

8

Backing Up and Recovering Your Server

IN THIS CHAPTER, YOU WILL LEARN TO:

- ▶ **UNDERSTAND BACKUP AND RECOVERY (Pages 254–262)**
 - Understand Backup and Recovery Terminology (Page 255)
 - Use Backup and Recovery Tools (Page 256)
- ▶ **MANAGE BACKUP AND RECOVERY (Pages 263–286)**
 - Back Up Your Server (Page 263)
 - Recover Your Data (Page 274)
 - Recover via Shadow Copy (Page 285)
- ▶ **PERFORM BACKUP AND RECOVERY WITH COMMAND TOOLS (Pages 287–292)**
 - Use wbadmin.exe (Page 287)
 - Use PowerShell (Page 290)

Accidents happen. There are many scenarios in which data can get lost, deleted, infected, or corrupted—from a user accidentally deleting a file to a hard drive failing to an operating system failing to a full disaster scenario during which Mother Nature decides to go after your data. It is time for you to shine as the hero for your data and bring it back!

One of the most important tasks you need to perform as an administrator is backing up your server. Performing regular backups on your server is a necessity to help protect you from any number of potential problems. Backups can save you time and money, and, more important, they allow you to sleep well at night. If you have performed proper backups and are proficient in the proper procedures to restore your data, you can quickly identify the proper backup media to begin recovering the data. No one wants to spend thousands of dollars to pay a recovery company to bring back data that you could retrieve yourself with the proper safety measures in place.

Backing up your data is just one part of the process. Learning recovery techniques is just as important. Understanding recovery techniques goes hand in hand with understanding backup solutions. Also, in certain situations you may be able to enable your users to help recover their own lost data. If you know your backup procedures backward and forward, this will allow you to get your recovery operation underway quickly and properly.

Knowing the terminology and when and where to perform backups will allow you to perform the task of backing up and recovering your data efficiently and effectively. This will also allow you to establish proper policies and procedures to gain consistency in protecting your organization. In this chapter, you will learn the tools and terminology behind performing backups and recovery.

Understand Backup and Recovery

In this section, you will learn the terminology behind backup and recovery, as well as the many tools at your disposal to perform the tasks necessary to protect your data. The tools you will see in this chapter are all built in to your Windows Server 2008 R2 server, so they will incur you no additional costs. In fact, not having your data protected using these simple tools can definitely have some cost consequences.

In Windows Server 2008 R2, Microsoft has made several improvements to the backup tool. You now have the ability to back up specific files and folders. In Windows Server 2008 RTM, you had to back up an entire volume. In Windows Server 2008 R2, you can include or exclude folders or individual files. You can also exclude files based on the file types, and you can perform incremental backups of system state. Previously, you could only perform a full backup of the system state by using the `wbadmin.exe` utility. Now you can perform incremental backups of the system state by using the Windows Server Backup utility, the `wbadmin.exe` utility, or a PowerShell cmdlet. You can also perform scheduled backups to volumes or network shares. Lastly, Windows Server 2008 R2 has built-in PowerShell cmdlets for managing backups and restores.

Understand Backup and Recovery Terminology

When working with backup and recovery technologies in Windows Server 2008 R2 or any Windows environment, it is necessary to learn the lingo used by the operating system. Table 8.1 defines some of the key terms you will see used throughout this chapter.

Table 8.1: Backup Terms

Term	Definition
Normal or full backup	Normal backups, sometimes known as full backups, are the slowest for the backup process to complete. The time your backup will take is determined by how much data you are backing up. However, if you can perform a normal backup every night and have it completed during off-hours, this is the preferred way to protect your system. This is also the default setting for Windows Server Backup.
Incremental backup	Incremental backups are the fastest backup process because this type of backup tracks only the changes to your data since the last backup of any kind. Incremental backups will also control how your restore process will work. When you want to restore data with incremental backups, you first need to restore the latest normal backup followed by all the incremental backup sets in order. This method may also impact your servers' performance.

