In other words, you must specify the volume you plan to back up. For example, if I wanted to back up the Users directory on a server, I would need to back up that entire volume so that any other files and folders are automatically backed up. So, if the Users directory resides on the C drive of the server, performing a backup on that volume will back up that directory and the files within it. On our server, in Figure 5.20, you see that the user switley has numerous files in the Users\switley\lab results directory. To back this up we can do a full backup of the server or a backup of the volume where this user's data resides. As we showed earlier, to manually back up the server, just open **Windows Server Backup**, go to the **Actions** pane and select **Backup Once**.

After the backup, we'll run through a scenario where we will need to restore this data. Let's walk through backing up the drive to DVD using wbadmin.exe.

Figure 5.20 switley's User Directory



Backing Up Critical Volumes

Disks and volumes in a Windows Server 2008 system are divided into two categories: critical and noncritical. Critical volumes are those containing system state or operating system components. They include the boot and system volumes. A volume containing the Active Directory database (ntds.dit) on a DC is also an example of a critical volume. Critical disks are those that contain critical volumes. Here are two ways to back up critical volumes; the first uses the Windows Server Backup utility and the second uses wbadmin.

To back up critical volumes with the GUI:

1. Click **Start | Administrative Tools | Windows Server Backup**.
2. In the **Action** pane, select **Backup Once**.
3. In the wizard, at the **Backup options** screen, select **Different options** and then click **Next**.
4. If this is the first backup of the DC, select **Yes** to confirm that this is the first backup.
5. On the **Select backup configuration** screen, select **Custom** and then **Next**.
6. On the **Select backup items** screen, select the **Enable system recovery** checkbox, or you can clear that checkbox and select the individual volumes that you want to include. If you do this, you must select the volume(s) that store the operating system, ntds.dit, and SYSVOL.
7. On the **Specify destination type** screen, select **Local drives** or **Remote shared folder** and then click **Next**.
8. On the **Select backup destination** screen, select the backup location. If you are backing up to a local drive, in the **Backup destination** select a drive and click **Next**. If you're backing up to a remote shared folder, type the path using the UNC name and click **Next**.
9. On the **Specify advanced option** screen, select **VSS copy backup** (default) then click **Next**.
10. At the **Summary** screen, review your selections and click **Backup**.
11. After the backup is complete choose **Close**.

To back up critical volumes using wbadmin.exe do the following:

1. Click Start | Command Prompt.
2. At the command prompt type **wbadmin start backup -allCritical -backuptarget: targetdrive: -quiet**.

The *-quiet* switch allows you to bypass having to type **Y** when asked to proceed with the backup operation.

Recovering System State Data

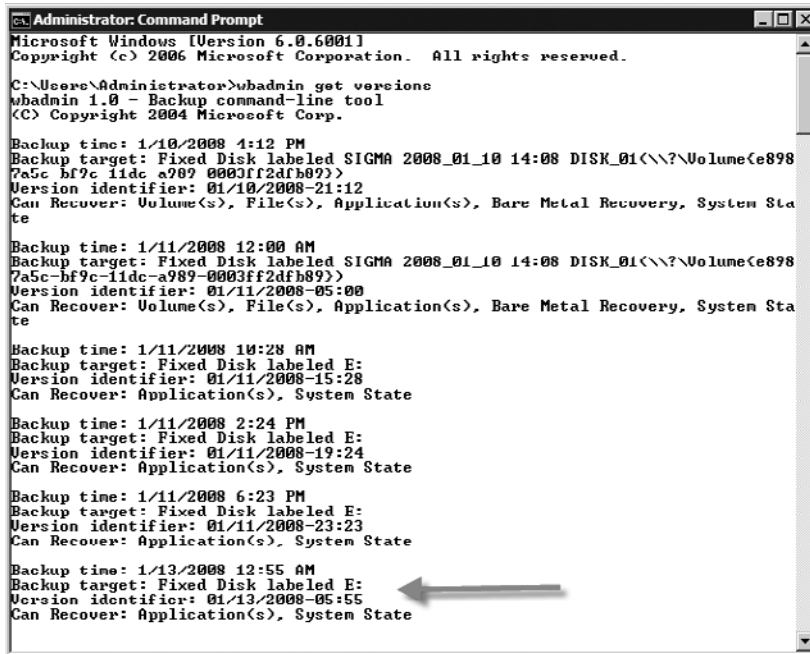
Sometimes the operating system may become corrupt or unstable. Maybe a role or service needs to be rolled back to a previously backed up state. The fastest and easiest method to do this is to perform a system state recovery. As we already know, the only way to back up system state independently is to use wbadmin.exe. This is the same for recovery. You must use wbadmin to independently restore the system state. In our example in backing up the system state, we saved the system state on another local hard drive on the server (the E drive). The .vhd file, which is the actual backup file, resides in E:\WindowsImageBackup\SIGMA\SystemStateBackup\Backup 2008-01-13 055541. Exercise 5.5 walks you through the steps in recovering the system state for a member server.

EXERCISE 5.5

RECOVERING SYSTEM STATE FOR MEMBER SERVER

1. To recover a system state we must log on to the server as the administrator.
2. Pull up the command prompt (**Start | Command Prompt**).
3. In the command prompt type **wbadmin get versions**. You'll see a list of the backups you've made on that server. They will be arranged by date and time. You'll also see what you can recover with each backup. At the bottom of the list in Figure 5.21, notice that the last backup's time of backup, its target, the version identifier, and what it can recover match our example earlier in the chapter. That is the backup we will recover.

Figure 5.21 The Command Prompt



```

Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Backup time: 1/10/2008 4:12 PM
Backup target: Fixed Disk labeled SIGMA 2008_01_10 14:08 DISK_01(\\?\Volume{e898
7a5c-bf9c-11dc-a989-0003ff2dfb89})
Version identifier: 01/10/2008-21:12
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System Sta
te

Backup time: 1/11/2008 12:00 AM
Backup target: Fixed Disk labeled SIGMA 2008_01_10 14:08 DISK_01(\\?\Volume{e898
7a5c-bf9c-11dc-a989-0003ff2dfb89})
Version identifier: 01/11/2008-05:00
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System Sta
te

Backup time: 1/11/2008 10:28 AM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-15:28
Can Recover: Application(s), System State

Backup time: 1/11/2008 2:24 PM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-19:24
Can Recover: Application(s), System State

Backup time: 1/11/2008 6:23 PM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-23:23
Can Recover: Application(s), System State

Backup time: 1/13/2008 12:55 AM
Backup target: Fixed Disk labeled E:
Version identifier: 01/13/2008-05:55
Can Recover: Application(s), System State

```

4. In the command prompt, select your desired backup by highlighting the version identifier, which in our case is **01/13/2008-05:55**, and pressing **Enter**. This stores it in the Clipboard.
5. At the prompt, type **wbadmin Start SystemStateRecovery -version: 01/13/2008-05:55** and press **Enter** (remember that you can paste the version identifier by clicking on the upper-left corner of the command prompt and selecting **Edit | Paste**).
6. Next, wbadmin will prompt you with **Do you want to start the system state recovery operation?** Type **Y** for yes and press **Enter**.
7. The system state recovery takes a few minutes to complete. After it's finished, reboot the server and that's it. You've recovered the system state.

EXAM WARNING

To recover the system state for a DC, you must be in Directory Services Restore Mode (DSRM).

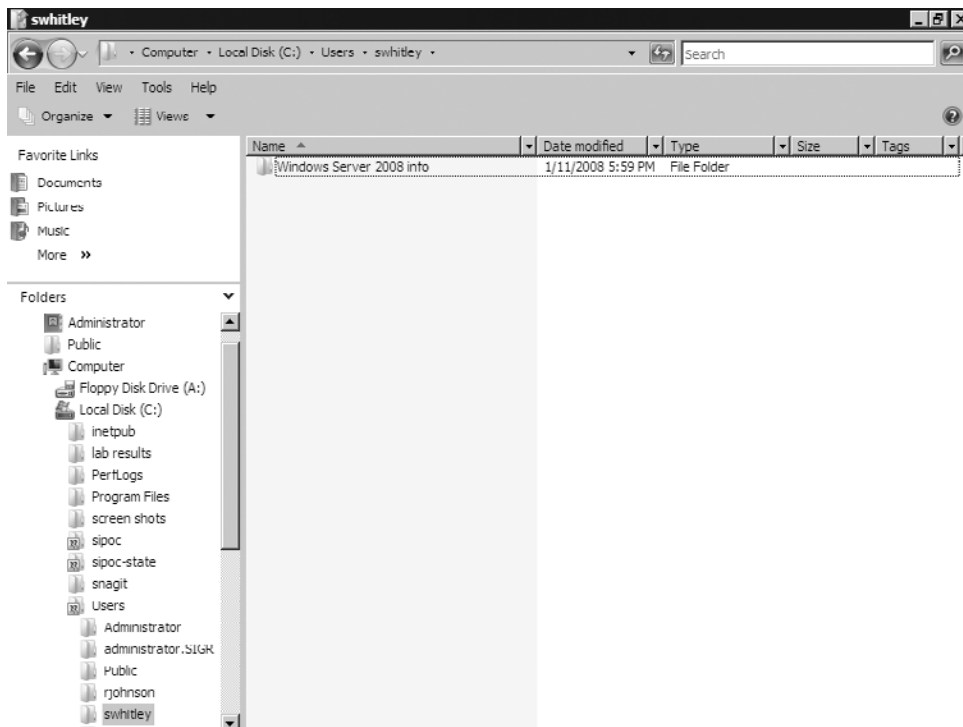
Recovering Key Files

With WSB, we can recover individual files and folders as long as the backup resides on a local drive with the system. In other words, if a full backup was made to a network drive, DVD, or any other remote/removable media we would have to restore the entire volume. In the “Backing Up Key Files” section earlier in this chapter, we showed that the user switley had a directory called lab results within her Users directory (refer back to Figure 5.20). As we all know, sometimes files and, worse, directories are deleted accidentally. Well, one day switley gets to work and notices her lab results directory is gone, as shown in Figure 5.22. She needs this directory ASAP. One option with Windows Server 2008 is to use WSB to individually recover directories and/or files. Exercise 5.6 shows how to do this.

EXERCISE 5.6

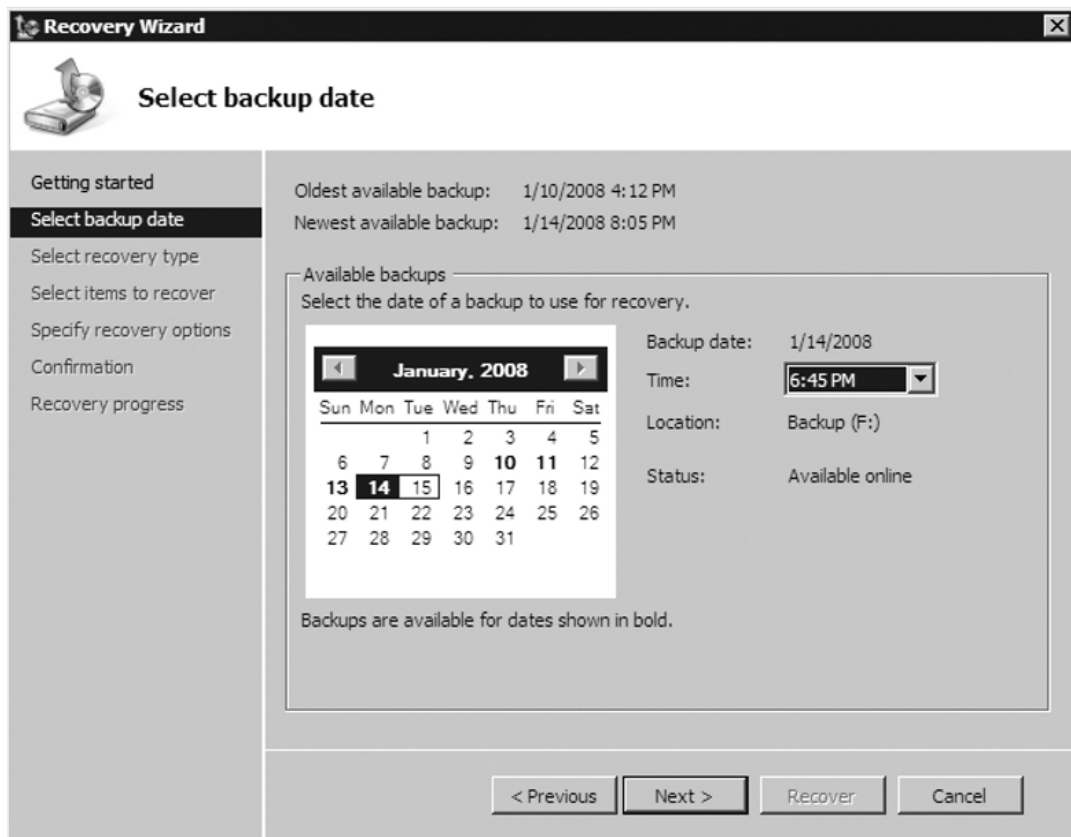
RECOVERING FILES AND DIRECTORIES

Figure 5.22 An Accidentally Deleted Directory



1. Pull up WSB (Start | Administrative Tools | Windows Server Backup).
2. In the **Actions** pane select **Recover**.
3. At the **Getting Started** screen, you're asked **Which server do you want to recover data from?** For our scenario, we will select **This server (SIGMA)**. Click **Next**.
4. In Figure 5.23, you see that we must select the date of a backup we want to use for the recovery. We will select a backup done on 01/14/2008 at 6:45 P.M. located on the E drive. Click **Next**.

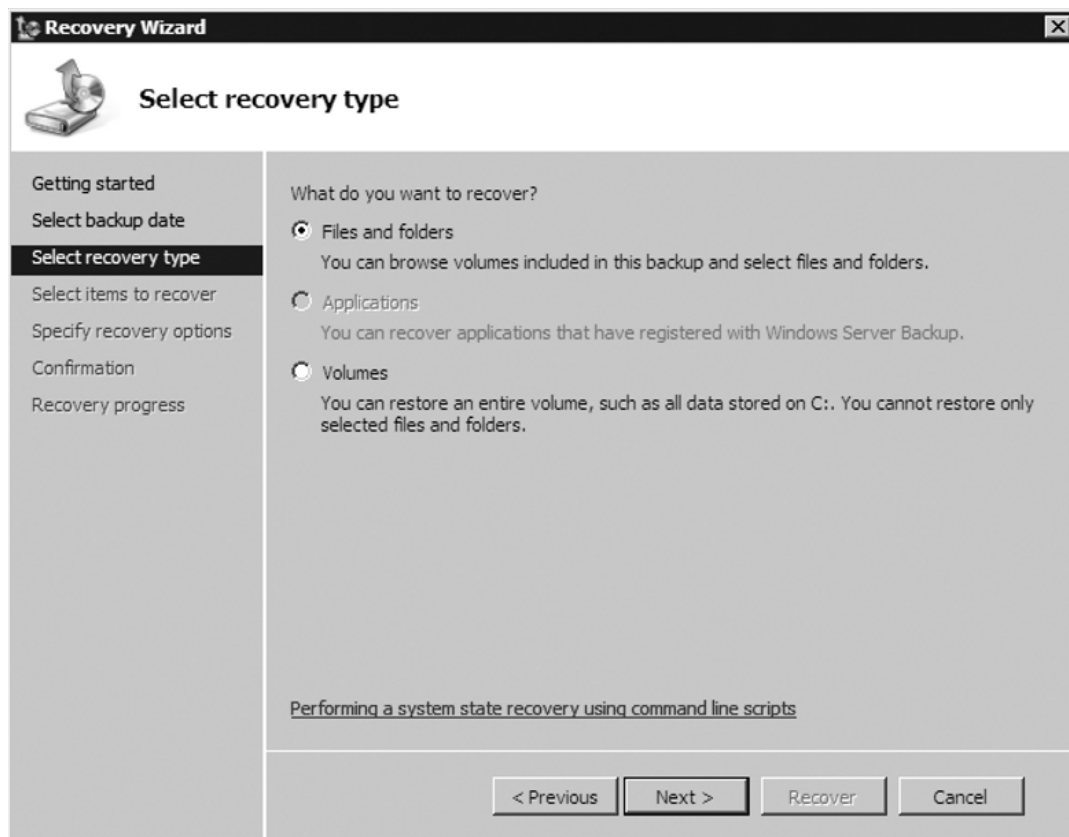
Figure 5.23 Selecting the Backup Date



5. We now need to select a recovery type. We have three options: **File and Folders**, **Applications** (grayed out), and **Volumes**. If we select **Volumes**, we can restore the entire volume, such as drive C, but we will not be able to individually select files or folders to

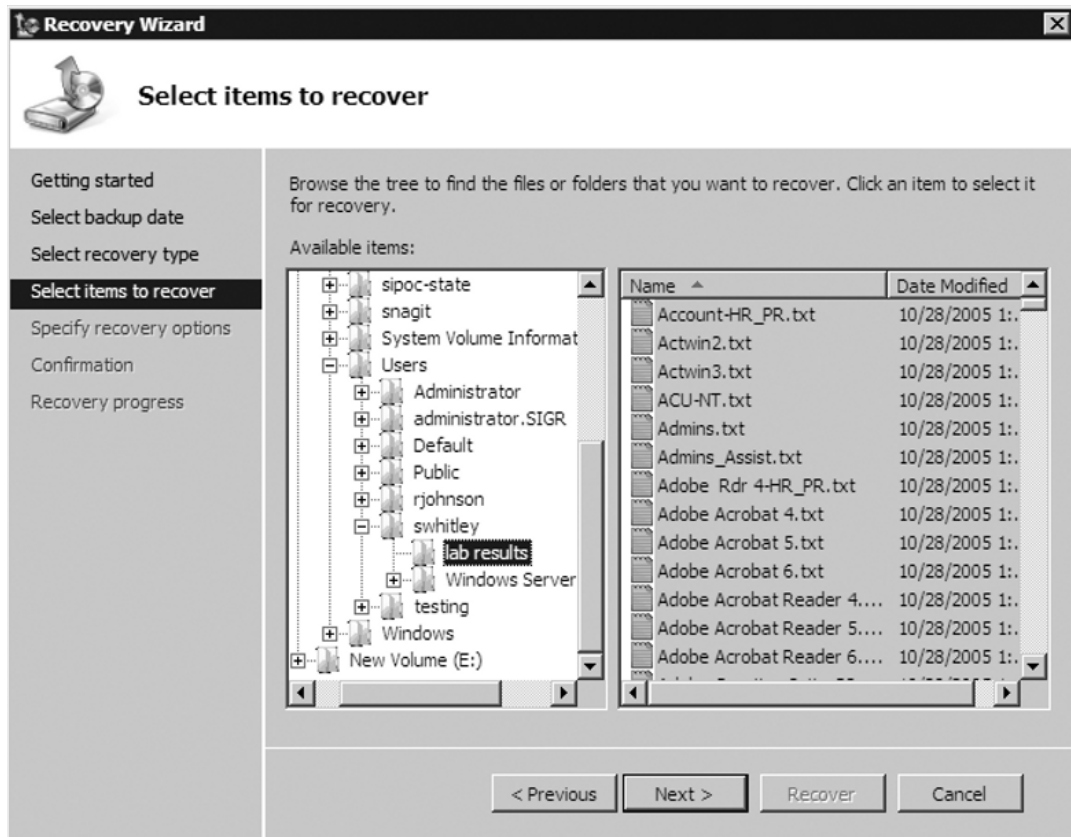
recover. **Applications** are available when an application's plug-ins are registered. Currently we do not have any; therefore, this option is grayed out. **Files and Folders** will allow us to individually select what files or folders we want to recover. Because we want to recover switley's lab results folder, we will choose this option, as shown in Figure 5.24. Click **Next**.

Figure 5.24 Selecting the Recovery Type

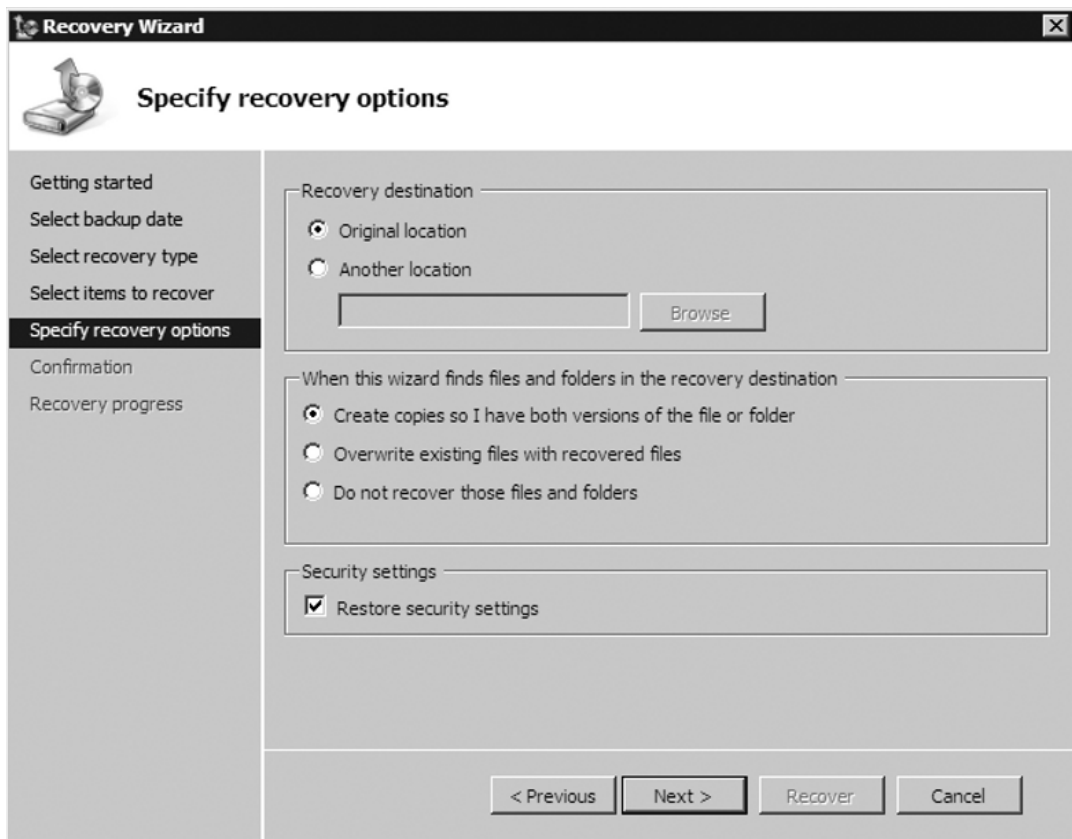


6. We must now choose what items we want to recover. We need to get to switley's Users directory and choose **Lab Results**, as shown in Figure 5.25, and then click **Next**.

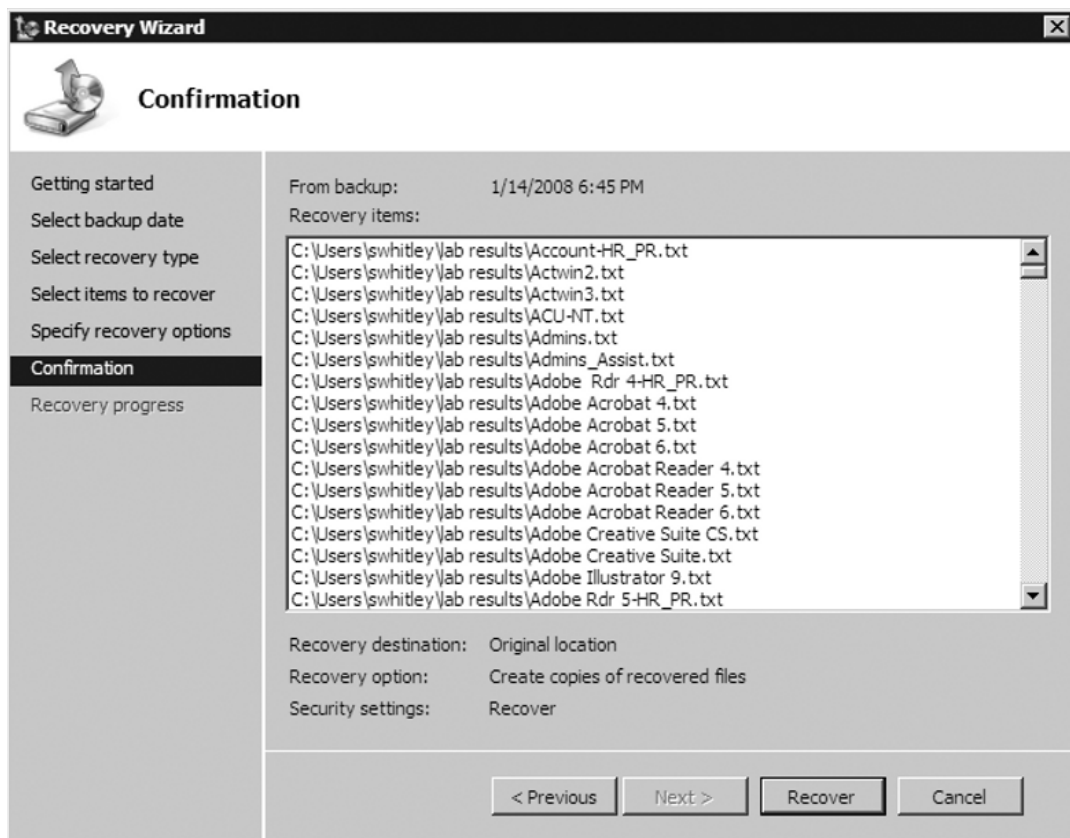
Figure 5.25 Selecting Items to Recover



- Figure 5.26 shows that we have to specify recovery options such as recovery destination, how to handle conflicts, and whether to restore security settings. We will be recovering the lab results folder in its original destination. We will also select **Create copies so I have both versions of the file or folder**. This is the safest option we have. Finally, we want the original security settings that were there before the folder was deleted in place. Once we've done that we can click **Next**.

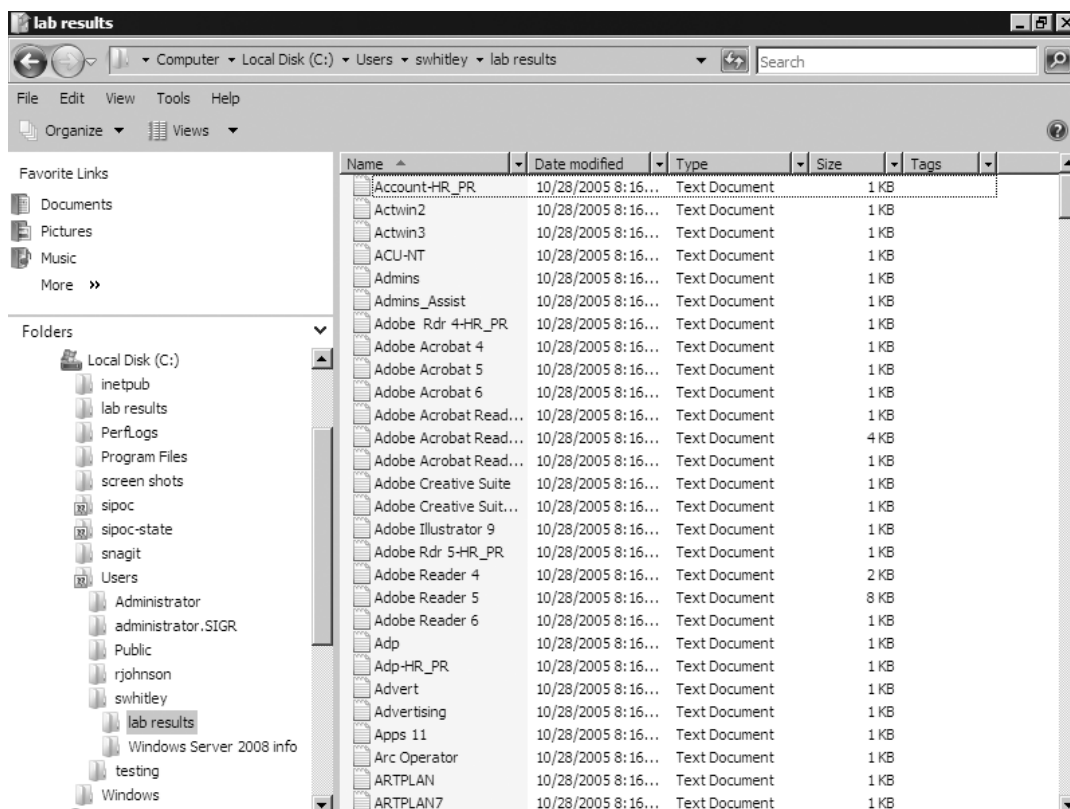
Figure 5.26 Specifying Recovery Options

8. WSB will now ask us to confirm what we want to recover, as shown in Figure 5.27. Once we've done that we can click **Recover**.

Figure 5.27 Confirming What We Want to Recover

9. After the recovery process is over, just click **Close**.

We can now check switley's Users directory to see whether the lab results directory was recovered and whether the files that resided there are restored as well. Figure 5.28 shows that we have a successful recovery of her directory and the files that reside there.

Figure 5.28 Verifying That the Directory and Files Have Been Restored

Directory Services Restore Mode

Directory Services Restore Mode (DSRM) is a special boot mode in Windows Server 2008. You use it to log on to a DC when either Active Directory has failed or an object needs to be restored. During setup, you were asked to provide a password for the DSRM administrator. This administrator account (Administrator) is separate from the domain administrator account. This account is used once you boot into DSRM.

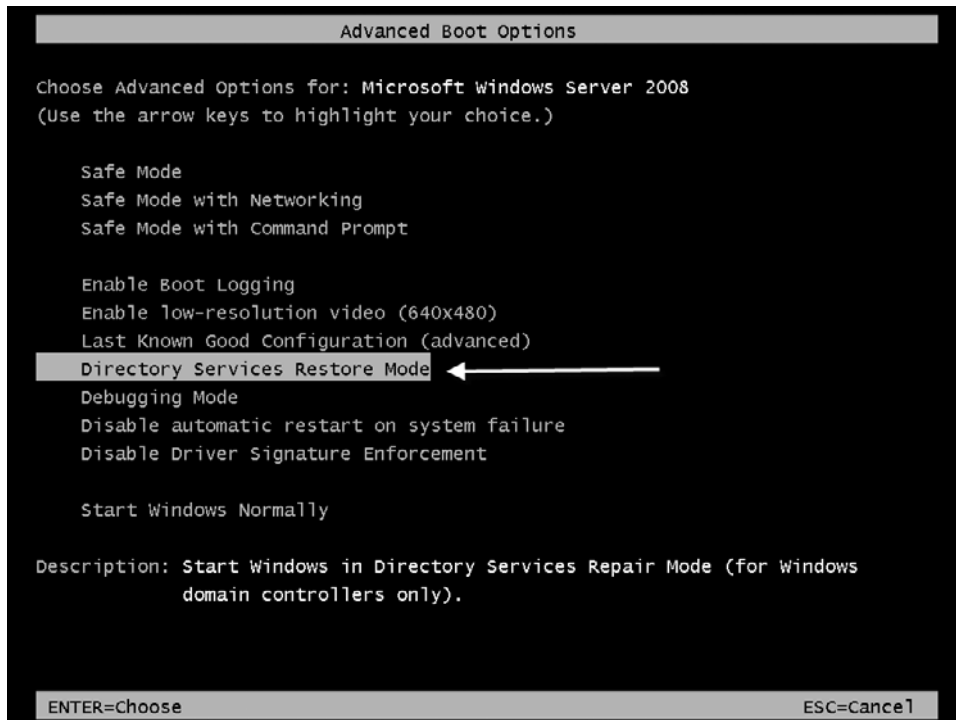
If you have forgotten the DSRM password, you can reset it by doing the following:

1. Click Start | Command Prompt.
2. In the command prompt, type **ntdsutil** then press **Enter**.
3. At the ntdsutil prompt, type **set dsrm password** and press **Enter**.

4. At the **Reset DSRM Administrative Password** prompt, type **reset password on server null** (if you are resetting the DSRM password on a remote server, type **reset password on server <servername>**).
5. Type in the new password, press **Enter**, and then retype the password for verification and press **Enter** again.
6. After you receive the Password has been set successfully message, type quit at both the Reset DSRM Administrator Password prompt and the ntdsutil prompt.

To access DSRM, you must restart the DC and then press **F8** immediately after the BIOS POST screen and before the Windows Server 2008 logo appears. Once you've done this, you will see the **Advanced Boot Options** screen shown in Figure 5.29. To restore Active Directory you would choose **Directory Services Restore Mode** and then perform either an authoritative or a nonauthoritative restore, which we will cover in more detail in the next section.

Figure 5.29 Choosing Directory Services Restore Mode



So, what if you don't remember the password for the DSRM administrator? No problem; Microsoft anticipated this. Just follow the steps in Exercise 5.7.

EXERCISE 5.7

RESETTING THE DSRM ADMINISTRATOR PASSWORD

1. Open a command prompt (**Start | Command Prompt**).
2. At the C prompt, type **ntdsutil** and press **Enter**.
3. At the **ntdsutil** prompt, type **set dsrm password** and press **Enter**.
4. You will now come to the **Reset DSRM Administrator Password** prompt. Type **reset password on server null** and press **Enter**.

Configuring and Implementing...

Resetting DSRM Administrator Passwords

You can reset the DSRM Administrator password on another server by typing **reset password on server <servername's FQDN>** at the **Reset DSRM Administrator Password** prompt.

5. At the **Please type password for DS Restore Mode Administrator Account** type the new password. You will notice that you will not see the characters that you are typing. After you do this, press **Enter**.
6. You will now be prompted to confirm the password; do so and press **Enter**.
7. After you have done this correctly, **ntdsutil** will confirm that the password has been reset.
8. Now type **q** and press **Enter** at the **Reset DSRM Administrator Password** prompt.
9. At the **ntdsutil** prompt, type **q** and press **Enter**. You have now reset the DSRM Administrator's password, which you can see in Figure 5.30.

Figure 5.30 Successfully Resetting the DSRM Administrator's Password

Performing Authoritative and Nonauthoritative Restores

One day you may find yourself with a DC that has a corrupted copy of `ntds.dit`. To resolve issues such as this you would need to perform a nonauthoritative restore, which we will cover soon. Other times you may have accidentally deleted an object (user, computer, printer, etc.) from Active Directory and you have no way to restore it within Active Directory. This is usually because after the object is deleted, the change has already been replicated to the other DCs in the domain. To fix this you need to perform an authoritative restore, which we will discuss in the next section.

Authoritative Restore

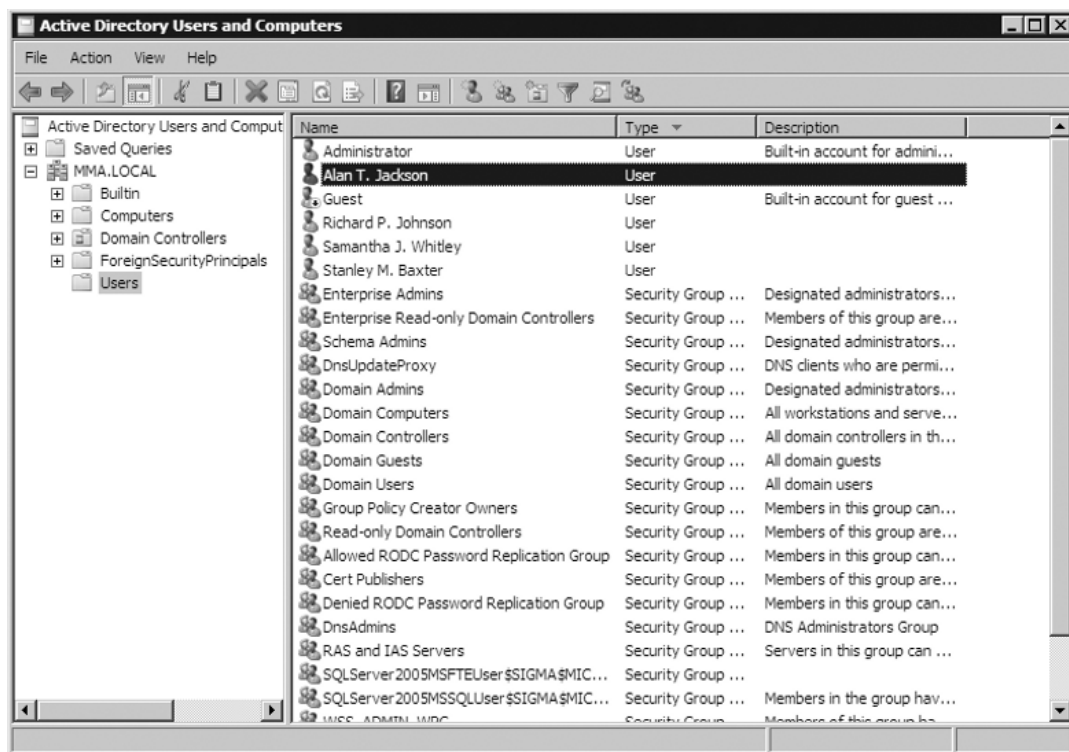
As just mentioned, one of the reasons to perform an authoritative restore is when an object is accidentally deleted in Active Directory and the deletion has already replicated to the remaining DCs. If you simply did a nonauthoritative restore, the object would restore but would be deleted after the other DCs replicated with the recovered system. Exercise 5.8 provides the steps for conducting an authoritative restore.

EXERCISE 5.8

PERFORMING AN AUTHORITATIVE RESTORE

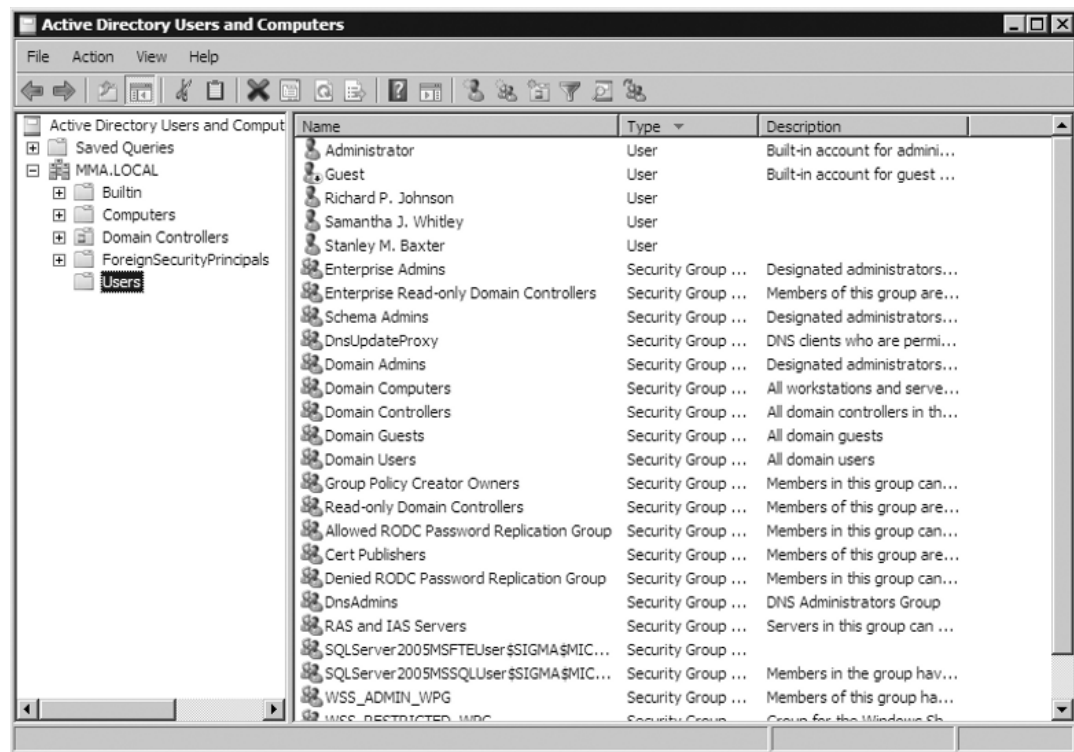
In this example, we are going to “accidentally” delete the user Alan T. Jackson. As you see in Figure 5.31, you Alan’s user account is in the Users organizational unit (OU). We will now “accidentally” delete it.

Figure 5.31 User Alan T. Jackson before Deletion



In Figure 5.32, you can see that Alan’s user account has been deleted.

Figure 5.32 User Alan T. Jackson Deleted



Here are the steps to follow to perform an authoritative restore so that we can restore Alan's user account:

1. First we need to get the version identifier for the most recent backup. Go into a command prompt (**Start | Command Prompt**) and type **wbadmin Get Versions** and press **Enter**. You should see a list of the backups that have been performed on that server. At the bottom is the backup about which we need to get the information. The **Version identifier** for the backup we want is **01/15/2008-01:05**. Also notice that it is stored on the server's E drive in Figure 5.33.

Figure 5.33 Getting Backup Information

```

Administrator: Command Prompt
C:\Users\Administrator>wbadmin Get Versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Backup time: 1/10/2008 4:12 PM
Backup target: Fixed Disk labeled SIGMA 2008_01_10 14:08 DISK_01(\\?\Volume{e8987a5c-bf9c-11dc-a989-0003ff2dfb89})
Version identifier: 01/10/2008-21:12
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System State

Backup time: 1/11/2008 12:00 AM
Backup target: Fixed Disk labeled SIGMA 2008_01_10 14:08 DISK_01(\\?\Volume{e8987a5c-bf9c-11dc-a989-0003ff2dfb89})
Version identifier: 01/11/2008-05:00
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System State

Backup time: 1/11/2008 10:28 AM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-15:28
Can Recover: Application(s), System State

Backup time: 1/11/2008 2:24 PM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-19:24
Can Recover: Application(s), System State

Backup time: 1/11/2008 6:23 PM
Backup target: Fixed Disk labeled E:
Version identifier: 01/11/2008-23:23
Can Recover: Application(s), System State

Backup time: 1/13/2008 12:55 AM
Backup target: Fixed Disk labeled E:
Version identifier: 01/13/2008-05:55
Can Recover: Application(s), System State

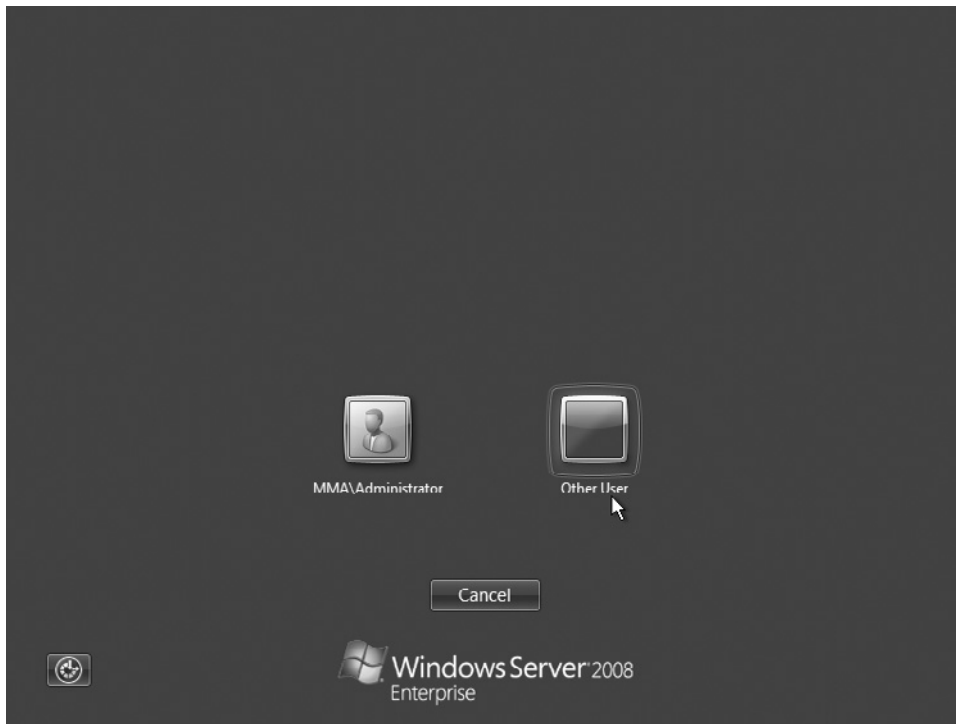
Backup time: 1/14/2008 6:45 PM
Backup target: Fixed Disk labeled Backup(F:)
Version identifier: 01/14/2008-23:45
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System State

Backup time: 1/14/2008 8:05 PM
Backup target: Fixed Disk labeled E:
Version identifier: 01/15/2008-01:05
Can Recover: Application(s), System State

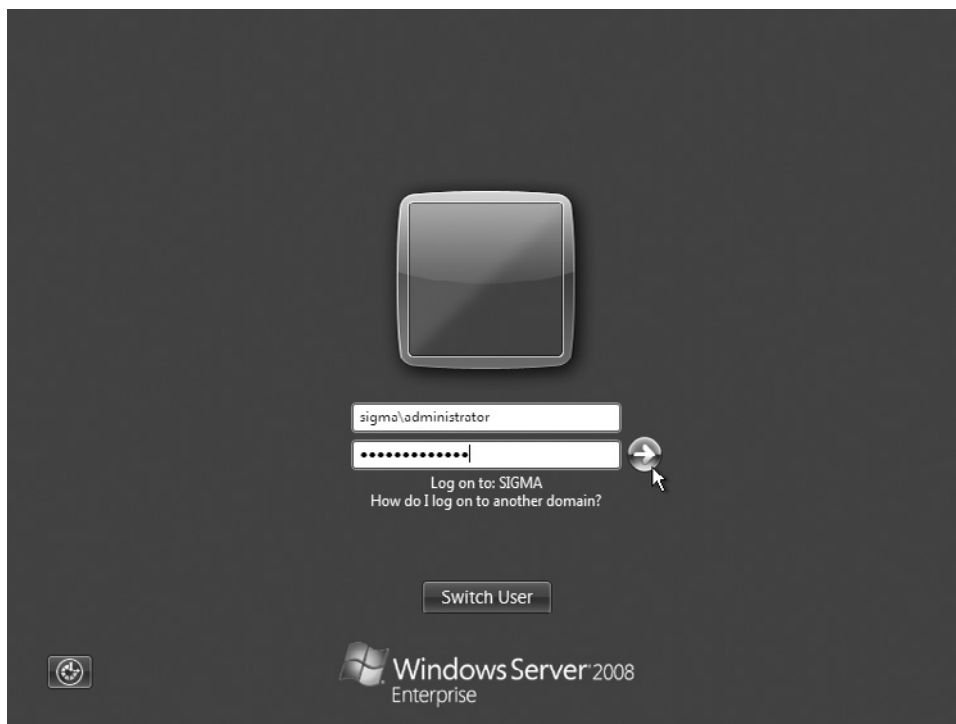
```

2. Restart the server and press **F8** to open the **Advanced Boot Options**. However, in the **Advanced Boot Options**, select **Directory Services Restore Mode** and press **Enter**.
3. DSRM will boot up into safe mode and will check the file system on all locally attached drives (except for DVDs). Press **Ctrl + Alt + Del** when asked. At the logon screen, click on **Switch User** so that you don't try to log on as the domain administrator, and then click on **Other User**, as shown in Figure 5.34.

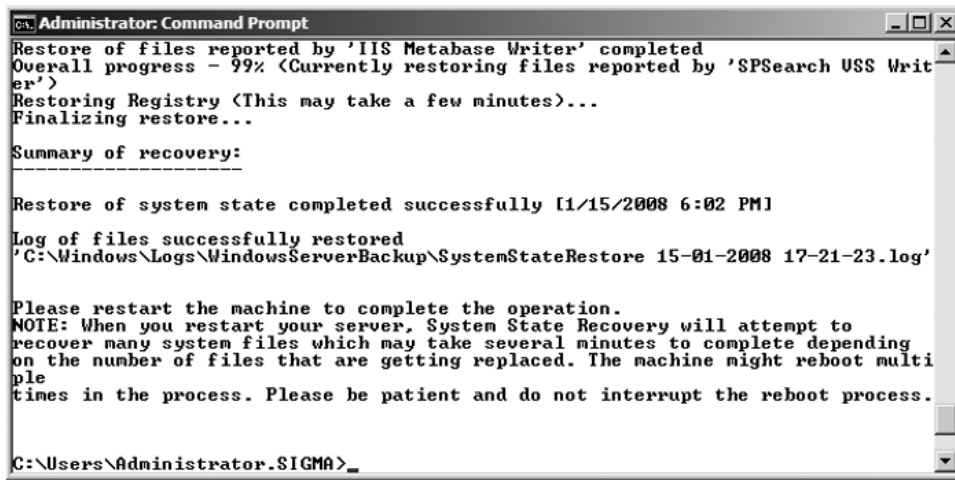
Figure 5.34 Selecting Other User



4. For the username, type in the DSRM's administrator account and its password. Notice in Figure 5.35 that we have typed it as **sigma\administrator**. Click on the **blue button with the white arrow** next to where the password is typed to continue.

Figure 5.35 Logging On As the DSRM Administrator

5. Once in safe mode, open the command prompt. Because all we need to do is restore the system state, we can type **wbadmin start SystemStateRecovery –version:01/15/2008-01:05**. This is the same format we covered earlier in recovering the system state.
6. You are then asked whether you want to start the system state recovery. Type **Y** for yes and press **Enter**. Recovery may take a few minutes or longer.
7. Once recovery is finished, you are asked to restart your computer, as shown in Figure 5.36. For an authoritative restore you do not restart the system.

Figure 5.36 The System State Recovery Is Complete

8. As this is an authoritative restore, we must pull up `ntdsutil` to restore the user `ajackson`. At the command prompt, type **ntdsutil** and press **Enter**.
9. At the `ntdsutil` prompt, type **activate instance ntds** and press **Enter**.
10. The `ntdsutil` prompt will return. At the prompt, type **authoritative restore** and press **Enter**.
11. This will bring up an **authoritative restore** prompt. At the prompt, type **restore subtree CN=ajackson,CN=Users,DC=MMA,DC=LOCAL** and press **Enter**. Note there are *no* spaces between the commas and the next entry.
12. You will now be asked whether you are sure you want to perform the authoritative restore. Click **Yes**.
13. One record will be found and will be successfully updated. You will see the message **Authoritative Restore completed successfully**. At the **authoritative restore** prompt just type **q** for quit and do the same at the `ntdsutil` prompt. You can now restart the computer and let it come to the normal logon screen.
14. Log on as the domain administrator and let the system state recovery finish. Once it's done, you can examine **Active Directory Users and Computers (ADUC)** and go to the Users OU and see that the user Alan T. Jackson has been restored.

Nonauthoritative Restore

Nonauthoritative restores are used to bring back Active Directory Domain Services to a working state on a DC. The prerequisite for a nonauthoritative restore is that a critical-volume backup exists. A nonauthoritative restore is in order for situations such as lost data that can include updates to passwords for user accounts, computer accounts, and even trusts. Updates to group memberships, policies, the replication topology, and its schedules to name a few. To conduct a nonauthoritative restore follow the same procedures we outlined for the authoritative restore. After the system state is restored, you can go ahead and restart the server when prompted instead of loading ntdsutil. Once a nonauthoritative restore is complete, any changes to Active Directory objects are replicated to the server from that has just gone through a nonauthoritative restore.