Table 8.1: Backup Terms (*continued*)

Term	Definition
System state	System state contains most of the system's configuration information. It does not contain all the needed configuration for your system; you should always consider using this in conjunction with a full backup. Also, the roles you currently have installed on the server will determine what components make up the system state. See the "Perform a System State Backup" section to see what is backed up.
Bare-metal recovery	A bare-metal recovery allows you to recover a full server environment based on a backed-up image you had created previously (without first installing an OS). This allows you to recover a server that may otherwise have been inoperable because of any number of errors that a regular backup and recovery could not fix. Bare-metal recovery is one of your last lines of recovery to bring back a failed system.
Shadow copies	Shadow copies are point-in-time copies of data typically located on file shares. A shadow copy provides your users with a self-service method of recovering files they have deleted or overwritten accidentally.
Volume Shadow Copy Service (VSS)	VSS is the master service inside Windows Server 2008 R2 governing the majority of the backup infrastructure. It is also the service providing you with the ability to create shadow copies.

Use Backup and Recovery Tools

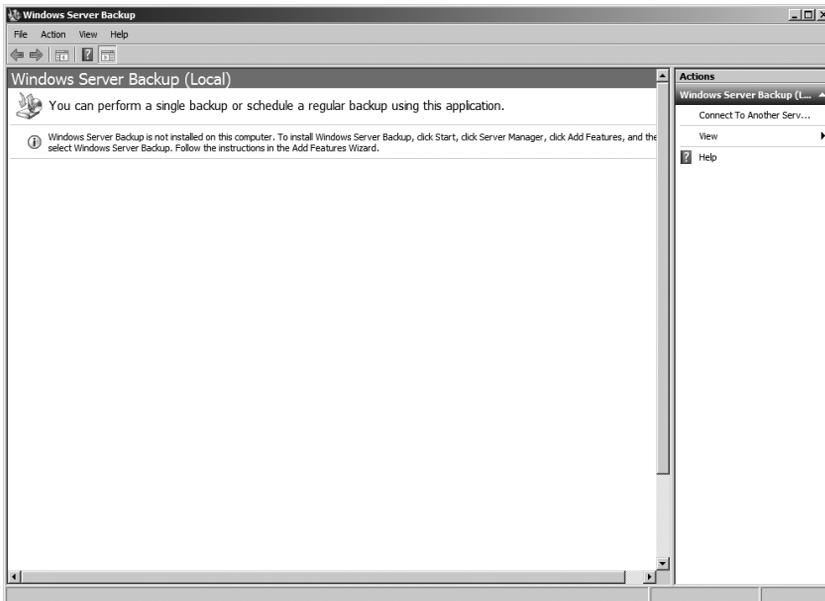
Three tools allow you to access the backup and recovery tool set in Windows Server 2008 R2. You have a fully functioning GUI management tool called Windows Server Backup, you have a command-line tool called `wbadmin.exe`, and lastly you have PowerShell cmdlets at your disposal to perform these commands. On a Windows Server 2008 R2 Server Core installation, you only have `wbadmin.exe` and PowerShell cmdlets to back up a Server Core installation.

In addition to these tools, another valuable tool you can leverage to help protect data located in the file shares is Volume Shadow Copy Service. This tool creates point-in-time backup copies of your file on shared resources. This powerful utility gives your users the ability to protect themselves from accidentally deleting or overwriting files and even allows them to compare versions of a file.

Install Windows Server Backup Tools on a Full Server

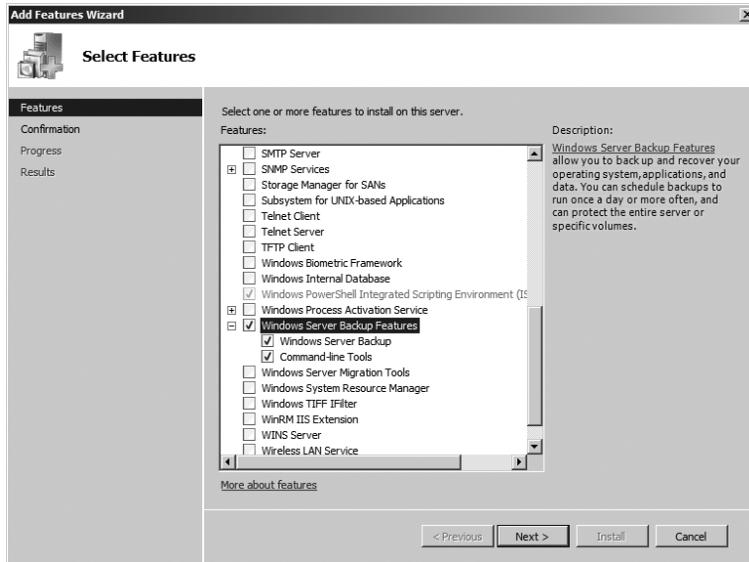
Before you can use any of these tools, you need to first install the tools on their respective server environments. Even though you will see the Windows Server Backup utility in the administrative tools on your Windows Server 2008 R2 server, the feature is not installed by default, and you will see a message similar to Figure 8.1 when you first try to run it.