Linked Value Replication

When the forest level is at Windows Server 2003 or above, linked value replication (LVR) is available. Previously in Active Directory, primarily with Windows 2000, when an attribute changed the entire attribute was replicated to all other DCs on the network. Now, with LVR, changes in group membership to store and replicate values for individual members instead of replicating the entire membership as a single unit. LVR lowers the amount of bandwidth used in replication and the amount of processor power used during replication.

Backing Up and Restoring GPOs

Backing up a Group Policy Object (GPO) consists of making a copy of the GPO data to the file system. The backup consists of the following data:

- Domain where the GPO resides
- Owner of the GPO
- Date created
- Date modified
- User revisions
- Computer revisions
- Globally unique identifier (GUID)
- GPO status

Exercise 5.9 takes you through the steps of backing up a GPO.

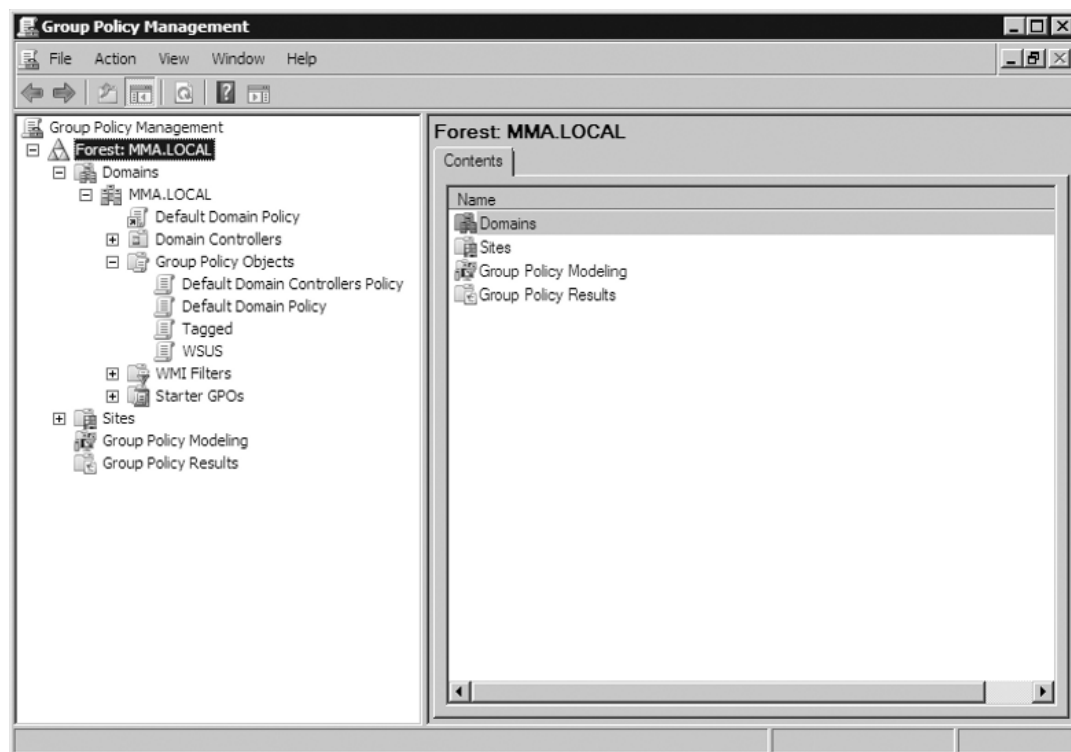
EXERCISE 5.9

BACKING UP THE GPO

You must back up GPOs from the Group Policy Management Console (GPMC). You can get to it by clicking on **Start | Administrative Tools | Group Policy Management**. Let's walk through the process of backing up GPOs:

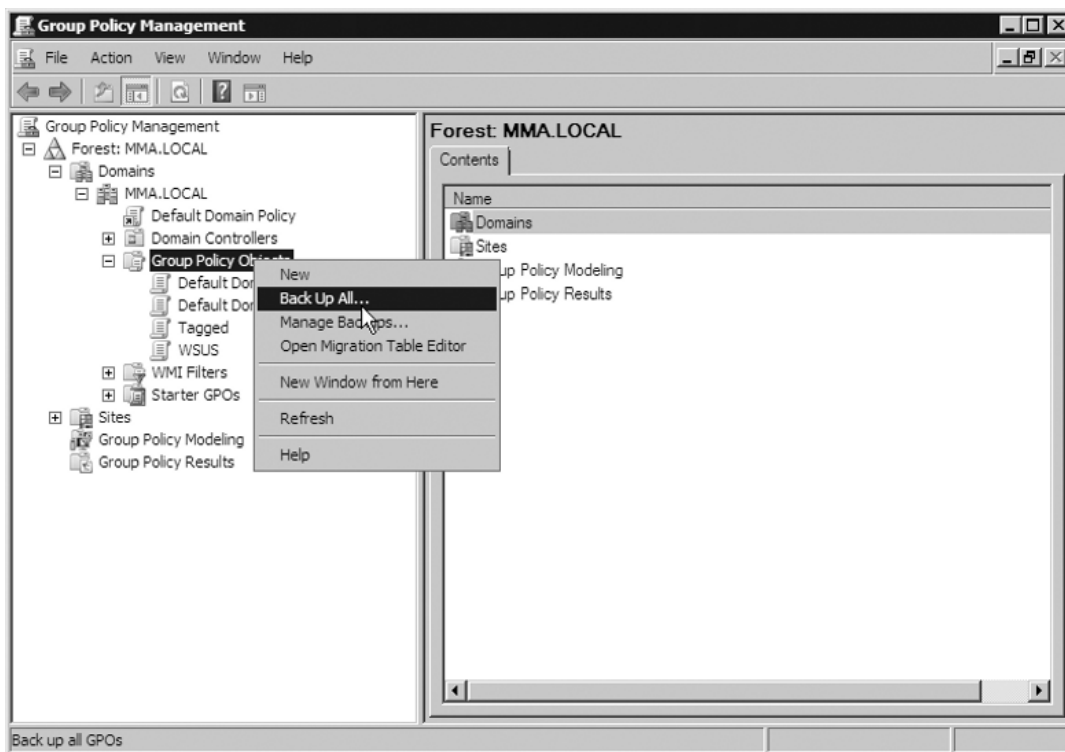
1. Open the GPMC.
2. In the console tree, click on the plus sign (+) next to the forest. In our case, we click on the plus sign next to **Forest:MMA.LOCAL**.
3. Scroll down the tree **Domains | <Domain Name> | Group Policy Objects**. In Figure 5.37, you see that we have four GPOs. In reality, you would probably have significantly more, but for demonstration purposes we'll keep it simple.

Figure 5.37 The GPMC

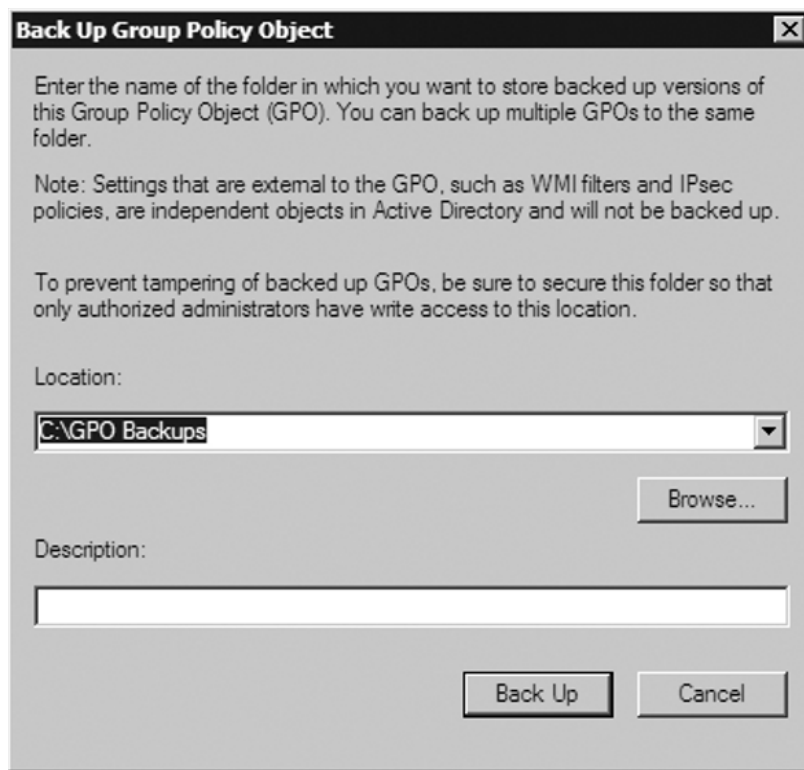


4. Highlight **Group Policy Objects** and right-click it. Select **Back Up All**, as shown in Figure 5.38.

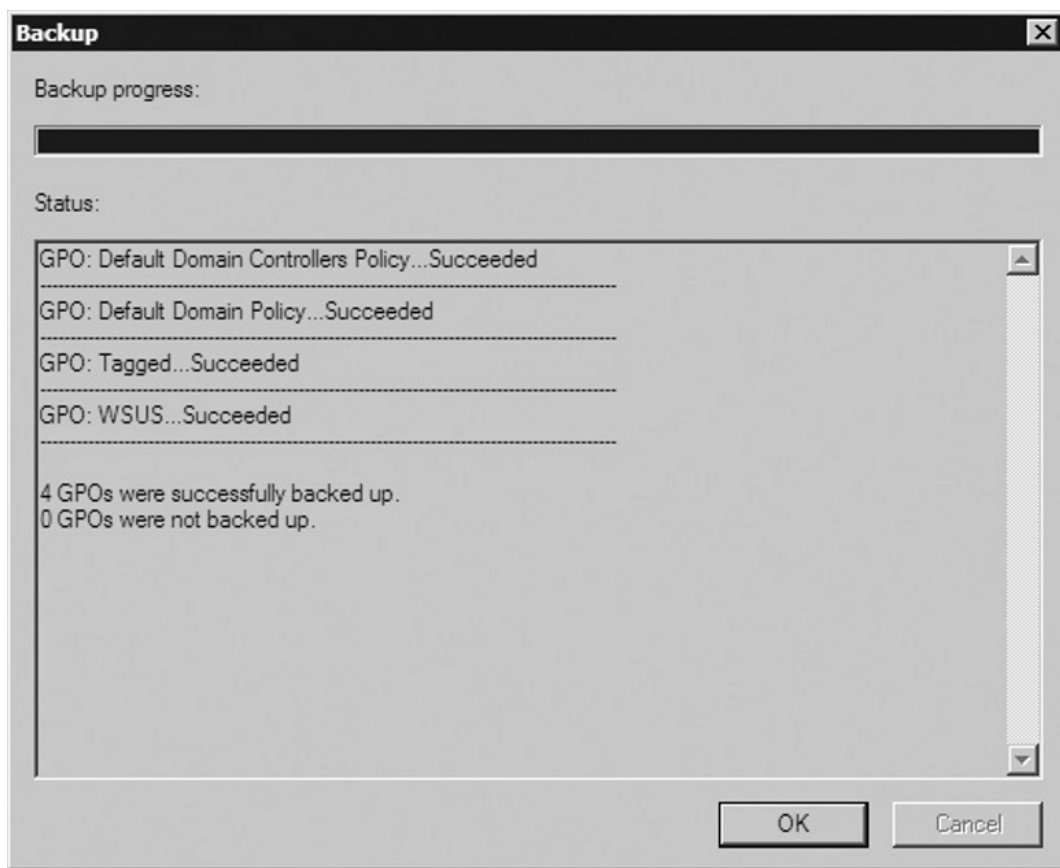
Figure 5.38 Selecting Back Up All



5. When the **Back Up Group Policy Object** screen comes up, as shown in Figure 5.39, set the location to a directory either on a local drive or on a mapped drive on a remote server. In our case, we are backing up our GPOs to the directory C:\GPO Backups. As for a description, you can type anything you want that will remind you what this certain backup pertains to. After you've done this, you can click on **Back Up**.

Figure 5.39 Location to Store Backups

6. Next you'll see the backup progress take place. Once it's finished, it will provide you with the status of the backup for each GPO. As you can see in Figure 5.40, our four GPOs were successfully backed up. Once your GPOs have backed up successfully, just click **OK** to finish.

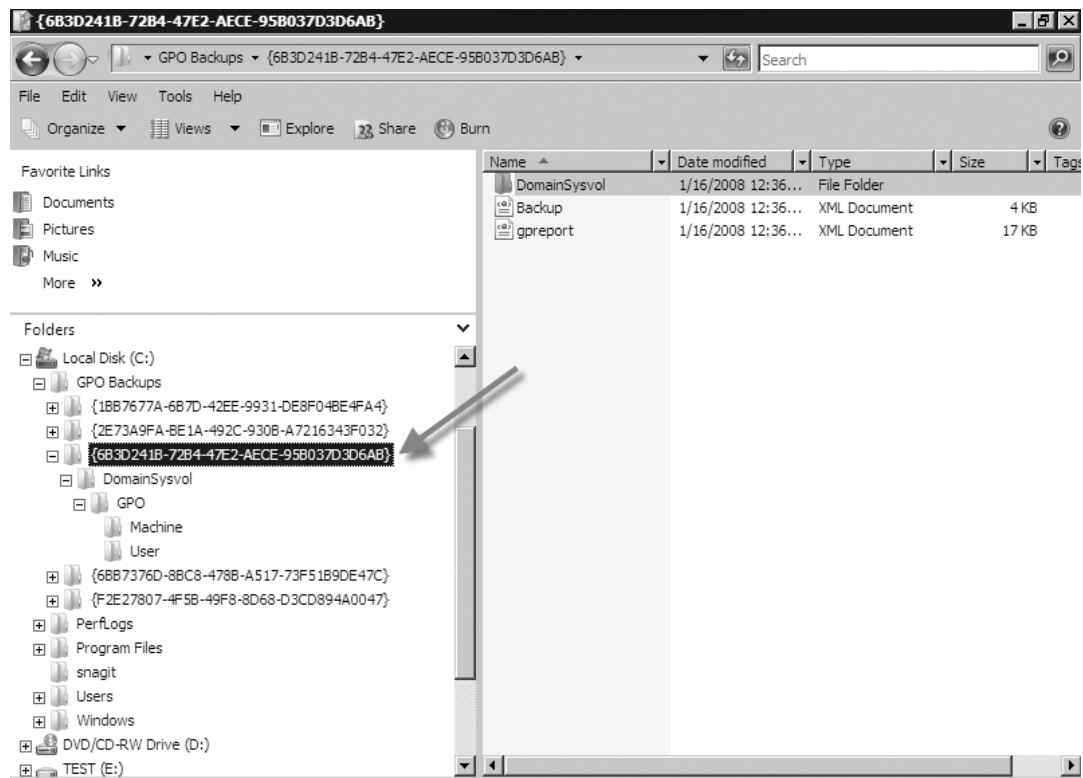
Figure 5.40 Backup Status

EXAM WARNING

With Windows Server 2008 comes a new type of GPO called Starter GPOs. Starter GPOs are not included in the backup of GPOs; you have to back them up separately. To do so, highlight the **Starter GPOs** folder, right-click it, select **Backup Up All**, and follow the same procedure we went through in Exercise 5.9.

In the directory where we backed up our GPOs, you see that each GPO has a folder with a GUID as the name, as shown in Figure 5.41. Inside each folder will be two XML documents—one named Backup and the other named gpreport—along with a folder called DomainSysvol. The DomainSysvol folder holds a GPO folder with two subfolders—one for machine settings and the other for user settings. If there are settings, say, for a machine and none for a user a registry.pol file will exist in that folder and vice versa, or if the GPO has settings for both each folder will contain a registry.pol file.

Figure 5.41 The Folder Layout for GPO Backups



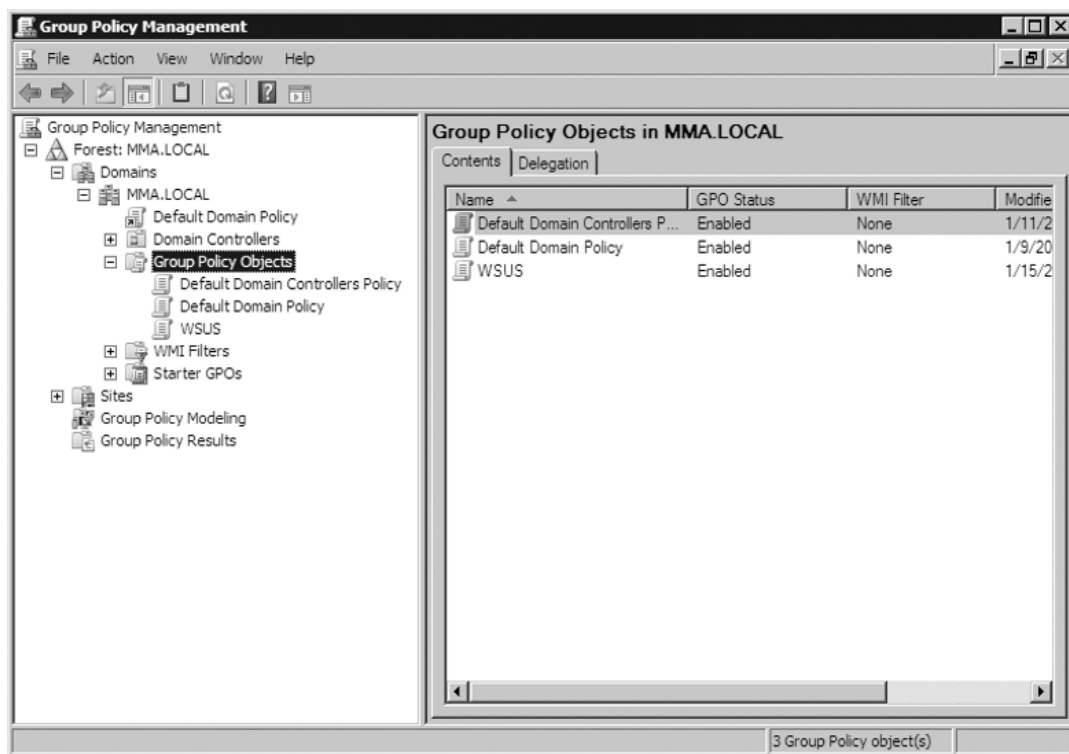
In Figure 5.38, you can see that we have a GPO named **Tagged**. How would we restore that GPO if it were accidentally deleted? The process is quite simple; let's walk through it in Exercise 5.10.

EXERCISE 5.10

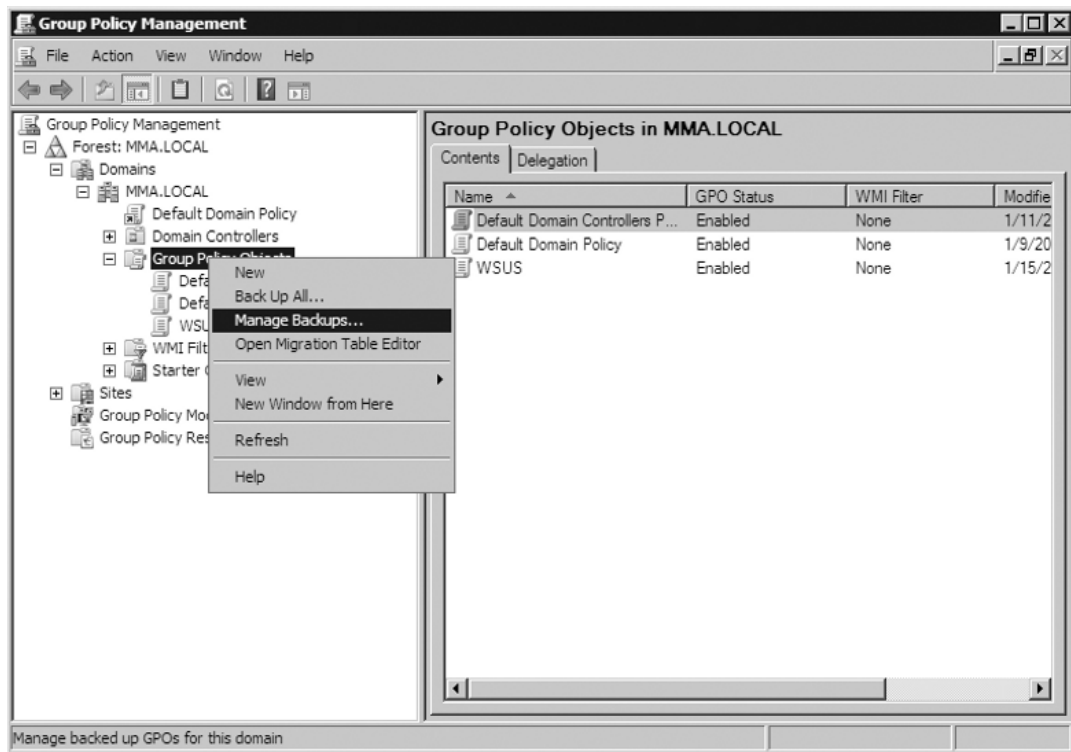
RESTORING A GPO

1. Open the GPMC (**Start | Administrative Tools | Group Policy Management**).
2. In the GPMC, go to **Forest:MMA.LOCAL | Domains | MMA.LOCAL | Group Policy Objects** and verify that the GPO has been deleted. In Figure 5.42, you see that the Tagged GPO is no longer there.

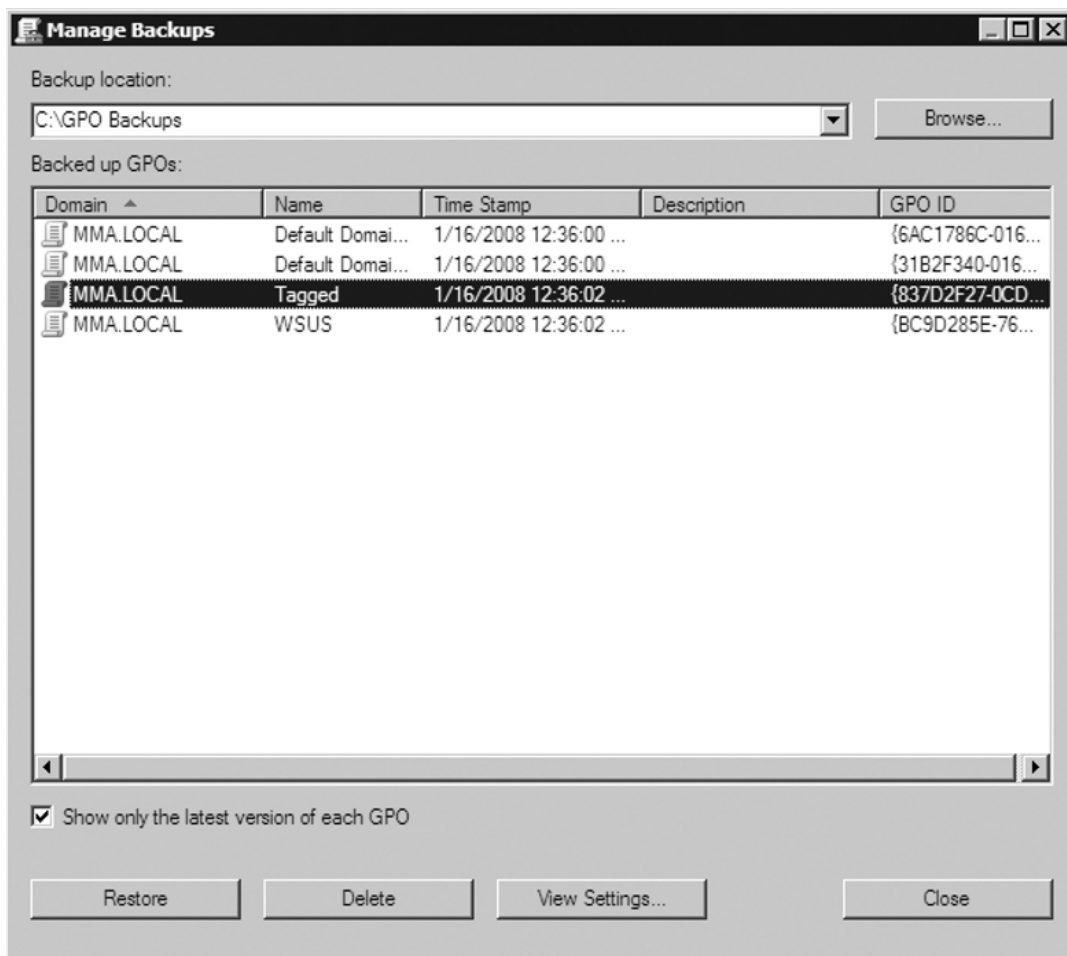
Figure 5.42 The Tagged GPO Deleted



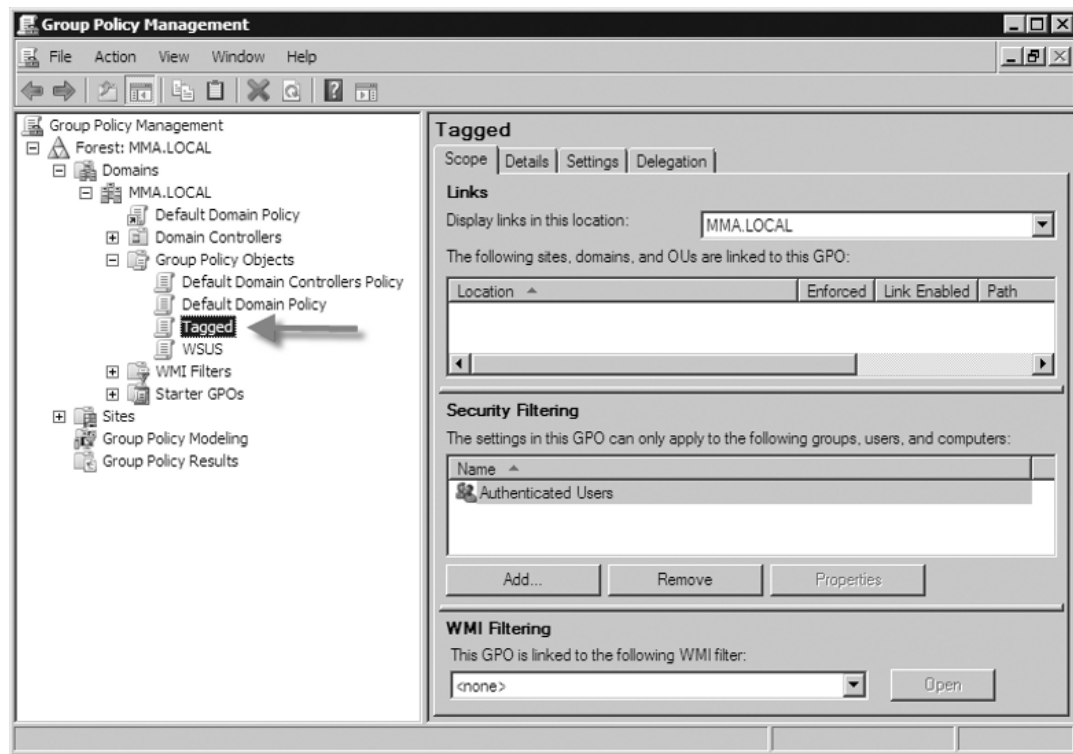
3. In the GPMC, right-click **Group Policy Objects** and select **Manage Backups**, as shown in Figure 5.43.