Figure 8.1: Windows Server Backup message



To install the tools, you just need to install the built-in Windows Server 2008 R2 feature:

1. Open Server Manager.
2. Click Features in the tree menu on the left.
3. Click Add Features in the details pane on the right to begin the installation.
4. Scroll down the feature list to find Windows Server Backup Features. Click the + sign next to the feature name. You will see you have two options to install, as shown in Figure 8.2.

Figure 8.2: Installing Windows Server Backup

The Windows Server Backup choice installs the GUI management tool for your backup administration, and the Command-Line Tools option installs the `wbadmin.exe` command-line tool and the PowerShell cmdlets.

5. Select the management tools you want to install, and click Next.
6. Review the Confirm Installation Selections screen, and when ready, click Install to install the backup tools.
7. After the installation completes, click Close to use the tools.

Install Windows Server Backup Tools on Core Server

Windows Server Core has the same built-in backup tools and functionality as a full Windows Server 2008 R2 server installation. Because of the nature of the Server Core installation, there is no GUI tool; however, you can install either the `wbadmin.exe` command-line tool or the PowerShell backup cmdlets. Just like the Windows Server 2008 R2 full installation, the backup tools are not installed by default.

1. Log on your Server Core server.
2. Type the following command and hit Enter to see the current state of the backup tools (as well as other features installed on Server Core):

```
dism /online /get-features
```

You are looking for the two features called `WindowsServerBackup` and `WindowsServerBackupCommandlet`, and by default the current state for both will be `Disabled`.

3. Type in one or both of the following commands to install the backup tools on the Server Core server.

To install the `wbadmin.exe` tool, type the following command, and hit Enter:

```
dism /online /enable-feature
/featurename:WindowsServerBackup
```

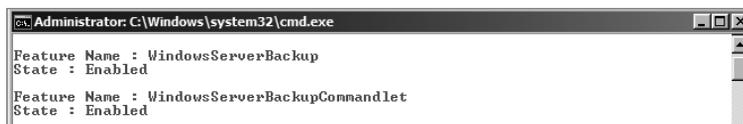
Make sure you have enabled PowerShell on your Windows Server 2008 R2 server before you install the backup cmdlets. To install the PowerShell commands for backup, type the following command, and hit Enter:

```
dism /online /enable-feature
/featurename:WindowsServerBackupCommandlet
```

4. To verify the tools installed properly, you can run the following command and hit Enter. You will see the current state of your backup tools as `Enabled`, and you will see a screen similar to Figure 8.3.

```
dism /online /get-features
```

Figure 8.3: Server Core backup tools enabled



Enable Shadow Copies

Shadow copies help protect data located in the file shares and drives of your Windows Server 2008 R2 server. Shadow copies are point-in-time backup copies of your files on shared resources. They're enabled at the volume level. This means that when you enable this on a volume you protect all the resources and shares residing on the volume. While you cannot select individual shares to turn this on or off for, you will still be able to recover information individually if needed because the volume is protected.

When a shadow copy is created for a file, only the incremental changes are stored for the file. This means the amount of storage needed for your network could be minimal, based on how many files and changes are made to the files. The copies you create can be stored on the same volume the data is stored. You can move the shadow copies to another volume, which will help the performance of the shadow copies and the volumes themselves. Before you enable shadow copies, you should also be aware you can have only 64 copies on the volume at one time. This will impact the schedule you choose as well, which is Monday through Friday from 7 a.m. to 12 p.m. (noon) by default. Shadow copies are run by the Volume Shadow Copy Service (VSS). When you enable shadow copies, there is a 100MB backup file automatically created. Additionally, by default the maximum size used for the backups is set to 10 percent of the volume's total space. What this means is that if you run out of space, VSS will start deleting older versions of your shadow copies.

Allowing your users to work quickly with these volumes will save you from having to use your recovery media to help restore lost data. However, shadow copies are not a replacement for your current backup and recovery implementation. Rather, they provide a nice complement for your backup and recovery tool belt.

For more information on Shadow Copy, take a look at the following:

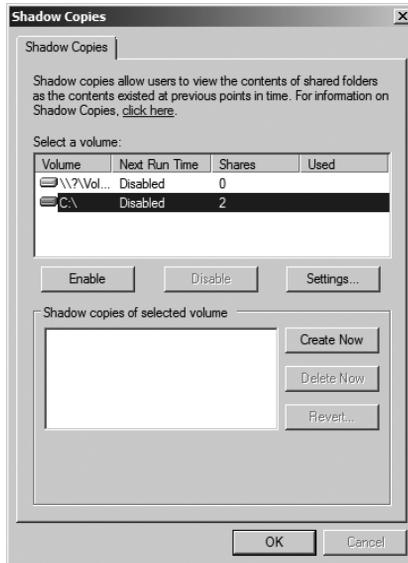
<http://technet.microsoft.com/en-us/library/cc771305.aspx>

Enabling shadow copies is just a matter of enabling the volume, and you can do this for both Windows Server 2008 R2 full and Server Core installations.

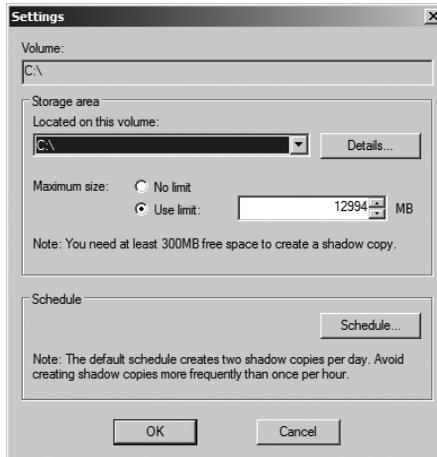
1. Open Computer Management by selecting Start ⇨ Administrative Tools ⇨ Computer Management.

- In the Computer Management tree on the left, right-click Shared Folders, and select All Tasks ⇨ Configure Shadow Copies. You will see a screen similar to Figure 8.4.

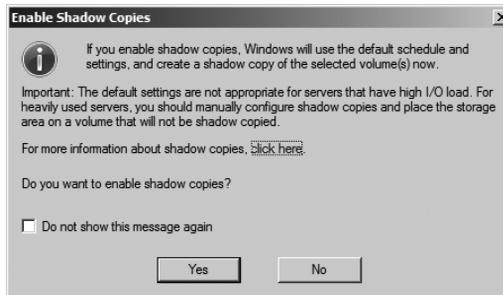
Figure 8.4: Enabling shadow copies



- Select the volume where the shares are located that you want to enable this feature on.
- To modify the settings for shadow copies, click Settings; you will see a screen similar to Figure 8.5. The Settings screen will allow you to control the location and schedule for the shadow copies. You can change the storage location for the shadow copies only when they are disabled on the volume. So, you want to make sure you change the location of the shadow copy storage before you enable shadow copies.

Figure 8.5: Shadow copy settings

5. After you have modified the settings, click Enable to enable shadow copies on your selected volume; you will see the warning shown in Figure 8.6.

Figure 8.6: Shadow copy warning

6. Click Yes to enable shadow copies. You can also select the Do Not Show This Message Again check box to not see the warning again.

Manage Backup and Recovery

Now that you have seen some of the tools for backups and recovery, it is time to put them to use. When you perform backups traditionally, you want to have the backups on a schedule so you are sure they are happening at regular intervals. This will make finding the right media for recovery easy. Even though backup and recovery are performed separately, they are joined together in form and function. The type of backup you perform will always dictate the recovery options available to you. In reality, the backup strategy is determined by your recovery requirements and what your service-level agreement is with your users and business. Is it OK if a user has to wait 24 hours to recover a file? What if the user is the CEO? Is it OK to turn off a server during work hours? What if the server is mission critical to your organization? These are all key questions, among many others, that you need to address when defining your policies and procedures and determining the best way to handle the needs of your organization.