Figure 5.43 Selecting Manage Backups

4. In the **Manage Backups** screen shown in Figure 5.44, select the **Tagged** GPO and click **Restore**. You will be asked whether you want to restore the selected backup; choose **OK**. As you'll notice here, we could show only the most up-to-date backups if we wanted to, or we could have all backups come up. We can delete the backup of the GPO(s) and we can view settings from the GPO itself. In the settings you will see items such as the GPO's GUID, whether it is enabled, any links, Security Filtering, WMI Filtering, delegation, and computer and user configuration. The settings will come up as an .htm file and will be shown in Internet Explorer.

Figure 5.44 The Manage Backups Screen

5. Once the restore is complete, the status window should read **Tagged...Succeeded**. If so, just click **OK**. Then click **Close** in the **Manage Backups** screen.
6. Now looking at the GPOs via the GPMC, you should see that the Tagged GPO has been restored, as shown in Figure 5.45.

Figure 5.45 The Tagged GPO Restored

Offline Maintenance

In the past, with Windows 2000 and Windows Server 2003, to do any offline maintenance such as defragging the Active Directory database you would have to reboot and go into the DSRM. If users relied on services such as file and print, the Dynamic Host Configuration Protocol (DHCP), and others they were out of luck until the server was back online. That has now changed under Windows Server 2008. Windows Server 2008 now supports the use of restartable Active Directory Domain Services which brings offline maintenance to a whole new level.

Restartable Active Directory

Restartable Active Directory Domain Services is a new feature in Windows Server 2008. It allows administrators to perform routine maintenance tasks on a DC far quicker and with less interruption than ever before. The key is that Active Directory

Domain Services can be stopped without affecting other services on a DC, such as DHCP and file/print. With the advent of restartable Active Directory Domain Services, DCs running Windows Server 2008 now have three possible states to run in, as shown in Table 5.2.

Table 5.2 Three States of Server 2008 DCs

State	Description
Active Directory Domain Services Started	Active Directory Domain Services is running. Services provided by a DC are running.
Active Directory Domain Services Stopped	Active Directory Domain Services has been stopped. From an administrator's point of view, this provides the ability to perform offline maintenance just like running in DSRM. Maintenance is much faster than having to use DSRM. This primarily will act as a member server while the service is stopped.
Directory Services Restore Mode	This is unchanged from Windows Server 2003, except that an administrator can run <i>dcpromo /forceremoval</i> to remove Active Directory Domain Services from that particular DC.

There are some things to keep in mind regarding restartable Active Directory Domain Services. A DC cannot start up with Active Directory Domain Services stopped. If you set the **startup type** to **Disabled** and reboot the server, it will come back with Active Directory Domain Services started and set back to **automatic**. Stopping Active Directory Domain Services also stops the File Replication Service (FRS), Kerberos Key Distribution Center (KDC), intersite messaging, the domain name system (DNS) server (if installed), and Distributed File System (DFS) replication. Restarting Active Directory Domain Services, though, will automatically restart those services as well.

You can stop and start restartable Active Directory Domain Services using the Microsoft Management Console (MMC) via Services or by using the *net.exe* command. Exercise 5.11 runs through stopping and starting Active Directory Domain Services in Windows Server 2008.

EXERCISE 5.11

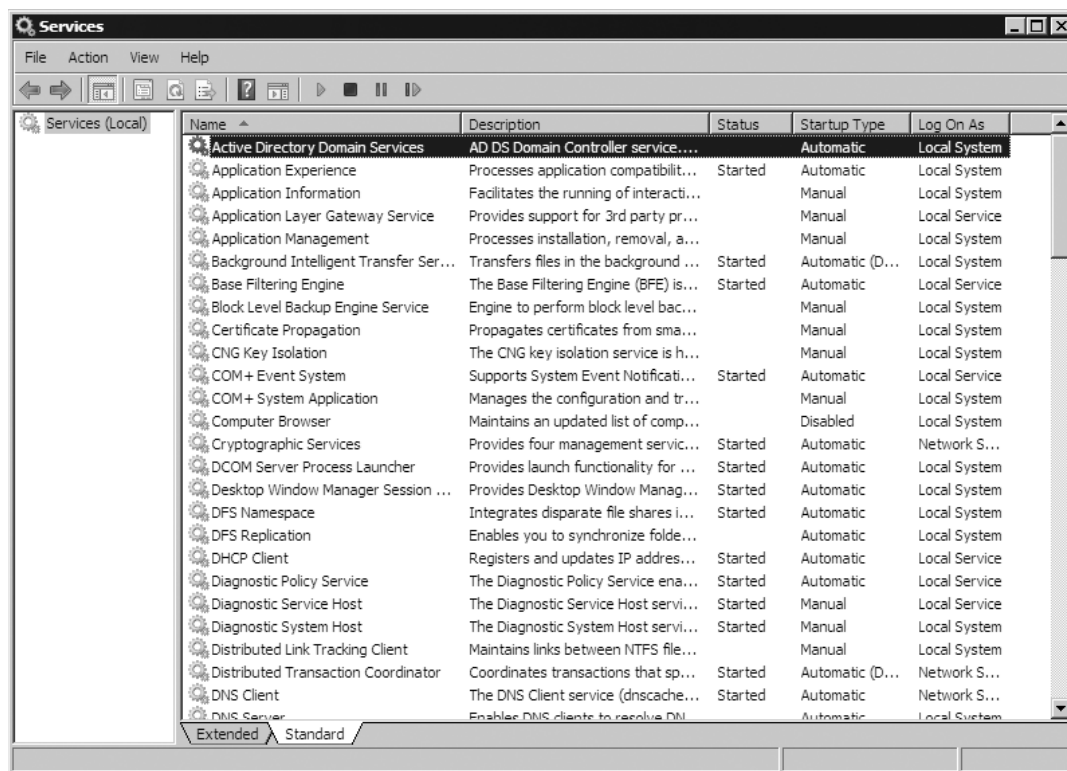
STOPPING AND STARTING RESTARTABLE ACTIVE DIRECTORY DOMAIN SERVICES

1. Log on to a DC as an administrator.
2. Click **Start | Administrative Tools | Services**.
3. In the list of services, highlight and right-click on **Active Directory Domain Services** and click **Properties**.
4. The service status should read **Started**; just click **Stop**.
5. After you click **Stop**, a window will pop up titled **Stop Other Services**, which you can see in Figure 5.46. This window will inform you of the other services that will also be stopped. Click **Yes** and then **OK**.

Figure 5.46 Services That Stop with Active Directory Domain Services



6. Now you will see that Active Directory Domain Services has stopped (see Figure 5.47).

Figure 5.47 Active Directory Domain Services Stopped**EXAM TIP**

In step 3 of Exercise 5.11, you could simply right-click on the Active Directory Domain Services service and select **Stop**. This will stop the service just as well.

Offline Defrag and Compaction

Active Directory's database file is `ntds.dit`, and it is based on the Extensible Storage Engine (ESE) and is located in `C:\Windows\NTDS`. One of the biggest reasons, if not the only reason, to defrag/compact the `ntds.dit` file is if you are running low on disk space. Depending on the size of your environment, the `ntds.dit` file can grow

to more than 6 GB in size, even though the database within it may only be 1 GB. Back in the days of Windows 2000 and Windows Server 2003, we had to perform offline defrags in the DSRM because there was no way to easily shut down Active Directory and perform the defrag. As you've already seen, that has changed, and for the better, in Windows Server 2008. We simply go into **Services** and stop **Active Directory Domain Services**. Exercise 5.12 lists the steps involved in defragging Active Directory in Windows Server 2008.

EXERCISE 5.12

DEFRAGGING ACTIVE DIRECTORY DOMAIN SERVICES

1. Before performing a defrag of `ntds.dit`, perform a system state backup of the DC or perform a full server backup. Even though we can move or rename the old `ntds.dit` file, having a backup is essential in case of catastrophe.
2. Go to **C:\Windows\NTDS** and note the size of the `ntds.dit` file. In our case, because this is a lab machine our `ntds.dit` file is only 12 MB. Create a new directory to initially hold the new `ntds.dit` file that will be created during the defragging process. Our directory is **C:\Windows\NTDS\defragged**.
3. Log on to the server as an administrator and stop the **Active Directory Domain Services** service, as discussed in the preceding section.
4. After Active Directory Domain Services has stopped, open a command prompt (**Start | Command Prompt**), type `ntdsutil`, and press **Enter**.
5. At the `ntdsutil` prompt, type **Activate Instance ntds** and press **Enter**. You will get a message stating **Active instance set to "ntds"**.
6. At the `ntdsutil` prompt, type **files** and press **Enter**. This will pull up the **file maintenance** prompt.
7. At the file maintenance prompt, type **info** and press **Enter**. This provides you with information about the location of the `ntds.dit` file, the backup directory, the working directory, and the log directory. Figure 5.48 shows an example.

Figure 5.48 The Drive and DS Path Information

```

C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: info

Drive Information:

      C:\ NTFS <Fixed Drive  > free<2.7 Gb> total<24.9 Gb>
      E:\ NTFS <Fixed Drive  > free<13.7 Gb> total<19.9 Gb>
      F:\ NTFS <Fixed Drive  > free<14.5 Gb> total<34.9 Gb>
      Z:\ NTFS <Network Drive> free<25.7 Gb> total<74.5 Gb>

DS Path Information:

Database   : C:\Windows\NTDS\ntds.dit - 12.1 Mb
Backup dir : C:\Windows\NTDS\dsadata.bak
Working dir: C:\Windows\NTDS
Log dir    : C:\Windows\NTDS - 30.0 Mb total
              edbres00002.jrs - 10.0 Mb
              edbres00001.jrs - 10.0 Mb
              edb.log - 10.0 Mb

file maintenance: _

```

8. At the file maintenance prompt, type **compact to c:\windows\ntds\defragged** and press **Enter**. The defrag process will run. The larger your ntds.dit file is, the longer the defrag process will take. Figure 5.49 shown an example of a successful defrag.

Figure 5.49 A Successful Defrag

```

Administrator: Command Prompt
Initiating DEFRAGMENTATION mode...
Source Database: C:\Windows\NTDS\ntds.dit
Target Database: c:\windows\ntds\defragged\ntds.dit

      Defragmentation  Status <% complete>

      0   10   20   30   40   50   60   70   80   90  100
      !---!---!---!---!---!---!---!---!---!---!
      .....

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
  copy "c:\windows\ntds\defragged\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
  del C:\Windows\NTDS\*.log

file maintenance: q
ntdsutil: q
C:\Users\Administrator>

```

9. After the defrag has completed, type **q** at the file maintenance prompt and do the same at the **ntdsutil** prompt. This should bring you back to a normal **C** prompt; you can close the command prompt at this time.
 10. Go to the **C:\Windows\NTDS** folder and either rename the **ntds.dit** file there or delete it.
 11. Go to the **defragged** directory and move the **ntds.dit** file from there to the **C:\Windows\NTDS** directory.
 12. In the **C:\Windows\NTDS** directory, rename or delete the **edb.log** file.
 13. Go back to **Services** and **restart** Active Directory Domain Services. After it restarts, you're finished.
-

Active Directory Storage Allocation

As you've learned, the **ntds.dit** file can get quite large. With this comes concern regarding available drive space. To conserve drive space, we've already walked through defragging and compacting the **ntds.dit** file. Sometimes that's not enough, and you have to move it and its log files to another drive or partition. Before doing this, you have to confirm the size of the files in the **C:\Windows\NTDS** folder. You need to check the amount of drive space used by the files in the directory when Active Directory Domain Services is online and offline, because the files that are offline are what you will actually move, but when Active Directory Domain Services is back online the amount of drive space increases.

So, why is there a difference in the amount of space used in **C:\Windows\NTDS** when Active Directory Domain Services is offline versus online? The answer is quite simple: Active Directory will create a **temp.edb** file and you have to consider that when determining the amount of space to allocate to Active Directory. Here are some scenarios in which you would determine storage allocation for Active Directory:

- **NTDS.DIT only** The size of the file plus an additional 20% of the current file size or 500 MB, whichever is greater
- **Log files only** The combined size of the log files plus 20% of the combined logs or 500 MB, whichever is greater

- **NTDS.DIT and log files** If the database file and the logs are located on the same partition, the free space should be at least 20% of the combined NTDS.DIT and log files, or 1 GB, whichever is greater

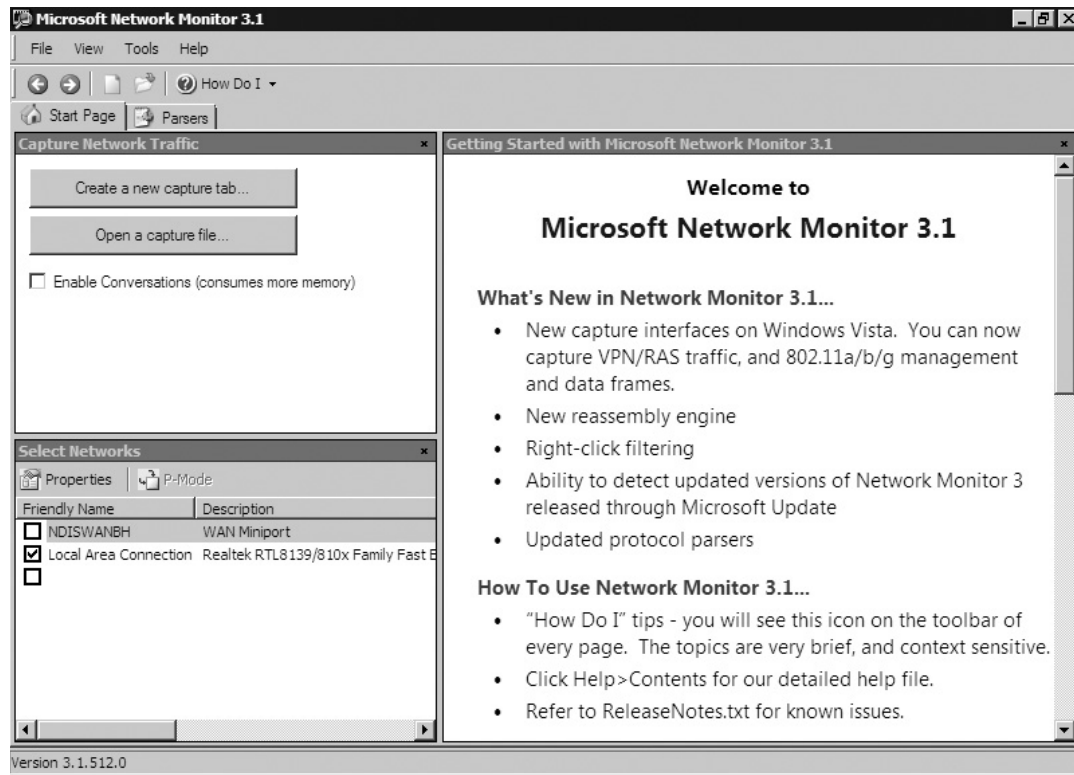
Monitoring Active Directory

Monitoring Active Directory is a key in making sure that objects and attributes are up-to-date and consistent among DCs, whether they are local to each other or located at different sites. One area to monitor is replication between the DCs. To do this we use tools such as Network Monitor, the Event Viewer, replmon, and repadmin. We also need to ensure the performance of the DCs so that they are able to authenticate and replicate in a timely manner by using tools such as the Task Manager, systems resource manager, reliability and performance monitor, and the Event Viewer. Let's examine each of these tools.

The Network Monitor

It's important for administrators to keep tabs on network traffic that's flowing across the network. Monitoring the network has allowed administrators to have a better understanding of how the bandwidth on their networks is being utilized. Network Monitor from Microsoft is such a tool. It is a protocol analyzer that allows administrators to capture network traffic, and then view and analyze it. Administrators can see things such as DHCP requests, DNS name resolutions, Hypertext Transfer Protocol (HTTP), and so on. As of this writing, Network Monitor Version 3.1 runs on Windows Server 2008. It does not ship with Active Directory, but you can download it from www.microsoft.com/downloads/details.aspx?FamilyID=18b1d59d-f4d8-4213-8d17-2f6dde7d7aac&displaylang=en.

To start Network Monitor just click **Start | Microsoft Network Monitor 3.1 | Microsoft Network Monitor 3.1**. You will see the **Start Page** shown in Figure 5.50. Here you can create a new capture or open an existing one. You will also notice the Welcome screen to the right, which will mention all the changes in Network Monitor. In addition to the Start Page tab, you will see the Parsers tab, which allows you to parse packs. Network Monitor applies knowledge of the structure of the various protocols to the hex data contained in the packets and displays the resultant interpretation.

Figure 5.50 The Network Monitor

Although we can't actually see the information transmitted across the wire for Active Directory replication, we can see things such as when a new DC comes up and queries DNS for an existing Lightweight Directory Access Protocol (LDAP) server at the **Default-First-Site-Name** sight. Figure 5.51 shows this in the **Display Filter**.

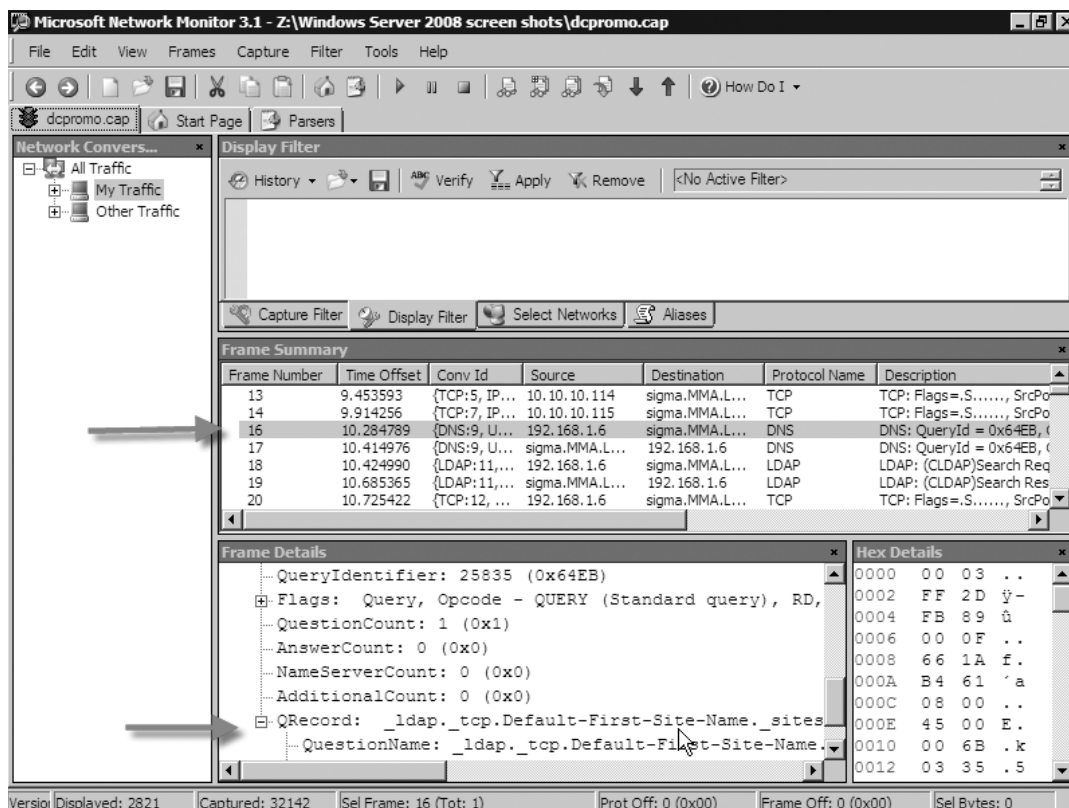
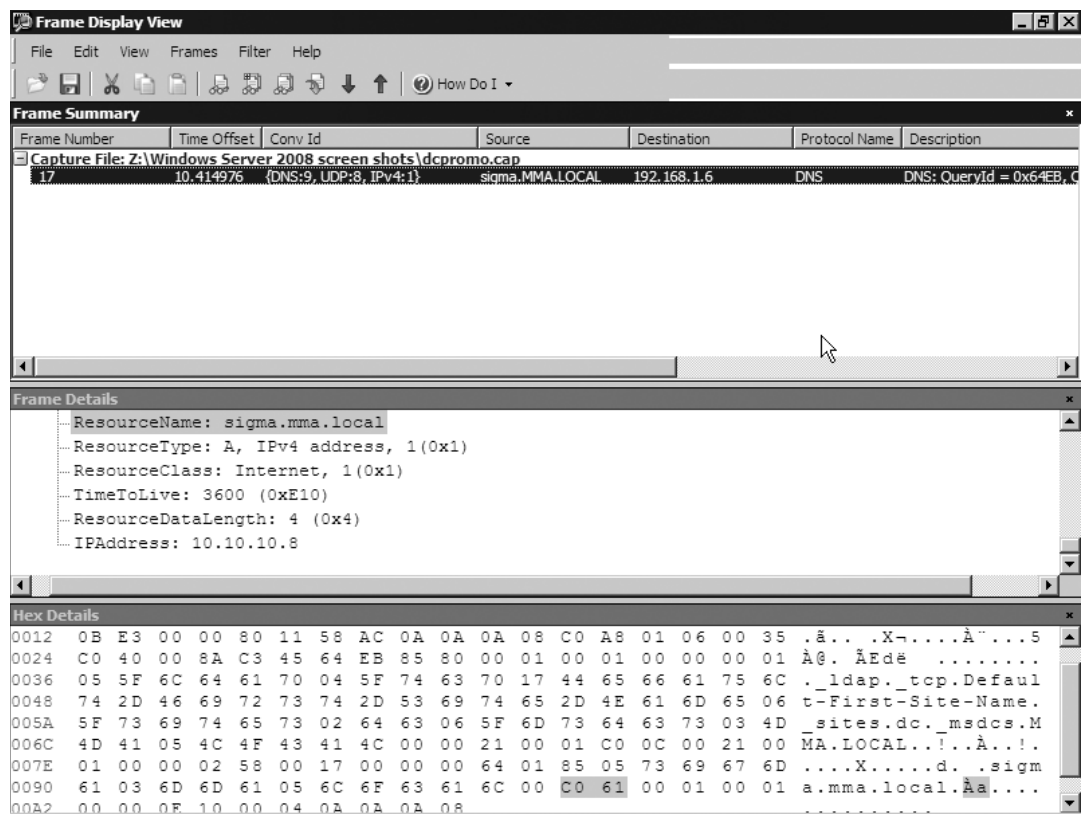
Figure 5.51 The Display Filter in Network Monitor 3.1

Figure 5.51 represents a snapshot of what was happening when a member server was running DCPROMO and was being promoted to a DC. In the figure, the new DC (192.168.1.6) performs a DNS query to SIGMA.MMA.LOCAL, wanting the information about the LDAP server at that site. The DNS server, in this case SIGMA.MMA.LOCAL, responds with the A record and a type SRV of _ldap._tcp.Default-First-Site-Name. As you can see in Figure 5.52, it informs the new DC (192.168.1.6) that the resource name is SIGMA.MMA.LOCAL and that the Internet Protocol (IP) address is 10.10.10.8. In this example, it just so happens that the LDAP server at this site is also the DNS server. In some instances it may not be, depending on the environment.

Figure 5.52 The Response to the DNS Query



To get the view in Figure 5.52, we highlighted the **Frame Number** in the **Frame Summary** and right-clicked on it, and then chose **View Selected Frame(s) in a New Window**. This made it easier for us to read the DNS server's response. Alternatively, we could have right-clicked the Frame Number and selected **Copy**, **Copy Cell Value**, **Copy Cell as Filter**, **Add Cell to Display Filter**, **Parse Frame as XML**, **View Selected Frame(s) in a New Window**, or **Add Selected Frame(s) To**.