Whether you choose to perform backup and recovery tasks with the GUI, command-line tool, or the PowerShell cmdlets, you are essentially performing the same task. In this section, you will learn how to use the backup and recovery tools to perform your daily tasks. Not that to perform either backup or recovery, you do need to be a member of the Backup Operators or Administrators groups.

Back Up Your Server

After you have determined your backup strategy, it is time to back up the server. When you back up your server, you want to make sure you schedule your backup times to not impact your network or your users. Try to schedule the backups after-hours, when the system is being used the least. You also want to make sure your backups complete in a timely manner; this is where knowing the difference between full and incremental backups can offer value to you and your organization.

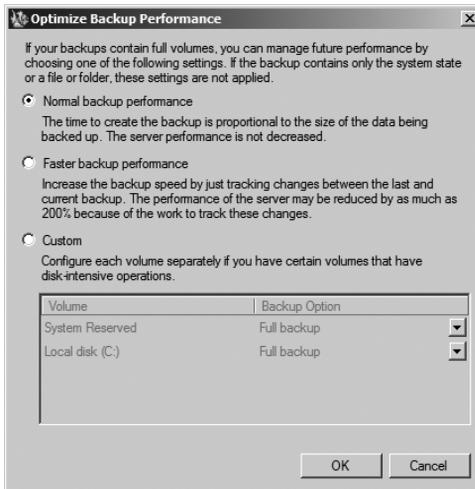
Configure Backup Settings

Before you perform your backup, you may need to define your backup settings. You have only a few selections to make to configure your backup. Specifically, you need to determine whether you want to perform a full/normal backup, an incremental backup, or a custom combination

of both of these methods. To configure your server, perform the following steps:

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. In the right Actions task pane, click Configure Performance Settings; you will see a screen similar to Figure 8.7.

Figure 8.7: Backup performance settings



The three options listed determine how the backup will be performed. It is important for you to know the choices you make here will not be applied if you are backing up only system state.

- Normal Backup Performance is the default method for Windows Server Backup, and this method will perform a normal backup.
 - Faster Backup Performance will perform an incremental backup for your system.
 - Custom will allow you to choose a combination of the previous two options for your drives. For example, you could perform a full backup on your data volume but only an incremental backup on your system drive.
3. Select the setting for your system, and click OK.

Back Up Your Server

After you have installed the backup tools, it is now just a matter of setting up the tasks to begin protecting your system. When you are ready to perform the backup and you know what files and folders you want to protect, you are ready to set up the backup test and schedule.

The first time you load the tool, you will see a message telling you no backup has been configured and you need to either set up a backup schedule or set up a backup once to begin protecting your system. Whether you choose to create a backup schedule or perform a backup once, the choices in the wizard are the same, with the exception of configuring the schedule:

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the backup wizard, in the Actions pane on the right, select Backup Schedule to create a regular backup task, or select Backup Once if you just want to perform an immediate backup. For this set of tasks, you will see the Backup Schedule choice.
3. Review the Getting Started screen, and click Next to see a screen similar to Figure 8.8.