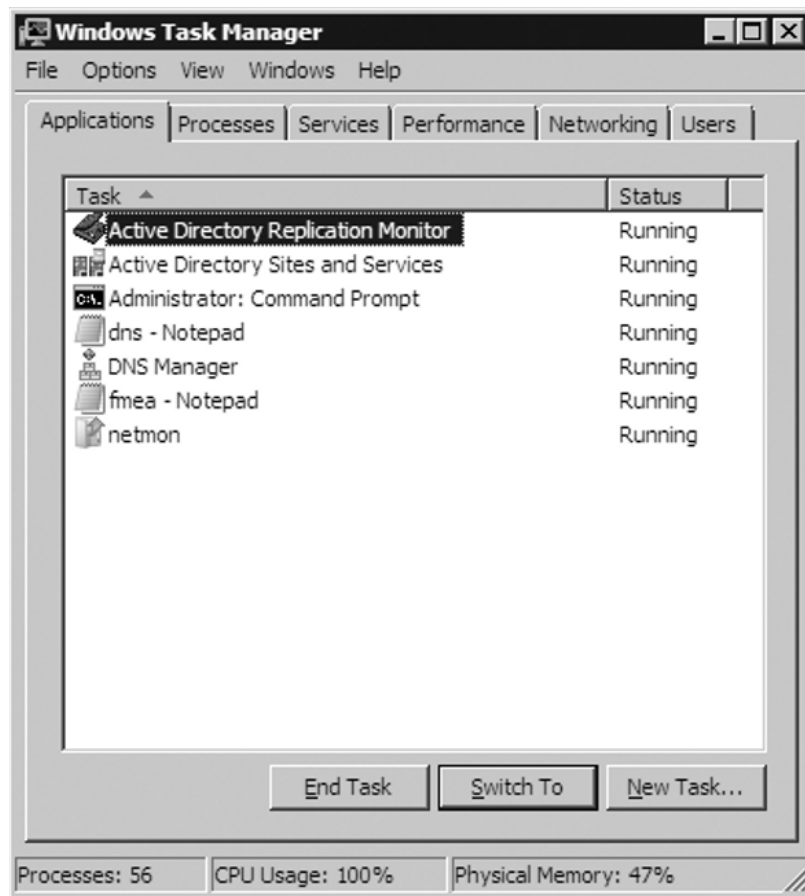
As you can see, a tool such as Network Monitor can be valuable in determining what is actually happening on the wire and where problems may arise.

The Task Manager

You can monitor the load and performance of DCs through the Task Manager, which hasn't changed much since Windows Server 2003. The Task Manager shown in Figure 5.53 can show administrators what may be causing slow logons for users,

along with what processes and executables are using resources, causing strain on a DC. You can pull up the Task Manager in quite a few ways. The easiest way is to just click **Start** | **Run** and type **taskmgr.exe** and press **Enter**. Other ways to launch the Task Manager include right-clicking the **task bar** and selecting **Task Manager**, pressing **Ctrl + Shift + Esc**, and pressing **Ctrl + Alt + Delete** and selecting **Start Task Manager**.

Figure 5.53 The Task Manager



The Task Manager is very useful for administrators looking for an immediate view of resources such as processor activity, process activity, network activity, memory usage, resource consumption, and even user information. A Services tab has been added to the Task Manager, along with a Services button that allows administrators

to pull up the Services Management Console. Another big change is the Resource Monitor button within the Performance tab. Let's briefly go over each tab in the Task Manager.

The Applications Tab

The first tab in the Task Manager is the Applications tab, which lists all the tasks and programs currently running on the server and their status. The status of programs will be either **Running** or **Not Responding**. However, when an application's status is at Not Responding, it may be waiting for a process to respond, in which case it could return to a Running state. If an application remains at a Not Responding state for some time, an administrator can simply right-click the application in the list and choose **End Task**, as shown in Figure 5.54.

Figure 5.54 Ending a Task

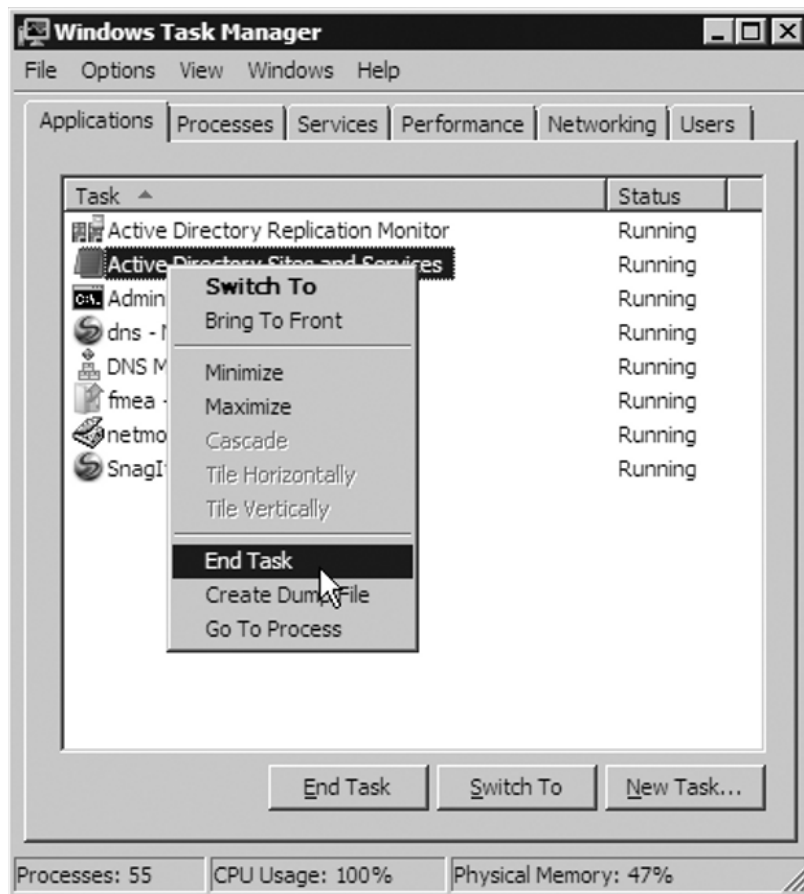
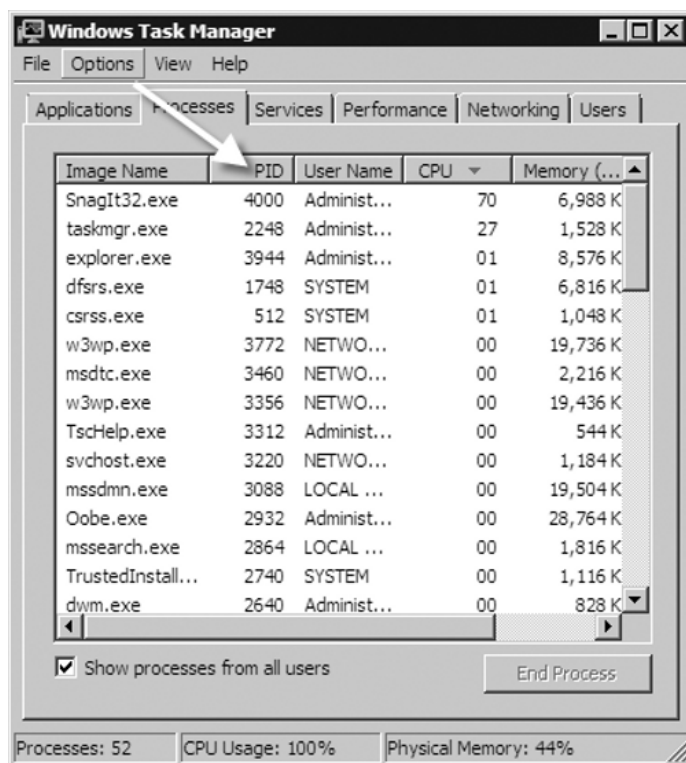


Figure 5.54 shows other options as well. By selecting **Switch To** you can switch to a different running task. Selecting **Bring To Front** will bring that application/task to the front of the desktop. You can use **Create Dump File** for a point-in-time snapshot of whatever process you need to examine for more advanced troubleshooting.

The Processes Tab

The Processes tab provides a list of processes that are currently running on the server. These processes are measured by performance by such things as **CPU**, **User Name** (or the context under which the image is running), and **Memory** (Private Working Set), among others. Administrators can sort out what processes are using the most or least CPU cycles by clicking on CPU and Memory column headers. You can shut down a process by right-clicking the process name and selecting **End Process**. You also can add other columns; for instance, you can add a PID column by clicking on **View | Select Columns** and choosing **PID (Process Identifier)**, and then clicking **OK**. Figure 5.55 shows the results.

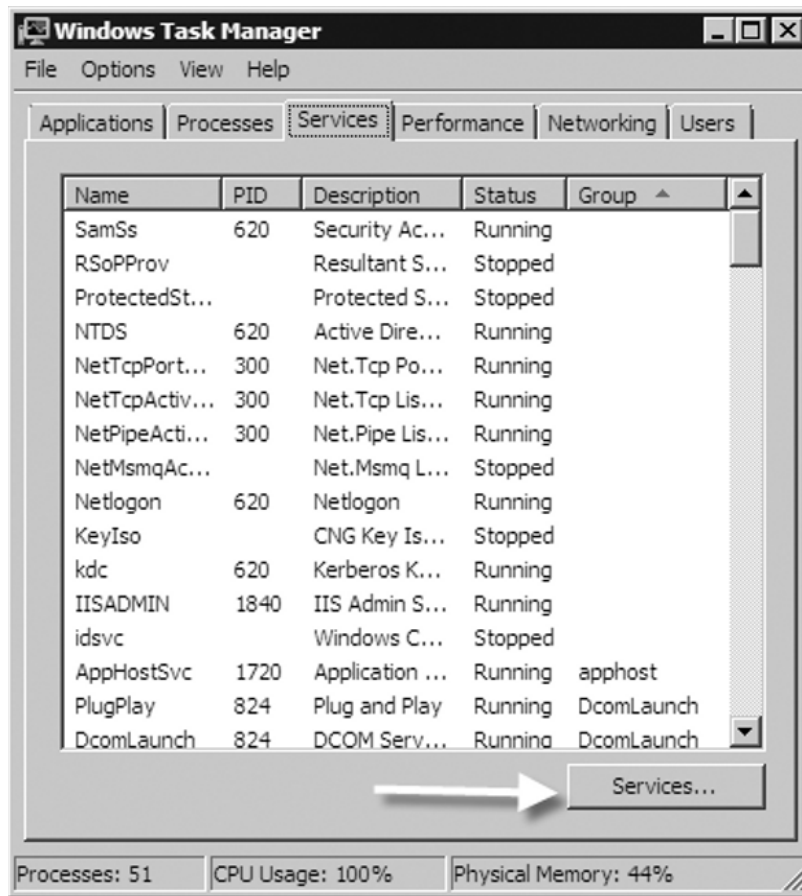
Figure 5.55 Adding a PID Column



The Services Tab

The newest tab in the Task Manager—but one that's been overdue—is the Services tab. With this tab, administrators can quickly assess and troubleshoot a specific service by viewing its status. By default, it shows the service's name, PID, description, status, and group. As mentioned earlier, you can even launch the Services Console by clicking on the **Services** button in the bottom-right corner, as shown in Figure 5.56.

Figure 5.56 The Services Tab

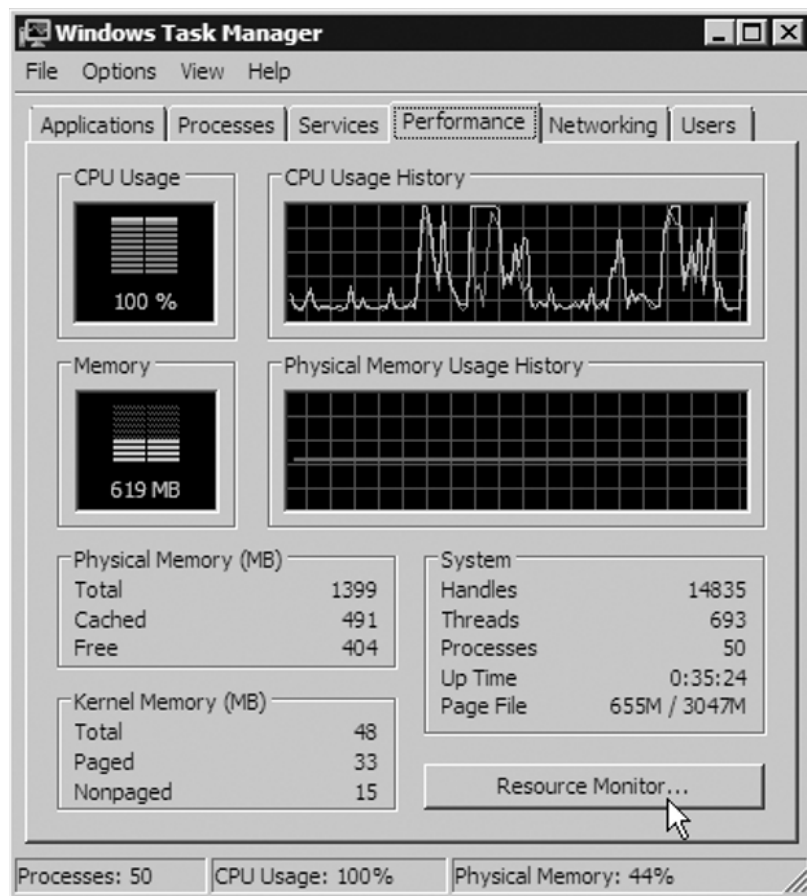


The Performance Tab

The Performance tab allows administrators to view CPU and physical memory usage in an easier-to-understand/graphical manner. It is very useful when an administrator needs a quick analysis of how the system is running. The Performance tab shows CPU usage in a real-time manner, while also showing a brief usage history.

It does the same for memory usage as well. By default, the Performance tab shows usage by User Mode processes and threads. If you want to see Kernel Mode usage as well, all you have to do is click on **View | Show Kernel Times**. You will then see kernel mode operations in red in the CPU Usage area. If your server has multiple processors, you will be able to view each individual processor and its corresponding graph. Notice in Figure 5.57 a button in the bottom right labeled Resource Monitor. By clicking on this, you can perform even more analysis. We will cover the System Resource Monitor a little later.

Figure 5.57 The Performance Tab

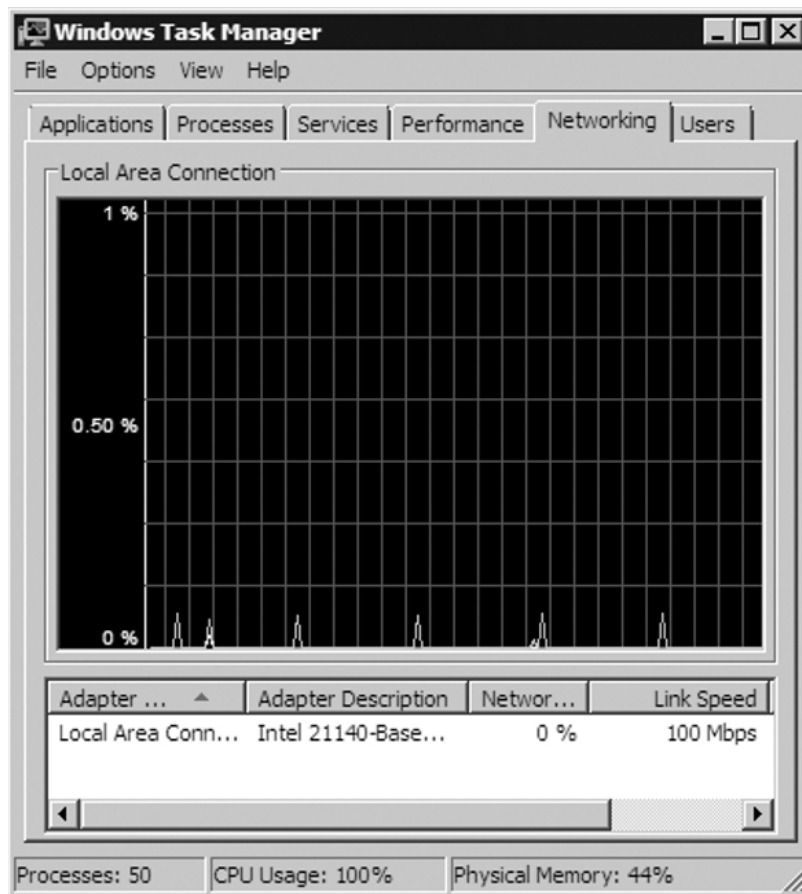


The Networking Tab

The Networking tab provides information about network traffic for each adapter in a particular server. Multiple adapters and adapter types are supported. For instance,

you could have a LAN connection, a virtual private network (VPN) connection, and a dial-up connection all showing up as separate adapters. The Networking tab will show a graphical comparison of the traffic for any connection a server has. Administrators are able to get information about network utilization, link speed, and even the state of the connection. You can examine network traffic in the graph in terms of bytes sent, bytes received, and the total number of bytes simply by clicking **View | Network Adapter History** and selecting what you want. As with many of the other tabs in the Task Manager, you can add more columns to widen your analysis. Simply click **View | Select Columns** and select the column(s) you need. In Figure 5.58, you see that we have added the column **Adapter Description**.

Figure 5.58 The Networking Tab



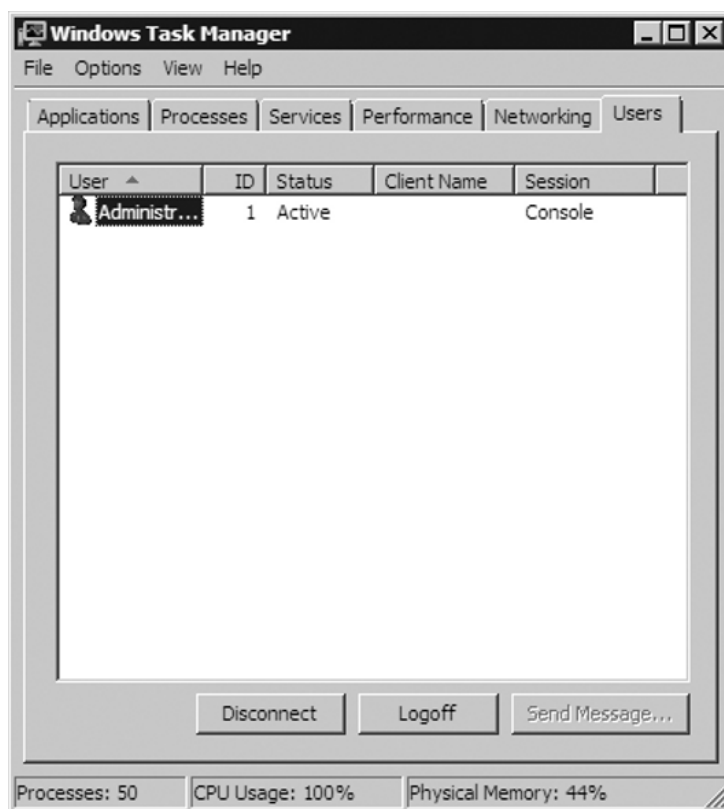
EXAM WARNING

You may be asked on the exam about a problem with a server and you'll need to quickly gather data. You should start up the Task Manager and look at key indicators such as CPU utilization, process utilization, available memory, and network utilization. Look for skewed numbers around 70% or higher that might be causing performance issues.

The Users Tab

The last tab in the Task Manager is the Users tab. It displays the users who are connected to or logged on to the server. It provides user, ID, status, client name, and session information by default. Although there are no additional columns to add, you can remove any you feel are unnecessary. Figure 5.59 shows that the only user connected to this server is the administrator and that he is at the console.

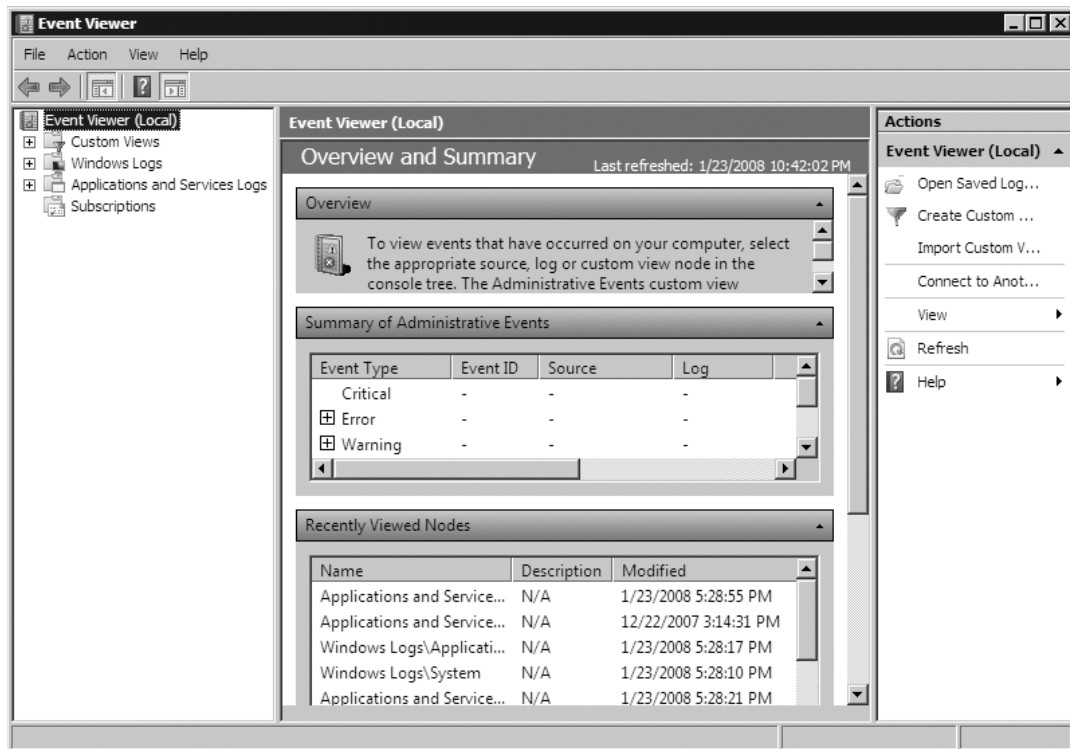
Figure 5.59 The Users Tab



The Event Viewer

The Event Viewer is traditionally the first place to look when troubleshooting anything in Windows (see Figure 5.52). You can access the Event Viewer by clicking on **Start | Administrative Tools | Event Viewer**. This tool which has stood the test of time since the days of NT 3.1 has been completely rewritten and is based on XML. Many new features, functionality, and even a new interface have been added to the Event Viewer in Windows Server 2008. Figure 5.60 shows the new interface for the Event Viewer, taken from MMC Version 3.0.

Figure 5.60 The Event Viewer



Looking at Figure 5.60, you'll notice that the Event Viewer consists of Custom Views, Windows Logs, Applications and Services Logs, and Subscriptions. Let's examine each of these more closely.

Custom Views

Custom Views in the Event Viewer are filters created by either Windows Server 2008 or an administrator to the system. Custom views created by Windows

Server 2008 can happen when a server takes on a new role such as a DC running Active Directory Domain Services or installs a feature such as DNS. Administrators are able to create filters that target only the events they are interested in viewing. In Exercise 5.13, we'll create a custom view in the Event Viewer. To create a custom view in the Event Viewer, right-click **Custom Views** and select **Create Custom View**.

EXERCISE 5.13

CREATING A CUSTOM VIEW

1. Open the Event Viewer by clicking **Start | Administrative Tools | Event Viewer**.
2. In the Event Viewer, right-click **Custom Views** and select **Create Custom View**.
3. Next, the **Create Custom View** form comes up. In the **Logged** drop-down list choose when you want events logged. For instance, you can choose to do **Any time**, **Last hour**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, or a **Custom range**. When choosing **Custom range** you decide the date and time from the first event to the date and time of the last event. You can even choose the actual time. For our example, we chose **Last 30 days** for this exercise.
4. Next, choose the **Event level** you want to include. These are the same old standbys we've seen in previous versions of Windows: **Critical**, **Warning**, **Verbose**, **Error**, and **Information**. For our example, we'll select only **Warning**.
5. After you have decided on the **Event level**, you need to choose the event log(s) or the specific event sources to filter by. We'll simply choose **By log** and select **System** found beneath **Windows Logs**.
6. If you know exactly what event IDs you want to filter you can do that by simply typing the event ID(s). Because we don't, we'll leave it at **<All Event IDs>**. For **Keywords**, we can click on the pull-down menu and see a list of keywords from which to choose. We can enter any particular user or computer we like. For our example, we will only specify the server SIGMA in the **Computer(s)** line. Your **Create Custom View** should appear like the one in Figure 5.61. When you're done, click **OK**.

Figure 5.61 Creating a Custom View

Create Custom View

Filter XML

Logged: Last 30 days

Event level: ☐ Critical ☒ Warning ☐ Verbose
☐ Error ☐ Information

☒ By log Event logs: System

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

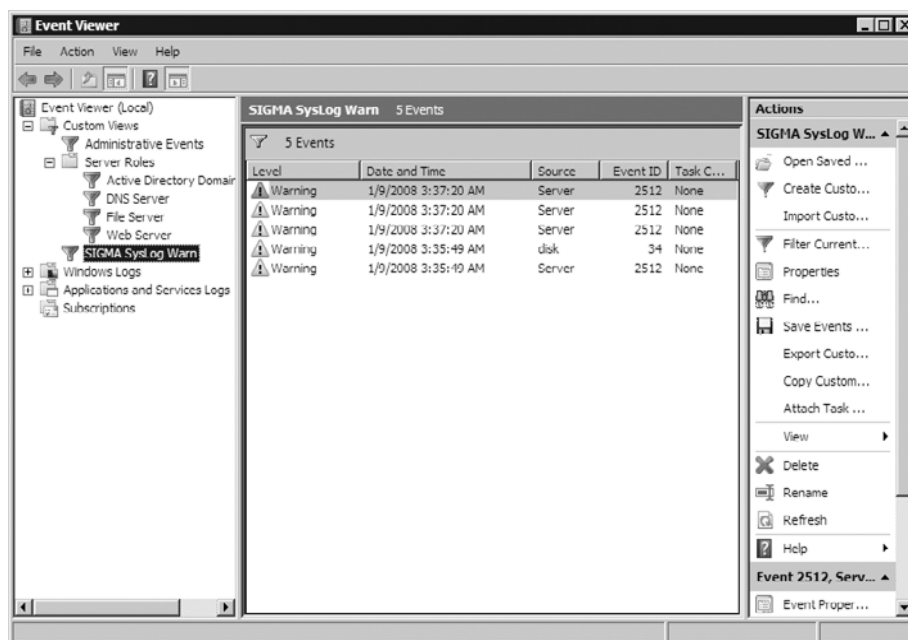
Computer(s): SIGMA

Clear

OK Cancel

7. Next, you come to **Save Filter to Custom View**. You can choose a name to call your filter and provide a description if you like. You also get to choose where you want your custom view saved. For our example, the name will be SIGMA SysLog Warn and we'll allow it to be saved in the default location.

In Figure 5.62, you see we have created our custom view SIGMA SysLog Warn and that there are five events in it. Your server will probably have different warnings than the one shown in the figure.

Figure 5.62 A Newly Created Custom View

Windows Logs

Underneath the Windows Logs folder are the traditional logs we've seen before, with two new ones added. Table 5.3 provides a brief description of each log.

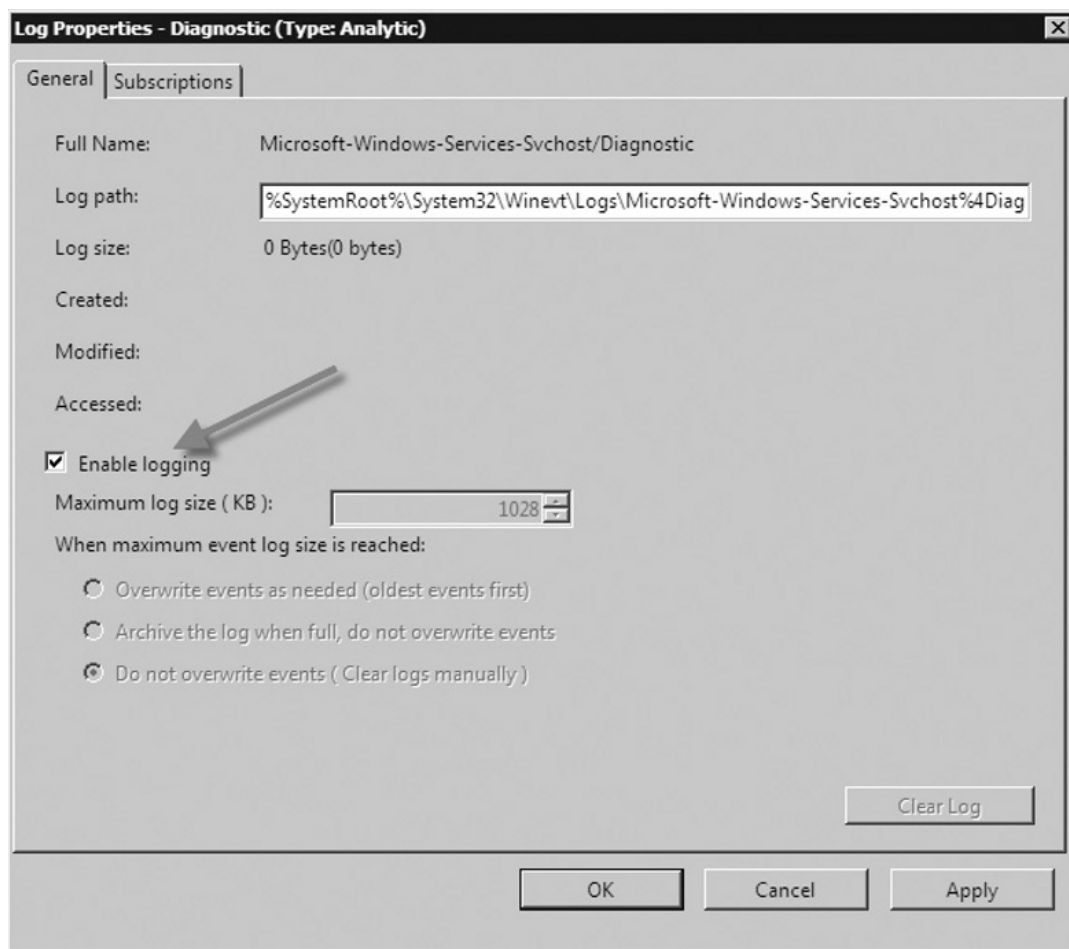
Table 5.3 Windows Logs

Log	Description
Application	Contains events from applications residing on the system
Security	Captures authentication and object access events that are audited
Setup	New log that captures events tailored around the installation of applications, server roles, and features
System	Events built around Windows system components are logged here
Forwarded Events	Consolidates and stores events that were captured from remote systems and sent to a single log to facilitate the identification, isolation, and solving of problems

Applications and Services Logs

There is a new category of event logs in Windows Server 2008: the Applications and Services logs. In Figure 5.62, you can see them just below the Windows Logs folder. These logs store events from a single application or component rather than events like the logs underneath Windows Logs. You can find four subtypes of logs here: Admin, Operational, Analytic, and Debug. Admin logs are tailored more for users and administrators looking to troubleshoot problems. The events in the Admin log will provide administrators with information and guidance regarding how to respond. Events found in the Operational log are more likely to require more interpretation but can be helpful as well.

The Analytic and Debug logs are not user-friendly. You can use Analytic logs to trace an issue, and therefore a high number of events are logged. Developers use the Debug logs when debugging applications. The Analytic and Debug logs are hidden and disabled by default in Windows Server 2008. To show these logs select **Event Viewer | View | Show Analytic and Debug Logs**. Remember that this only shows the logs; it does not enable them. To enable the Analytic and Debug logs, make sure they are not hidden and then highlight the Analytic or Debug log you want to enable. Click on **Action | Properties** and in the **Log Properties** screen, shown in Figure 5.63, select **Enable logging** and click **OK**. You can also enable these logs via the command line by typing **wevutil sl <logname> /e:true**.

Figure 5.63 Enabling an Analytic Log

Subscriptions

The last folder shown in the Event Viewer is also a new feature in Windows Server 2008, called Subscriptions. The Subscriptions folder allows remote servers to forward events so that they can be locally viewed at a central station. A subscription specifies exactly what events will be collected and to which log they will be stored. Once collected, data from a subscription can be viewed and manipulated just as though it came directly from the server from which you're examining them. To use subscriptions, you must configure both the forwarding and collecting servers. Both the Windows Remote Management (WinRM) and Windows Event Collector (Wecsvc) services are required. Exercise 5.14 teaches how to create a new subscription.

EXERCISE 5.14

CREATING A NEW SUBSCRIPTION

1. Go to the collector computer and run the **Event Viewer** as an administrator.
2. In the Event Viewer click **Subscriptions** in the console tree. If the **Windows Event Collector** service is not running, you will be prompted to run it; if you receive this message click **Yes**.
3. Click **Actions | Create Subscription**. The **Subscription Properties** box appears, as shown in Figure 5.64.

Figure 5.64 The Subscription Properties Box

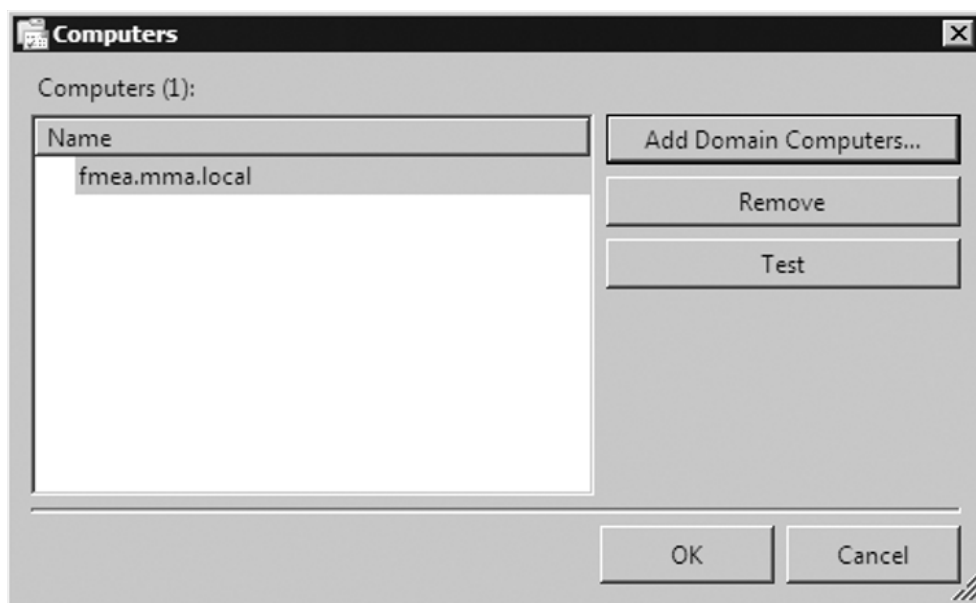
The screenshot shows the 'Subscription Properties' dialog box. It has a title bar with a close button. The dialog contains several fields and sections:

- Subscription name:** A text input field.
- Description:** A text input field with up and down arrow buttons on the right.
- Destination log:** A dropdown menu currently showing 'Forwarded Events'.
- Subscription type and source computers:** A section with two radio buttons:
 - Collector initiated:** Selected. Next to it is a 'Select Computers...' button. Below the radio button is the text: 'This computer contacts the selected source computers and provides the subscription.'
 - Source computer initiated:** Unselected. Next to it is a 'Select Computer Groups...' button. Below the radio button is the text: 'Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.'
- Events to collect:** A dropdown menu showing '<filter not configured>'. To its right is a 'Select Events...' button.
- User account (the selected account must have read access to the source logs):** A text field showing 'Machine Account'.
- Change user account or configure advanced settings:** A button labeled 'Advanced...'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

4. In the **Subscription name** box, type a name for the subscription. For our example, we chose **Test** as the name.

5. In the **Description** box, type an optional description for the subscription. We typed **Test subscription** for ours.
6. At the **Destination log** drop-down list, select the log file where the collected events are to be stored. The default, as you see in Figure 5.64, is **Forwarded Events**. For our example, we will accept the default.
7. Under **Subscription type and source computers**, choose the default of **Collector initiated** and click **Select Computers**.
8. In the **Computers** screen, click **Add Domain Computers**. You will now be asked to type the name of the computer(s) from which you would like to collect information. For our scenario, we typed **FMEA**. Click **Check Names** to verify and then click **OK** to continue.
9. Now the **Computers** screen will look like Figure 5.65, and you will see the computer we just selected. If it is correct click **OK** then **OK** again at the **Subscription Properties** screen.

Figure 5.65 The Computer Selected for Subscription



10. Now click **Select Events** and you should see the Query Filter. The Query Filter will be exactly like the Create Custom View you saw in Figure 5.61. For our example, we will choose **Any time** for

Logged, and **Critical**, **Warning**, and **Error** for **Event Level**. We will choose **By log** and the **Application** for **Event logs**. Everything else will remain the same, as shown in Figure 5.66. Now click **OK**.

Figure 5.66 The Query Filter

Query Filter

Filter XML

Logged: Any time

Event level: ☒ Critical ☒ Warning ☐ Verbose
☒ Error ☐ Information

☒ By log Event logs: Application

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

11. Now just go to the source server (the one that will forward events) and open a command prompt. In the command prompt, type **winrm quickconfig** and press **Enter**. On the collector server, at a command prompt type **wecutil qc** and press **Enter**.

12. Now add the collector server to the Administrators local group of the computer, and that's it!
-

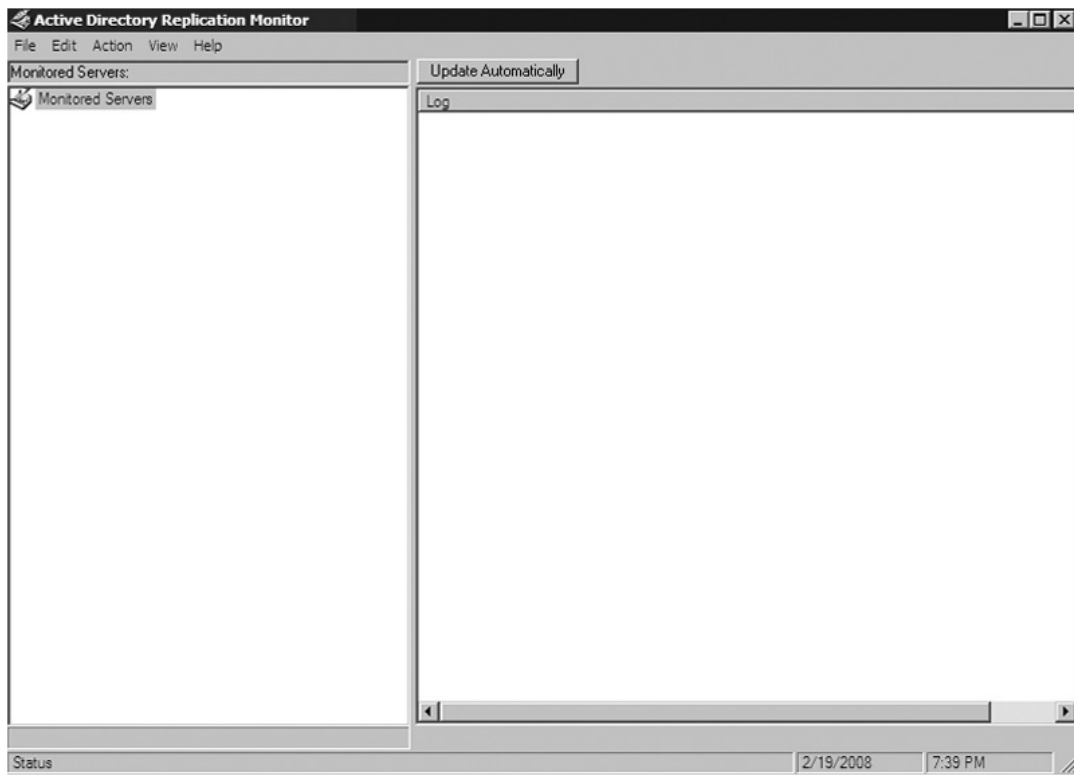
Replmon

Replication Monitor, better known as Replmon, is a GUI tool that you can install with the Support Tools found on the Windows Server 2008 DVD. This tool enables administrators to view the detailed status of Active Directory replication. It also allows administrators to force synchronization between DCs, view the topology in an easier-to-understand graphical format, and monitor the status and performance of DC replication. Replmon is useful but not limited to the following:

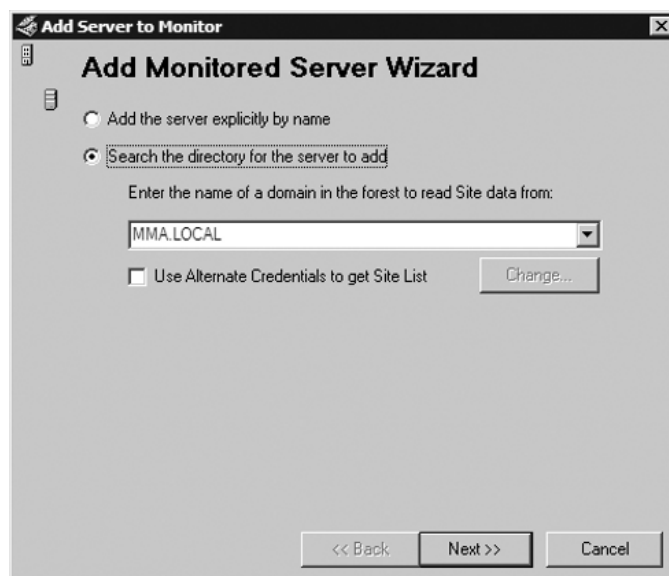
- Noticing when a replication partner fails
- Viewing the history of both failed and successful replication
- Viewing the properties of directory replication partners
- Generating status reports including direct and transitive replication partners along with detailing a record of changes
- Displaying replication topology
- Forcing replication
- Triggering the Knowledge Consistency Checker (KCC) to recalculate the replication topology
- Displaying a list of trust relationships maintained by a DC that is being monitored
- Monitoring the replication status of DCs from multiple forests

Using Replmon

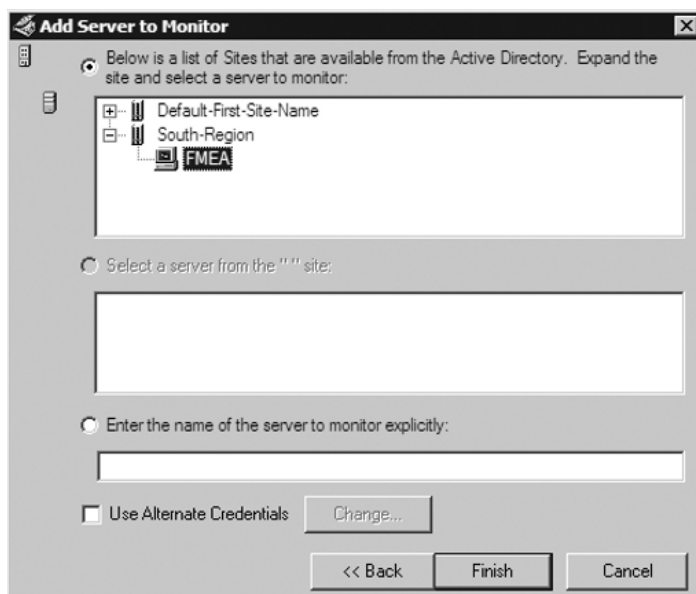
To use replmon you must be logged on to a DC. Once logged on, select **Start | Run** and type **replmon.exe** and press **Enter**. Replmon will then come up with a fairly blank page, as shown in Figure 5.67.

Figure 5.67 Replmon's Default Screen

Right-click on the **Monitored Servers** icon in the upper left. You now have the option to **Add Monitored Server**. In the **Add Monitored Server Wizard** you have the choice to explicitly type in the name of the DC you want to add or enter a name of a domain within the forest from which to read site data. Figure 5.68 shows that we have decided to search the directory for a server and that our domain is MMA.LOCAL. Once you've done this select **Next**.

Figure 5.68 The Add Monitored Server Wizard

At the next screen, you see a list of sites that are available from Active Directory. You can expand a site and select any particular server located there. In Figure 5.69, you see that we have chosen to monitor a DC out of the South-Region called FMEA. Once you've done this you can click **Finish**.

Figure 5.69 Selecting a DC to Monitor

In Figure 5.70, you see that the DC we’re monitoring has five directory partitions displayed. Underneath each partition you see this DC’s replication partner. In this case, it is a DC called SIGMA. Normally, if there are any replication issues you will see a red X underneath the partition(s) where the problem exists. In Figure 5.71, we show the replication status of the Schema and the Update Sequence Number (USN).

Figure 5.70 Directory Partitions

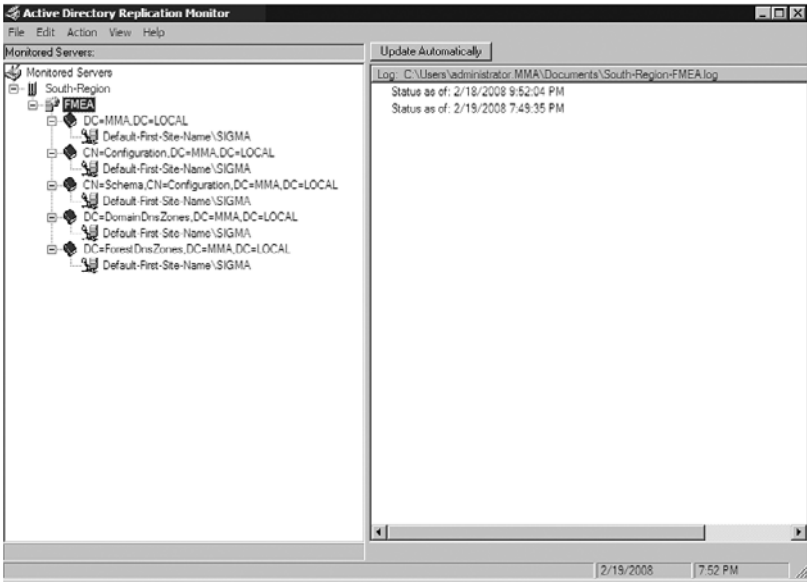
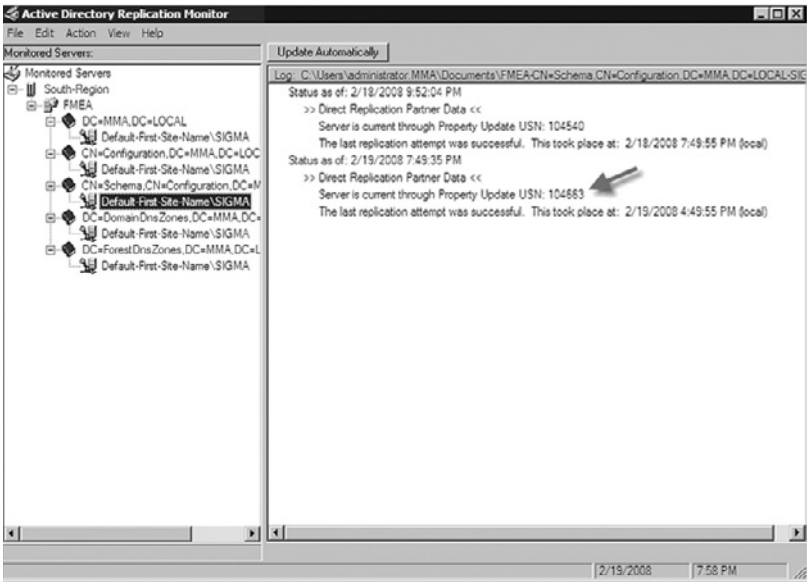


Figure 5.71 Viewing the Logs Pane in Replmon



If you right-click the server, you will see a list of options you have in replmon, as shown in Figure 5.72.

Figure 5.72 Replmon Options



Table 5.4 lists the options and their descriptions.

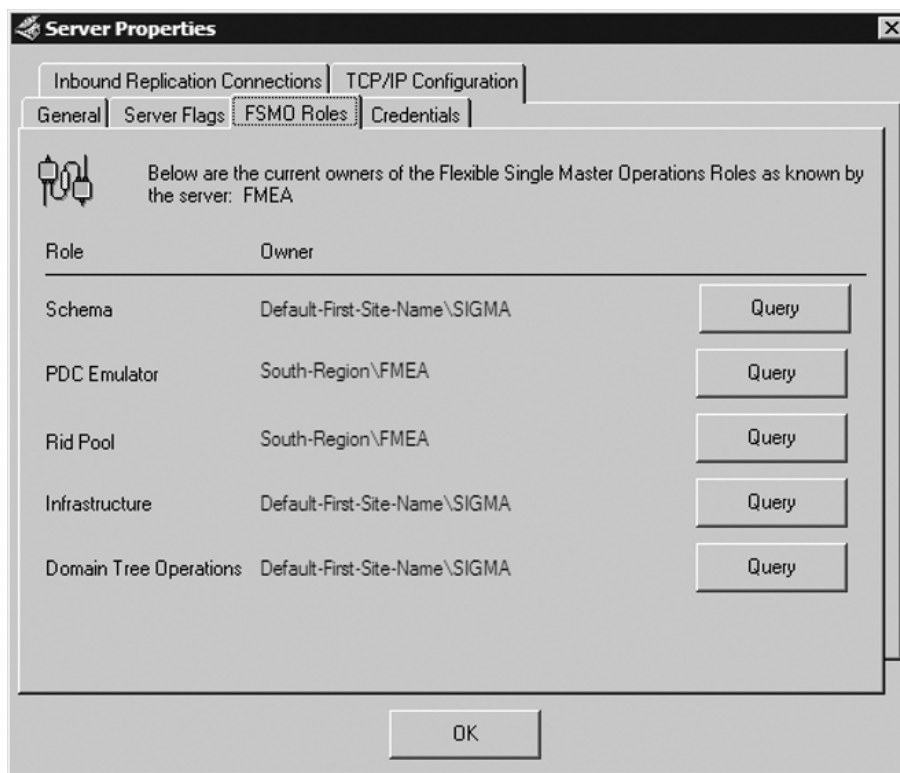
Table 5.4 Replmon Options Described

Option	Description
Update Status (only for this server)	Rechecks the replication status of the server. The time of the updated status is logged and displayed.
Check Replication Topology	Causes the KCC to recalculate the replication topology for the server
Synchronize Each Directory Partition with All Servers	Starts an immediate replication for all of the server's directory partitions with each replication partner
Show Domain Controllers in Domain	Lists all known DCs

Continued

Table 5.4 Continued. Replmon Options Described

Option	Description
Show Replication Topologies	Shows a graphical view of the replication topology
Show Group Policy Object Status	Lists all the Domain's Group Policies and their respective Active Directory and SYSVOL version numbers
Show Global Catalog Servers in Enterprise	Lists all Global Catalog servers
Show Bridgehead Servers	Two options are available: In This Server's Site and In the Enterprise. Will show bridgehead servers based on information provided by the monitored DC.
Show Trust Relationships	Will show all trusts with this domain
Show Attribute Meta-Data for Active Directory Object	Shows attribute data for a particular object specified using that object's distinguished name (DN)
Clear Log	Clears the <site-dcname>.log file
Delete	Deletes the DC from the monitored servers list
Properties	Shows server properties of the monitored DC. Provides information such as Flexible Single Manager Operation (FSMO) roles for the domain (shown in Figure 5.73), inbound replication connections, Transmission Control Protocol/Internet Protocol (TCP/IP) configuration, server flags, and other general information.

Figure 5.73 The FSMO Roles Tab in Server Properties

Replmon is a very useful and powerful tool in troubleshooting replication issues and for just finding information about a domain.

Head of the Class...

Support Tools

After installing Windows Server 2008, it is highly recommended that you install the support tools that reside on the installation media, allowing you immediate access to tools such as replmon.