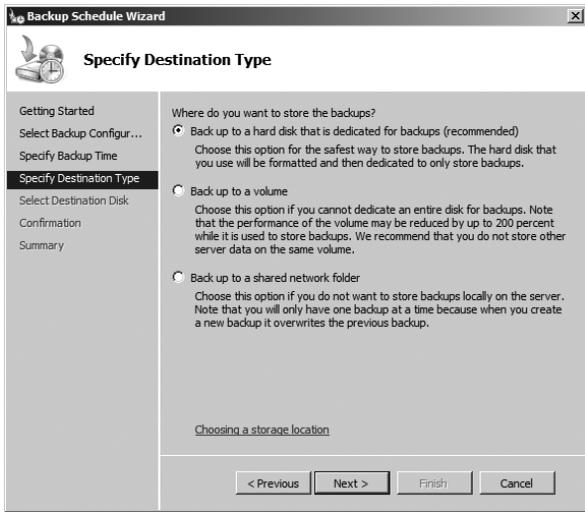
Figure 8.8: Configuring the backup



4. Select Full Server (Recommended), and click Next.
5. Set your schedule; the default is once a day at 9 p.m. You can also configure multiple times a day to perform the backup. After you set your schedule, click Next.
6. On the Specify Destination Type screen, as shown in Figure 8.9, you'll see two new choices in Windows Server 2008 R2; these allow you to store your backup to another volume and to a network share. These methods provide flexibility for your backup process that did not exist in prior versions of Windows servers. However, make sure you make note of the performance costs to your additional volume or network. You will have to decide what the right balance is for you and your organization. After you make your selection, click Next.

NOTE The first time you run the backup wizard, you may be asked to format the destination drive. When you select the default choice of Backup To Hard Disk That Is Dedicated For Backups, it will reformat the selected disk before the backup process begins. Make sure you have saved any necessary data off the drive. The format of the drive has to be NTFS; also, make sure you have at least 1½ times the free drive space compared to what you are backing up.

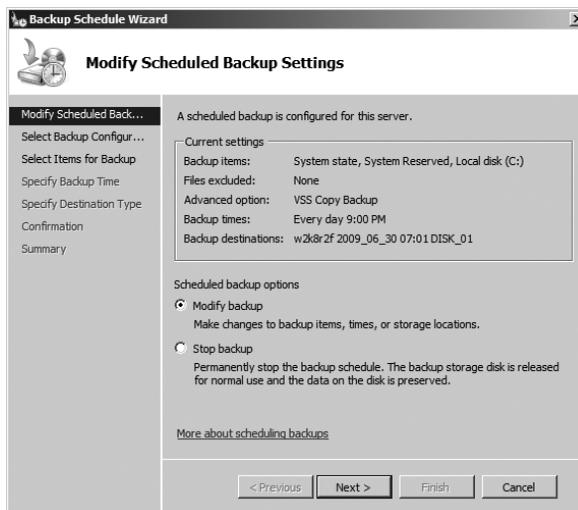
Figure 8.9: Backup destinations



7. On the Select Destination Disk page, select where you want to store your backups. For a scheduled backup, this can be another hard drive or a network share. It cannot be an optical drive or removable media. However, you can use optical drives or removable media for backup-once backups, and these media choices provide a great choice for bare-metal backups. After you make your selection, click Next.
8. If you are presented with a warning to format the disk and you are positive you want to use the selected disk, click Yes. Otherwise, click No, and select another drive to store your backup.
9. Review the Confirmation screen, and click Finish to create the scheduled task for backup and format the volume (if this is your first time using Windows Server Backup). If you chose Backup Once, you will click Backup to immediately perform the backup.
10. Review your Summary screen, and click Close.

NOTE After you have run the backup wizard the first time, the next time you run it you will see a screen similar to Figure 8.10. This allows you to modify the existing backup or stop the backup process. You can still configure the backup once if you need to create new backups for different files or needs, like bare-metal recovery.

Figure 8.10: Modifying the existing backup schedule

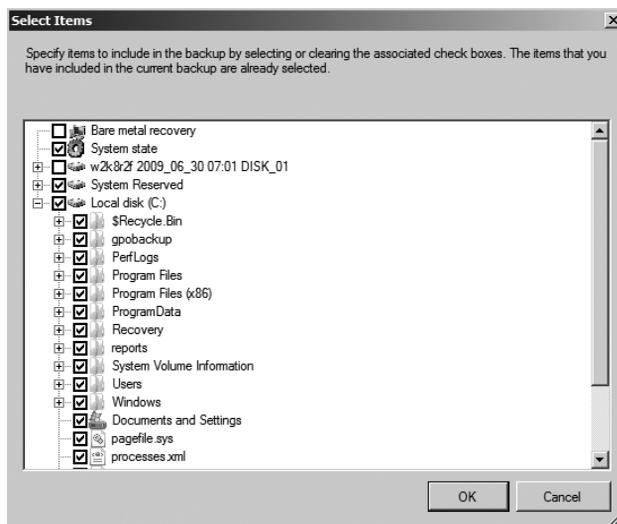


Back Up Specific Files

In Windows Server Backup in Windows Server 2008, you had to back up the entire volume. In Windows Server 2008 R2, you now can include or exclude folders or individual files. You can also exclude files based on the file types with filters. For this purpose, you will see how to modify an existing backup schedule.