RepAdmin

Another tool that comes with the installation of Windows Server 2008 is the command-line tool **RepAdmin**. Administrators can use RepAdmin to view replication topology, create replication topology, and force replication, whether it is for the entire directory or for specific portions of it. You also can use RepAdmin for monitoring an Active Directory forest. You must run the RepAdmin command in an elevated prompt, either by right-clicking the **Command Prompt** and then clicking **Run as administrator** or simply by logging on as an administrator and running it. You must also have administrative rights on every DC that RepAdmin targets. For instance, Domain Admins can run RepAdmin on any DC in the domain. Enterprise Admins can run RepAdmin on any DC in the forest. Here is the syntax for RepAdmin; Table 5.5 lists the commands:

```
Repadmin <cmd> <args> [/u: {domain\user}] [/pw:{password | *}] [/retry  
[:<retries>] [:<delay>]] [/csv]
```

Table 5.5 RepAdmin Commands

Command/Parameters	Description
<i>Repadmin /kcc</i>	Forces the KCC to immediately recalculate the inbound replication topology from the targeted DCs. Example: <i>repadmin /kcc site:south</i> The preceding command triggers the KCC to run on each DC in the south site.
<i>Repadmin /prp</i>	Specifies the Password Replication Policy (PRP) for read-only DCs (RODCs). Example: <i>repadmin /prp view SIGMA reveal</i> The preceding command lists the users whose passwords are currently cached on the DC named SIGMA.
<i>Repadmin /queue</i>	Shows the inbound replication requests that the DC must issue to become consistent with its source replication partners. Example: <i>repadmin /queue FMEA</i> The preceding command returns the queue of inbound replication requests that a bridgehead server named FMEA has yet to process.

Continued

Table 5.5 Continued. RepAdmin Commands

Command/Parameters	Description
<i>Repadmin /replicate</i>	<p>Triggers immediate replication of the specified directory partition to a target DC from a source DC.</p> <p>Example: <i>repadmin /replicate SIGMA FMEA DC=MMA, DC=com</i></p> <p>The preceding command replicates the MMA naming context from the SIGMA DC to the FMEA DC.</p>
<i>Repadmin /replsingleobj</i>	<p>Replicates a single object between two DCs that share common directory partitions.</p> <p>Example: <i>repadmin /replsingleobj SIGMA FMEA cn=swhitley, ou=sales, dc=MMA, dc=com</i></p> <p>The preceding command triggers replication of the <i>swhitley</i> object from the SIGMA DC to the FMEA DC.</p>
<i>Repadmin /replsummary</i>	<p>Identifies DCs that are failing inbound replication or outbound replication and summarizes the results in a report.</p> <p>Example: <i>repadmin /replsum * /bysrc /bydest /sort:delta</i></p> <p>The preceding command targets all DCs in the forest to retrieve summary replication status from each.</p>
<i>Repadmin /rodcpwdrepl</i>	<p>Triggers the replication of passwords for the specified users from the source DC to one or more RODCs.</p> <p>Example: <i>repadmin /rodcpwdrepl dest-rodcc* source-dc cn=swhitley, ou=sales, dc=MMA, dc=com</i></p> <p>The preceding command triggers replication of the passwords for the user <i>swhitley</i> from the source DC named <i>source-dc</i> to all RODCs that have the name prefix <i>dest-rodcc</i>.</p>
<i>Repadmin /showattr</i>	<p>Displays the attributes of an object</p> <p>Example: <i>repadmin /showattr SIGMA "cn=accountants, cn=users, dc=MMA, dc=com"</i></p>

Continued

Table 5.5 Continued. RepAdmin Commands

Command/Parameters	Description
	The preceding command queries the SIGMA DC and shows all attributes for the above object using its DN.
<i>Repadmin /showobjmeta</i>	<p>Displays the replication metadata for a specified object in Active Directory Domain Services. It can be an attribute ID, version number, originating and local USNs, the GUID of the originating server, and even a date and timestamp</p> <p>Example: <i>repadmin /showobjmeta SIGMA "<GUID=6f3427ba-g25c-5e85-c129-125bbc897d23>"</i></p> <p>The preceding command targets the SIGMA DC and requests the replication metadata for an object by specifying its GUID.</p>
<i>Repadmin /showrepl</i>	<p>Displays the replication status when the specified DC last attempted to perform inbound replication on Active Directory partitions.</p> <p>Example: <i>repadmin /showrepl * /errorsonly</i></p> <p>The preceding command reports inbound replication status for all DCs in the forest that are experiencing a replication error.</p>
<i>Repadmin /showutdvec</i>	<p>Displays the highest committed USN that Active Directory Domain Services, on the targeted DC, shows as committed for itself and its transitive partners.</p> <p>Example: <i>repadmin /showutdvec dc=MMA, dc=com</i></p> <p>The preceding command shows the highest committed USN on the local DC for the MMA.com directory partition.</p>
<i>Repadmin /syncall</i>	Synchronizes a specified DC with all replication partners.

Continued

Table 5.5 Continued. RepAdmin Commands

Command/Parameters	Description
	Example: <i>repadmin /syncall FMEA dc=MMA, dc=com /d /e /a</i> The preceding command synchronizes the target DC with all its partners, including DCs at other sites.

Windows System Resource Manager

Sometimes an application, process, or service will take up a majority of the CPU cycles to the point that it affects everything else running on the server. To combat that Microsoft has provided a feature in Windows Server 2008 called Windows System Resource Manager (WSRM). WSRM provides an interface where administrators can configure how both processor and memory resources are allocated among applications, services, and processes. The ability to do this allows administrators to ensure server stability. To install WSRM do the following:

1. Log on to a Windows Server 2008 system and launch **Server Manager**.
2. In **Server Manager**, click **Features** in the console pane on the left side and choose **Add Features** in the **Details** pane.
3. Next, the **Select Features** box opens. Scroll down to **Windows System Resource Manager** and select it. Then click **Next**.
4. At the **Confirm Installation Selections** screen, verify the feature you are installing and then click **Install**.
5. After the installation is finished, just click **Close** and you're done.

WSRM uses resource allocation policies to allocate CPU time and memory usage among applications, services, processes, and even users. These resource allocation policies can be in effect all the time or you can run them on a scheduled basis. WSRM policies, though, are enforced only when CPU usage goes above 70% and are never active on processes owned by the operating system or items in the exclusion list.

If and when certain events take place or the system behaves differently, WSRM can switch to a different policy and ensure system stability. If accounting is enabled in WSRM, administrators of the servers can examine the data collected and determine when and why resource allocation policies were either too restrictive

or too lax. Administrators can adjust resource allocation policies using the information obtained by accounting.

There are four predefined resource allocation policies with WSRM in Windows Server 2008. These predefined policies make it easy for administrators to quickly allocate resources. Table 5.6 shows the predefined resource allocation policies.

Table 5.6 WSRM Predefined Policies

Policy	Description
Equal per Process	Resources are equally allocated among all running processes, thus preventing one process from monopolizing all available CPU and memory resources.
Equal per User	Resources are equally allocated among all users, thus preventing one user from monopolizing all available CPU and memory resources.
Equal per Session	Resources are equally allocated among all Terminal Services sessions, thus preventing one session from monopolizing all available CPU and memory resources.
Equal per IIS Application Pool	Resources are allocated equally among all IIS application pools, thus preventing one application pool from monopolizing all available CPU and memory resources.

Matching criteria is a common task performed with WSRM. Administrators use these rules to include or exclude processes, services, or applications that WSRM needs to monitor. These rules are used later in the WSRM management process.

Custom resource allocation policies are similar to matching criteria rules in that they look for specific processes, services, and application criteria. The custom resource allocation policy provides an administrator with the ability to define how much of a resource should be allocated to a specific process, service, or application. For instance, if only 15% of the system processing should be reserved to the sqlwriter.exe process, the resource allocation would be defined to limit the allocation of resources to that process.

The calendar in WSRM is used to schedule policy enforcement on a set basis by one time event or recurring event(s). It's possible, for instance, that policy enforcement may be necessary only during business hours.

Administrators can allocate system resources to sessions or users who are active on Terminal Services. Configuring a policy can ensure that the sessions will behave correctly and that system availability will be stable for all users of Terminal Services. You can do this using the Equal per User or Equal per Session policy within WSRM.

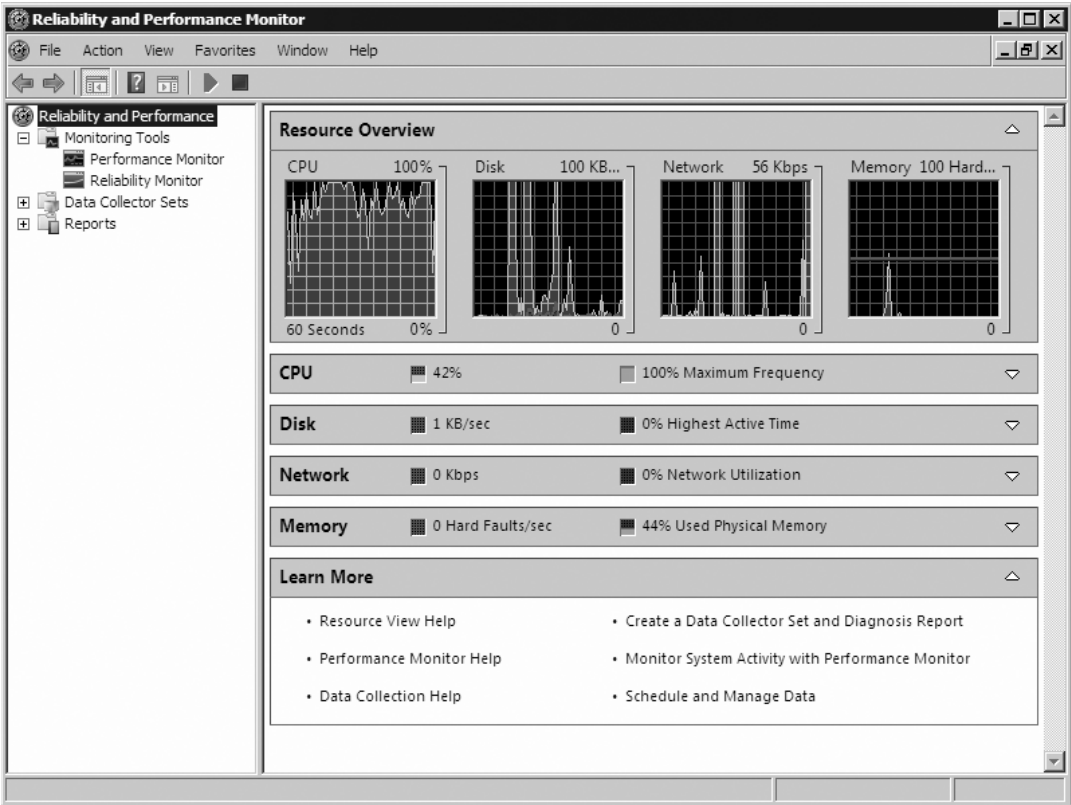
The Windows Reliability and Performance Monitor

The Windows Reliability and Performance Monitor allows administrators to monitor application and hardware performance in real time and customize data they want to collect in logs, predefined thresholds for alerts, and automatic actions. Administrators can generate reports and view past performance data in a variety of ways. The Windows Reliability and Performance Monitor is a combination of previous tools such as Performance Logs and Alerts, Server Performance Advisor, and System Monitor. It provides a graphical interface for the customization of Data Collector Sets and Event Trace Sessions. The Windows Reliability and Performance Monitor consists of three monitoring tools:

- Resource Overview
- Performance Monitor
- Reliability Monitor

There are two ways to start the Windows Reliability and Performance Monitor. One way is to click **Start | Administrative Tools | Reliability and Performance Monitor**; the other is to simply click **Start | Run**, type **perfmon**, and then press **Enter**. Figure 5.74 is a view of the Windows Reliability and Performance Monitor console.

Figure 5.74 The Windows Reliability and Performance Monitor



Resource Overview

The Resource Overview screen is also known as the Home Page in the Details pane. The Resource Overview screen presents data about the system in a real-time graphical manner. You see similar categories as those you saw in the Task Manager: CPU, Network, Memory, and Disk (the latter which is not shown in the Task Manager).

You can expand the subsections by clicking on the white down arrow to the far right of the bar. When you do you will see additional, more detailed information. For instance, if you expand CPU, you will see information such as the image, PID, description, threads, CPU, and average CPU. Table 5.7 lists the subsections and their associated headings.

Table 5.7 Subsections and Headings

Subsection	Headings
CPU	Image, PID, Description, Threads, CPU, Average CPU
Disk	Image, PID, File, Read, Write, IO Priority, Response Time
Network	Image, PID, Address, Send, Receive, Total
Memory	Image, PID, Hard Faults, Commit, Working Set, Shareable, Private

The Performance Monitor

Under Monitoring Tools is the Performance Monitor, which provides a display of built-in performance counters, in real time or viewed as historical data. The Performance Monitor allows administrators the ability to analyze system data, research performance, and bottlenecks. To open the Performance Monitor you can click on it underneath Monitoring Tools. The Performance Monitor is just like the System Monitor before it. The System Monitor in Windows Server 2003 allowed you to measure the performance of your own system or that of other Windows systems on the network. It allowed you to collect and view real-time performance data. With the Performance Monitor in Windows Server 2008, you have objects, counters, and instances. Table 5.8 provides a quick description of each.

Table 5.8 Components of the Performance Monitor

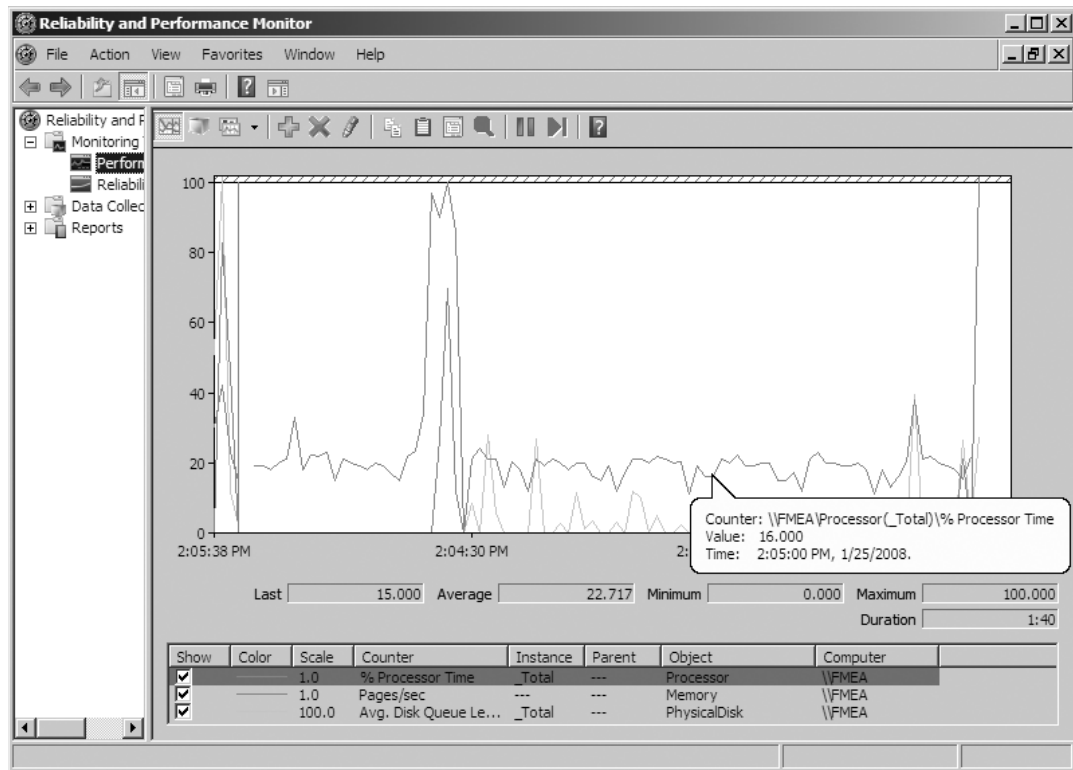
Component	Description
Object	System components are grouped into objects. They are grouped according to system functionality. Depending on the configuration, the number of objects depends on the system.
Counter	Provides a subset of objects. Also provides more detailed information about an object. Examples are queue length, session % used, and pages converted.
Instances	If more than one similar object is on a server, each one is considered an instance. Servers with multiple processors have an instance for each.

Exercise 5.15 takes you through the steps of counters in the Performance Monitor.

EXERCISE 5.15

ADDING COUNTERS IN THE PERFORMANCE MONITOR

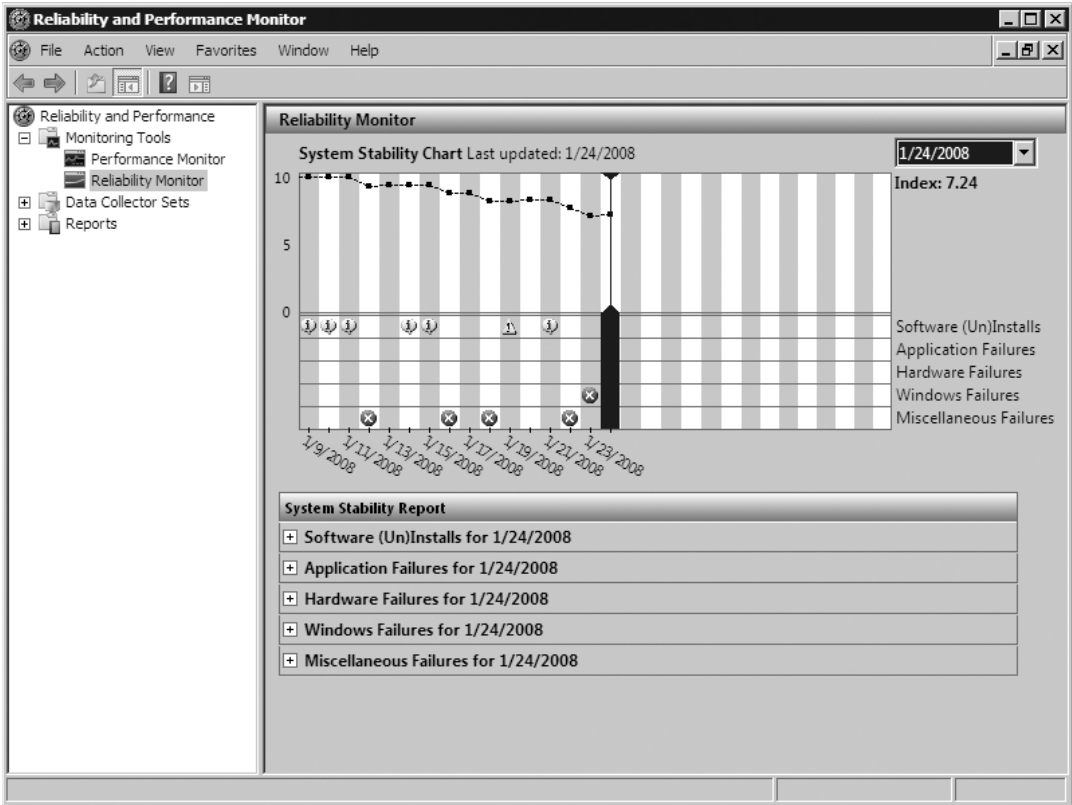
1. Open **Reliability and Performance Monitor** either by clicking **Start | Administrative Tools | Reliability and Performance Monitor** or **Start | Run**. Type **perfmon** and press **Enter**.
2. In the console tree, click **Monitoring Tools | Performance Monitor**. This will open the Performance Monitor.
3. Click the green plus sign in the Details pane and the **Add Counters** screen should come up and start loading a list of counters.
4. Now it's time to select the counters. We will be setting up counters to help us set up a baseline for the system. To do that the counters we need are **Memory-Pages/sec**, **Physical Disk-Avg. Disk Queue Length**, and **Processor-%Processor Time**.
5. To add **Memory-Pages/sec**, go down the list of counters and click on **Memory**. Now go down its list and select **Pages/sec** and then click **Add**. Do the same for **Physical Disk-Avg. Disk Queue Length** and **Processor-%Processor Time**. Once you're done adding your counters, click on **OK**. You may get a message letting you know that one of the counters is already present. That is the **%Processor Time**. Just click **OK**.
6. Now you should see the Performance Monitor with the counters you just added, similar to Figure 5.75. Notice that if you highlight any one of the lines on the chart you get the value at that point in time.

Figure 5.75 The Performance Monitor with Baseline Counters

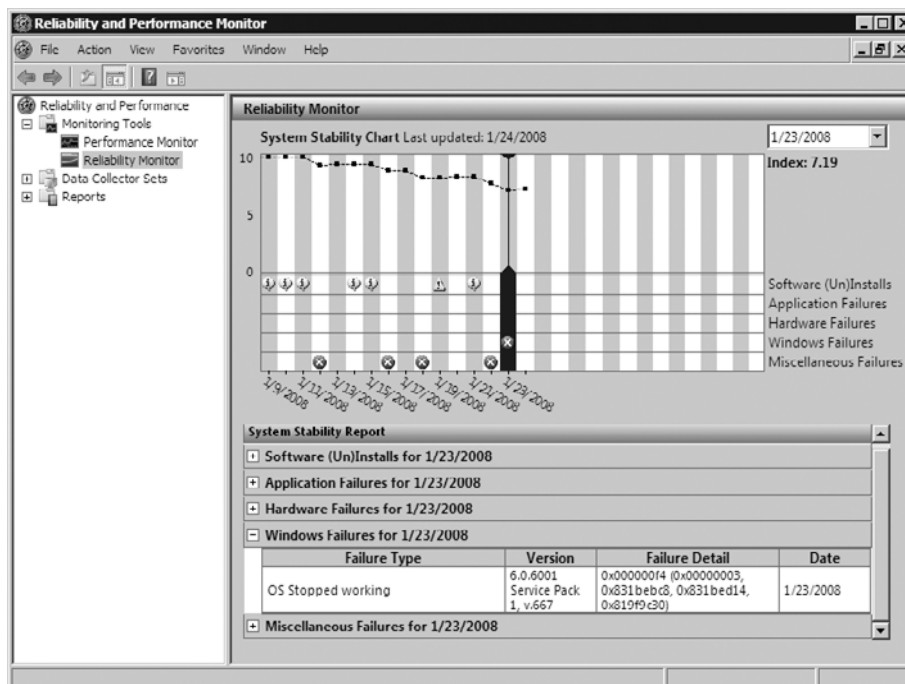
The Reliability Monitor

The Reliability Monitor provides a system stability overview and information about events that impact reliability. It is great for troubleshooting the root cause associated with any reduced reliability of the system. For instance, we may have a server that is slow to perform read and write requests. By using the Reliability Monitor, we can examine the server's trend over a period of time and examine failure types with details. The Reliability Monitor calculates the Stability Index which is shown in the System Stability Chart, and helps in diagnosing items that might be impacting the system. An index of 1 means the system is in its least stable stage, whereas an index rating of 10 indicates the system is at its most stable state. The index number is derived from the number of specified failures seen over a historical period. Figure 5.76 shows the System Stability Chart of the server called SIGMA.

Figure 5.76 The System Stability Chart



Notice that this server’s Index seems to have headed toward a downward slope. The current index is 7.24; although it is not the worst it could be, there are obviously some problems that need to be addressed. When you examine any of the System Stability Reports below the chart, you see information such as Failure Type, Version, Failure Detail, and Date. In Figure 5.77, we have opened the latest error that took place; the failure type is “OS Stopped working” and the failure detail is a group of hex values.

Figure 5.77 A Windows Failure in the System Stability Report

The failure detail here is one that is shown in a “blue screen” crash. The next thing this administrator should do is look for a file named `memory.dmp` and then contact Microsoft Product Support Services to have the file examined.

Data Collector Sets

A Data Collector Set organizes multiple data collection points into a single component that you can use to review or log performance. It can be created and then recorded separately, grouped with other sets, and incorporated into logs. Data Collector Sets can contain the following types of data collectors: performance counters, event trace data, and system configuration information. There are two types of Data Collector Sets: User Defined and System. User Defined are customized by the user/administrator whereas System Collector Data Sets are predefined and are broken down into Active Directory Diagnostics, LAN Diagnostics, System Diagnostics, and System Performance.

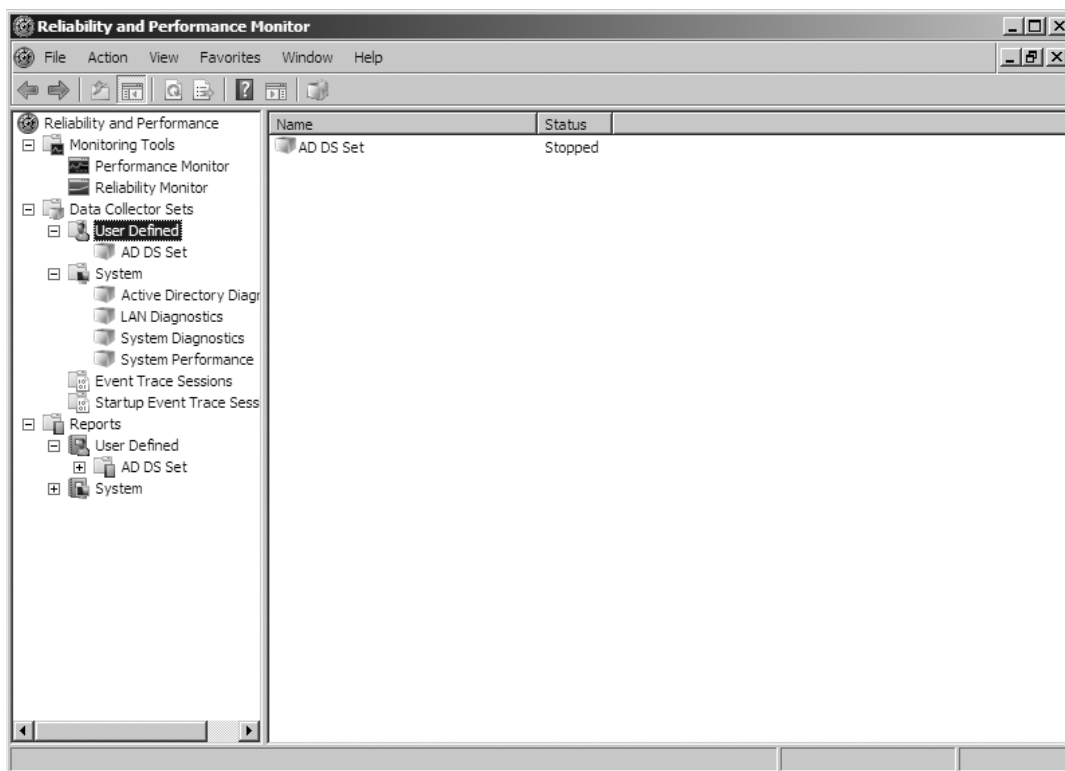
Data Collector Sets can be created from templates, existing sets of data collectors in a Performance Monitor view, or by selecting individual Data

Collectors and setting each individual option in the Data Collector Set properties. Exercise 5.16 walks you through the process of creating a User Defined Data Collector Set.

EXERCISE 5.16

CREATING A USER-DEFINED DATA COLLECTOR SET

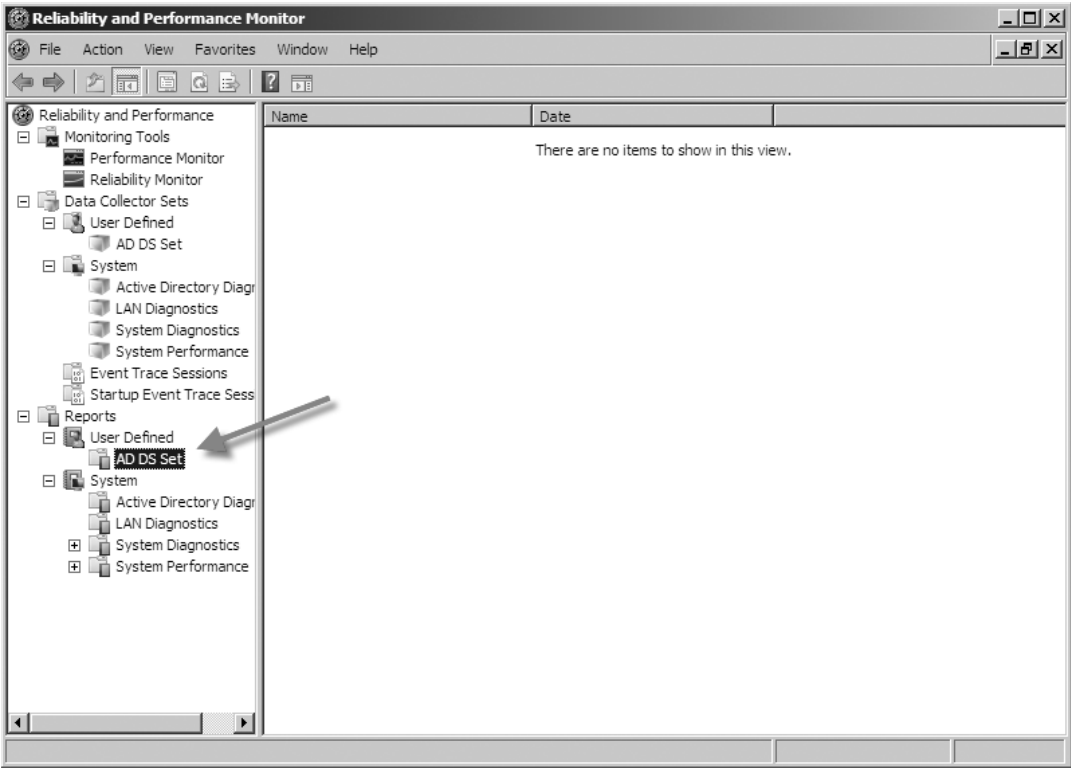
1. First go into the **Reliability and Performance Monitor** as you did in the previous exercise.
2. In the console tree, go to **Data Collector Sets | User Defined**.
3. Right-click on **User Defined** and select **New | Data Collector Set**.
4. At the first **Create a new Data Collector Set** screen type in a descriptive name. For our example, we called ours **AD DS Set**. Select **Create from a template** and press **Next**.
5. In the next screen, you are asked which template you would like to use. Because ours is called AD DS Set, we obviously want to select **Active Directory Diagnostics**, so we'll select that and click **Next**. The Active Directory Diagnostics will collect data on this local server that includes Registry keys, performance counters, and trace events that are helpful in troubleshooting Active Directory Domain Services performance issues.
6. Next we are asked where we would like the data to be saved. Accept the default, which in this case is **%systemdrive%\Perflogs\Admin\AD DS Set**, and then click **Next**.
7. Now we are asked whether we want to create the data collector set. Select the default of **Save and Close** and click **Finish**.
8. Now under **User Defined** beneath **Data Collector Sets**, you should see the newly created Data Collector Set AD DS Set, as shown in Figure 5.78.

Figure 5.78 Newly Created User-Defined Data Collector Set

Reports

The last folder in the Windows Reliability and Performance Monitor is Reports. Reports support administrators who need to troubleshoot and analyze system performance and issues. Reports are based on Data Collector Sets and are also broken down into User Defined and System. Once you've created the Data Collector Set, its corresponding reports folder is available, as shown in Figure 5.79.

Figure 5.79 A User-Defined Report Automatically Created



Summary of Exam Objectives

Maintaining an Active Directory environment constitutes 13% of the total exam for 70–640. It covers areas concerning backup and recovery, offline maintenance, and monitoring Active Directory. With the release of Windows Vista, backup and recovery have changed since Windows 2003 and those changes are further evident in Windows Server 2008. No longer is backup performed using `ntbackup.exe`, but rather through the Windows Server Backup interface or by using the `wbadmin` command-line tool. One of the changes in the new backup is DVD support. Also, after the first full backup all future jobs automatically run incremental backups by default. You can back up to removable media such as DVD only via the command prompt and not through the GUI. Restoration is also simplified in that administrators no longer have to restore from a multitude of media if the backup was done via an incremental backup. One thing that is no longer supported is the ability to back up to tape. Microsoft has removed this capability.

You install Windows Backup in Server 2008 via Server Manager and adding it as a feature. The command-line tools are not installed by default, so you must select them and they must be accompanied by the installation of the Windows PowerShell. Windows Server Backup is more conducive for personnel not heavily savvy in Windows or IT as a whole. The interface is easy to navigate and creating jobs is wizard-based. Specific backups such as only including the system state must be done via the `wbadmin` command. Full backups scheduled through the GUI do include the system state, but restoring just the system state is only done via the command line, and on a DC the administrator must be in DSRM.

DSRM is a special boot mode in Windows Server 2008. If the Active Directory database file (`ntds.dit`) becomes corrupt, for instance, it is through DSRM that an administrator can restore an uncorrupted version. You can access DSRM via the boot process before loading Windows and just after the BIOS POST. To enter DSRM, you must press F8 during the boot-up procedure and choose Directory Services Restore Mode from the list of options. It is in DSRM that authoritative and nonauthoritative restores are done.

Just as in previous versions of Windows Server, both authoritative and nonauthoritative restores are supported. In the case mentioned earlier regarding a corruption in `ntds.dit`, an administrator would perform a nonauthoritative restore of `ntds.dit` and any discrepancies between the restored copy and those residing on the other DCs in the domain would be updated or removed via the replication process. In some situations, though—for instance, accidentally removing an object such as a user account in Active Directory—performing a nonauthoritative restore

will do nothing to bring back the previously deleted object. This is where performing an authoritative restore is required. An authoritative restore is performed in DSRM and the object being restored is restored at the authoritative restore prompt. After an authoritative restore, the object is then replicated back to all the DCs in the domain.

Linked Value Replication is performed when the forest level is at a Windows Server 2003 level or above. LVR replicates individual values of an object—not the entire object or an entire attribute, but just the value that has changed—thus reducing the amount of bandwidth consumed during replication.

Backing up a Group Policy Object consists of making a copy of the GPO data to the file system. Backups and restores are performed within the Group Policy Management Console. Another type of GPO that can be backed up is the Starter GPO. These GPOs are not included in the backup of regular GPOs and must be specifically backed up within the GPMC.

Offline maintenance has changed under Windows Server 2008. No longer do tasks such as defragging and compacting require booting into DSRM; with the advent of Restartable Active Directory end-user productivity is less affected than before. Restartable Active Directory runs as a service known as Active Directory Domain Service and is seen in the Services console in Windows Server 2008. Services such as DHCP and file/print are unaffected by stopping the Active Directory Domain Service. Stopping the Active Directory Domain Service, though, will stop services such as the Kerberos Key Distribution Center (KDC), intersite messaging, DNS server, and DFS replication. Restarting the Active Directory Domain Service does restart those services as well. To defrag the *ntds.dit* file just stop the Active Directory Domain Service and run the *ntdsutil* command, activate the *ntds* instance, pull up the File Maintenance prompt, and then type the *compact* command. Once finished, there is no need to reboot the server; just restart the Active Directory Domain Service.

Making sure that objects and attributes are up-to-date and consistent among DCs is a key in monitoring Active Directory. Tools such as the Network Monitor (*netmon*), Event Viewer, Replication Monitor (*replmon*), and Replication Administrator (*repadmin*) are key. Performance of DCs is also of concern and tools such as the Task Manager, Windows System Resource Manager, Windows Reliability and Performance Monitor, and Event Viewer are used to monitor them.

Exam Objectives Fast Track

Backup and Recovery

- ☑ Windows Server 2008 backup uses block-level images and .vhd files.
- ☑ Tape is no longer supported.
- ☑ Windows Server Backup is the new GUI for backup in Windows Server 2008.
- ☑ Backups can be scheduled more than once a day and at specific times.
- ☑ Wbadmin.exe is the new command-line interface for backup.
- ☑ Backup and restore of just the system state must be done using wbadmin.exe.
- ☑ Directory Services Restore Mode (DSRM) is used to perform authoritative and nonauthoritative restores.
- ☑ Authoritative restores should be performed after an object in Active Directory has been accidentally deleted and replication to the other DCs has taken place.
- ☑ Nonauthoritative restores are good for lost updates such as a password for a user account and corruption found in the ntds.dit file.
- ☑ Linked Value Replication (LVR) is used when changes in group membership occur and only the individual member(s) is replicated and not the entire membership group as a whole.
- ☑ GPOs and Startup GPOs are backed up separately.

Offline Maintenance

- ☑ Active Directory Domain Services runs as a service under Windows Server 2008 and can be started and stopped at will but can never be paused.
- ☑ Because of restartable Active Directory Domain Services routine tasks can be performed without affecting other services such as DHCP and file/print services.
- ☑ The three states that a Windows Server 2008 DC runs in are AD DS Started, AD DS Stopped, and Domain Services Restore Mode (DSRM).
- ☑ Offline defrag and compaction shrink the size of ntds.dit, thus saving disk space.

- ☑ If ntds.dit and its logs are located on the same partition, free space should be at least 20% of the combined database file and logs or 1 GB, whichever is greater.

Monitoring Active Directory

- ☑ Tools used to monitor Active Directory are the Network Monitor, Event Viewer, replmon, and repadmin.
- ☑ DC performance and stability are monitored using the Task Manager, Windows System Resource Manager (WSRM), Windows Reliability and Performance Monitor, and Event Viewer.
- ☑ Network Monitor (netmon) Version 3.0 and later are supported on Windows Server 2008 and must be downloaded to install.
- ☑ Netmon is very useful in verifying that traffic is flowing as it's supposed to along with making sure name resolution is occurring correctly.
- ☑ The Task Manager is ideal for immediate viewing of resources being used on a server.
- ☑ The Event Viewer is typically the first place to start troubleshooting anything that has to do with the server or Active Directory.
- ☑ The Event Viewer is now based on XML.
- ☑ Replmon (Replication Monitor) is a GUI tool used to examine replication among DCs and view the replication topology.
- ☑ RepAdmin (Replication Administrator) is a command-line version of Replmon.
- ☑ The Windows System Resource Manager (WSRM) allows an administrator to configure how processor and memory resources are allocated among applications.
- ☑ The Windows Reliability and Performance Monitor allows administrators to monitor application and hardware performance in real time.

Exam Objectives

Frequently Asked Questions

Q: Since Windows Server Backup doesn't read .bkf files, is there any way to restore any information from one in Windows Server 2008?

A: Yes. You can download a version of ntbackup for Windows Server 2008 for the sole purpose of restoring items that were backed up with the old software, but you cannot back up with it. You can download the ntbackup for Windows Server 2008 from <http://go.microsoft.com/fwlink/?LinkId=82917>.

Q: Does Windows Server Backup support tape?

A: No. It supports backing up to disk, removable media such as DVD, and network drives.

Q: Does Windows Server Backup come preinstalled with Windows Server 2008?

A: No. You must add it as a feature.

Q: Can you back up just the system state with Windows Server Backup?

A: No. Windows Server Backup backs up at the volume level and does not include an option for choosing just the system state or a particular directory or file. You can use wbadmin.exe via a command prompt to back up just the system state.

Q: Since Windows Server 2008 supports backing up to DVD, can you also back up to USB-based flash drives as well?

A: Yes. To back up to any removable media such as DVD or USB flash drives, you must do so using the wbadmin.exe command-line tool.

Q: If I forget the Directory Services Restore Mode (DSRM) administrator's password, can I still get in DSRM?

A: No, but if you change the DSRM Administrator's password at the ntdsutil prompt in Windows Server 2008, you can.

Q: What is the difference between an authoritative restore and a nonauthoritative restore?

A: An authoritative restore restores a directory object, such as a user account that may have been deleted accidentally, and flags it so that its restoration is

replicated among the other DCs. A nonauthoritative restore is useful for when the Active Directory database file (ntds.dit) has become corrupt and you need to restore it. After restoration, directory replication brings it up-to-date with all the other DCs.

Q: Does Windows Server Backup back up GPOs?

A: No. You must back up GPOs and Starter GPOs via the Group Policy Management Console (GPMC).

Q: Do you still have to boot into DSRM to perform offline defragging?

A: No. You can simply stop Active Directory Domain Services in the Services console and perform it without going into the DSRM. Functions such as DHCP and file/print are unaffected and are still operational.

Q: Can I monitor Active Directory replication using the Network Monitor (netmon)?

A: You cannot see the actual replication itself, but you can verify that the DCs are talking to each other. A better alternative would be to use either the Replication Monitor (replmon) or Replication Administrator (repadmin).

Q: What are some of the new benefits of the Event Viewer?

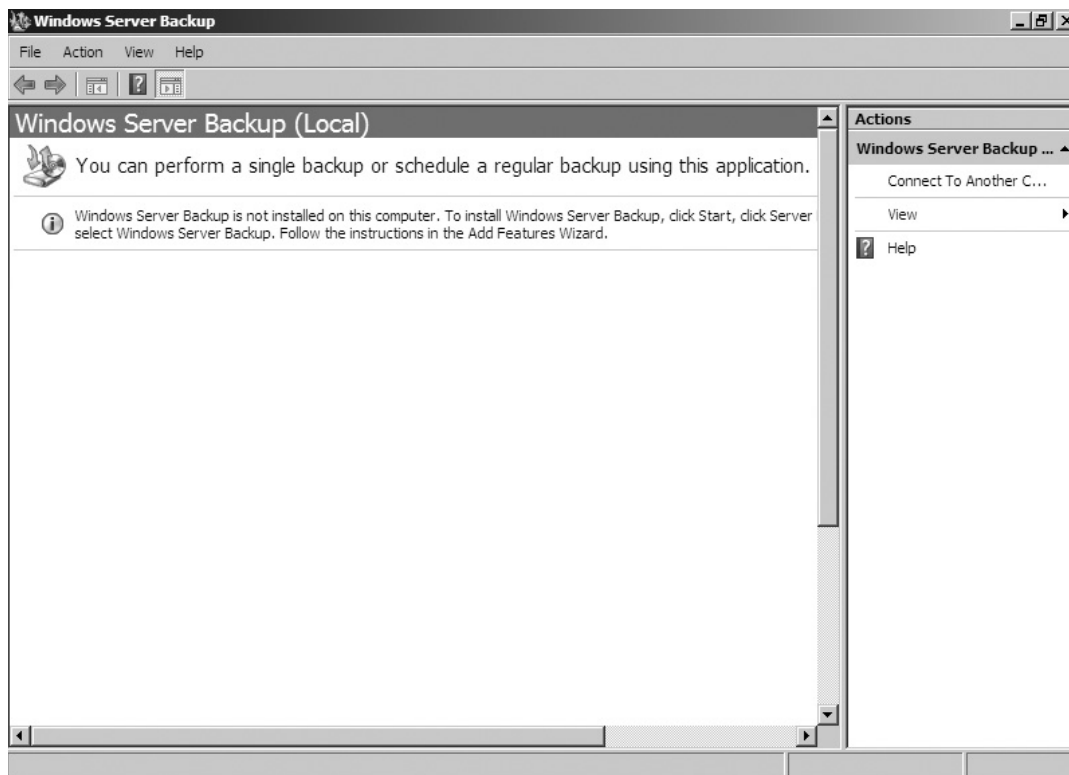
A: The Event Viewer is now XML-based, so it's even easier to import information from it into different applications. You can create subscriptions, which allows remote servers to forward events to a centrally located server so that they can be examined in one place.

Q: What does the Windows Reliability and Performance Monitor actually do?

A: It allows administrators to monitor application and hardware performance in real time as well as customize the data they collect in logs. It's made up of three primary monitoring tools: the Resource Overview, Performance Monitor, and Reliability Monitor. You can customize the data you log by creating Data Collector Sets which you can examine via Reports in the tool.

Self Test

1. You've just finished installing a new Windows Server 2008 DC. It is the policy of the IT department to perform a full backup of newly installed DCs. You click on **Start | Administrative Tools | Windows Server Backup**. When Windows Server Backup loads you see the following screen.



What do you need to do to ensure that the backup takes place?

- A. Run DCPROMO
- B. Install the Windows Server Backup feature
- C. Go to a command prompt and run wbadmin.exe
- D. Boot into DSRM and conduct the backup from there

2. You are responsible for performing backups on the DCs on your network. Your boss has requested that you conduct system state backups to DVD. How do you accomplish this?
 - A. Run the **Windows Server Backup Wizard**, select **System State Backup**, and set your target to the DVD drive
 - B. Run the **Windows Server Backup Wizard**, select a local drive as the target, and then copy the system state backup to the DVD drive
 - C. Run the *wbadmin.exe* command with the *start systemstatebackup* command and target it to the DVD drive
 - D. Run the *wbadmin.exe* command with the *start systemstatebackup* command, set the target to a local fixed drive, and then copy the system state backup to a DVD
3. You are the network administrator for your company. Last night you successfully performed a system state backup of one of your DCs. Do to an unforeseen issue, you now need to perform a system state restore. What do you need to do to conduct a system state restore on a DC?
 - A. Reboot the DC, go into DSRM, and run *wbadmin.exe* to perform the system state restore
 - B. Log on to the DC as usual and run *wbadmin.exe* to restore the system state
 - C. Stop Active Directory Domain Services and then run the *wbadmin.exe* command to restore the system state
 - D. Just restore the system state via the Windows Server Backup Wizard
4. You are the network administrator for your company. You have a scheduled backup job run three times a day: 10:00 A.M., 4:00 P.M., and 11:00 P.M. At 4:50 P.M., you get a call that user Janet Harrell has deleted the company budget on the server. There are no previous versions available. What should you do to restore the company budget?
 - A. Run **ntbackup**, select the company budget from the list of files backed up, and choose **Restore**
 - B. Run **Windows Server Backup**, select **Recover** from the **Actions** pane, choose **Files and Folders** as the recovery type. Select the company budget from the **Available items** list. Choose **Original location** for recovery destination, create copies so that you have both versions of the

file or folder under **When the wizard find files and folders in the recovery destination**, and choose **Restore security settings**.

- C. Go into **DSRM**, run **wbadmin.exe**, and conduct a system state recovery
 - D. Stop Active Directory Domain Services, load ntbackup, select the company budget, and choose Restore
5. You are the network administrator at your company. The Active Directory database file on one of your DCs is corrupt. You decide to perform a non-authoritative restore on the DC. You reboot the server into DSRM and try to log on as the domain administrator but you cannot. You need to get this DC back up and functioning as soon as possible. What can you do to achieve this?
- A. Log on to the server with another domain administrator's account
 - B. Log on to the server using the local administrator's account
 - C. Change the domain administrator's password from another DC and then log on using the account with the new password
 - D. Log on using the DSRM administrator's account and password
6. You are the domain admin for your company. You have tasked Susan, a member of the Account Operators group, to delete Amber Chambers' user account because she quit yesterday. Susan accidentally deletes Andy Chambers' account. Before she realizes what's happened the change is replicated to the other DCs. What can you do to bring back Andy Chambers' user account?
- A. Reboot the DC into DSRM, restore the system state, and conduct a nonauthoritative restore on Andy Chambers' user account from the most recent backup using wbadmin.exe
 - B. Reboot the DC into DSRM, restore the system state, and conduct an authoritative restore on Andy Chambers' user account from the most recent backup using wbadmin.exe
 - C. Log on to the DC in normal mode, stop Active Directory Domain Services, load Windows Server Backup, restore the system state, and perform an authoritative restore of Andy Chambers' user account
 - D. Log on to the DC in normal mode, stop Active Directory Domain Services, load Windows Server Backup, restore the system state, and perform a non-authoritative restore of Andy Chambers' user account
7. You are the domain administrator for your company. Examining one of the DCs, you notice that the file ntds.dit is almost 6 GB in size. You decide that

to save disk space and increase performance you will defrag Active Directory Domain Services. How would you accomplish this?

- A. Log on to the server as an administrator. Perform a system state backup of the DC. Create a new directory on the system drive called C:\defrag. Stop Active Directory Domain Services. Start an instance of ntdsutil and activate Instance ntds. At the ntdsutil prompt pull up the file maintenance prompt and type **compact to c:\defrag**. Go to the %systemdrive%\Windows\NTDS directory and delete the old ntds.dit file as well as any .log files. Copy the ntds.dit file in the C:\defrag folder to %systemroot%\Windows\NTDS, and then restart Active Directory Domain Services.
 - B. Log on to the server as an administrator. Perform a system state backup of the DC. Create a new directory on the system drive called C:\defrag. Start an instance of ntdsutil and activate Instance ntds. At the ntdsutil prompt, pull up the file maintenance prompt and type **compact to c:\defrag**. Go to the %systemdrive%\Windows\NTDS directory and delete the old ntds.dit file as well as any .log files. Copy the ntds.dit file in the C:\defrag folder to the %systemroot%\Windows\NTDS.
 - C. Log on to the server as an administrator in DSRM. Perform a system state backup of the DC. Create a new directory on the system drive called C:\defrag. Stop Active Directory Domain Services. Start an instance of ntdsutil and activate Instance ntds. At the ntdsutil prompt, pull up the file maintenance prompt and type **compact to c:\defrag**. Go to the %systemdrive%\Windows\NTDS directory and delete the old ntds.dit file as well as any .log files. Copy the ntds.dit file in the C:\defrag folder to the %systemroot%\Windows\NTDS, and then restart Active Directory Domain Services.
 - D. Log on to the server as an administrator. Perform a system state backup of the DC. Create a new directory on the system drive called C:\defrag. Stop Active Directory Domain Services. Start an instance of ntdsutil and activate Instance ntds. At the ntdsutil prompt, pull up the file maintenance prompt and type **compact to c:\defrag**. Go to the %systemdrive%\Windows\NTDS directory and delete the old ntds.dit file as well as any .log files. Copy the ntds.dit file in the C:\defrag folder to %systemdrive%\Windows\NTDS.
8. You are the domain administrator for your company. Your network consists of three DCs, each running Windows Server 2008. Two are at site A, and the third

is located at site B. There seems to be a replication problem between the DCs at site A and the DC at site B. What is the best tool to use in troubleshooting directory replication?

- A. Network Monitor
 - B. Task Manager
 - C. RepAdmin
 - D. Event Viewer
9. You are the domain administrator for your company. Your network consists of multiple DCs at multiple sites. A DC at your local site is having problems with replicating. You need to know when this DC last attempted to perform an inbound replication on the Active Directory partitions. How would you accomplish this?
- A. Open a command prompt on the DC and run *ntdsutil*
 - B. Open a command prompt on the DC and run *repadmin /replicate*
 - C. Open a command prompt on the DC and run *repadmin /rodcpwdrepl*
 - D. Open a command prompt on the DC and run *repadmin /showrepl*
10. You are the domain administrator for your company. At your site you have a single DC that also acts as an application server. From 10:00 A.M. to 4:00 P.M., users complain about slow logons to the network and that accessing resources from this DC is incredibly slow during most of the workday. You log on to the DC, pull up the Task Manager, and notice that a process called CustApp.exe is using just more than 90% of the CPU cycles. The application must remain running during the day, but you also need to resolve the slow logon issues. There is no money in the budget for additional hardware. What is the best way to handle this situation?
- A. Go into the Windows System Resource Manager on the DC, and create a new recurring calendar event to start at 8:00 A.M. and end at 5:00 P.M. daily. Associate the event with the Equal_Per_Process policy.
 - B. Go into the Task Manager and into the Processes tab. Find CustApp.exe and set the priority to Below Normal.
 - C. Go into the Task Manager and into the Process tab. Find CustApp.exe and end the process.
 - D. Purchase a second server to run only the CustApp.exe application

Self Test Quick Answer Key

- | | |
|------|-------|
| 1. B | 6. B |
| 2. D | 7. A |
| 3. A | 8. C |
| 4. B | 9. D |
| 5. D | 10. A |