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the backup wizard, in the Actions pane on the right, select Backup Schedule.
3. On the Modify Backup Schedules screen, verify that Modify Backup is selected, and click Next.
4. Select Custom, and click Next.
5. On the Select Items For Backup screen, you will see what you are currently backing up. If want to add or remove from the backup, click Add Items, and you will see a screen similar to Figure 8.11.

Figure 8.11: Backup item selection

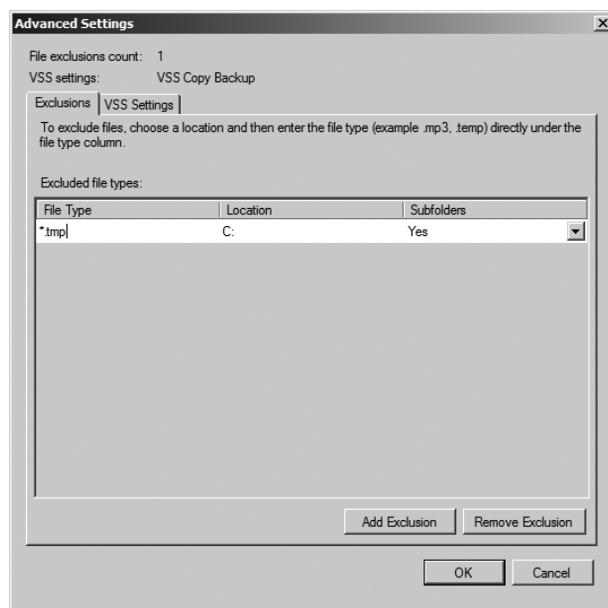


6. Select the items you want to add to or remove from the backup by selecting or deselecting the check boxes next to the items. If

you want to select specific folders, click the + sign next to your listed hard drives to expand the directory tree and then make your folder selections. When you are done selecting items to back up, click OK.

7. If you want to exclude certain files from your backup, such as temporary files (*.tmp) or music files (.wmv, .mp3, and so on), click the Advanced Settings button.
8. Click Add Exclusion to select the drive or folders you want to apply your exclusions.
9. Select the drive you want to use. Typically you will want your full volumes to have the exclusion applied. However, you can select individual folders or files to exclude directly. When you're done selecting your locations, click OK.
10. To exclude certain files, click in the File Type column, and type in your exclusion. You can also specify whether you want apply the filter to the subfolders. For example, if you wanted to exclude .tmp files from your backup, type *.tmp. Your screen would look similar to Figure 8.12.

Figure 8.12: Backup exclusions



If you want to add more exclusions, click **Add Exclusion**, and repeat the process. Likewise, if you want to remove the exclusion, you can select it and click **Remove Exclusion**.

11. When you are finished creating exclusions, click **OK** to proceed through the rest of the wizard.
12. Set or modify your schedule, and click **Next**.
13. Select your destination type, and click **Next**.
14. Select the destination disk, and click **Next**.
15. If you are presented with a warning to format the disk and you are positive you want to use the selected disk, click **Yes**. Otherwise, click **No**, and select another drive to store your backup.
16. Review the **Confirmation** screen, and click **Finish** to create the scheduled task for backup and format the volume (if this is your first time using **Windows Server Backup**). If you chose **Backup Once**, you will click **Backup** to immediately perform the backup.
17. Review your **Summary** screen, and click **Close**.

Perform a System State Backup

When you back up the system state, you are backing up a majority of the system configuration information. In **Windows Server 2008 R2**, you can perform the system state backup inside the **Windows Server Backup Tool**, and you do not have to solely use `wbadmin.exe`. Also, if you have installed additional roles on the **Windows Server 2008 R2** server, your system state will contain more data. By default, on a server with no additional roles, the system state backup always contains the following components:

- Registry
- COM+ class registration database
- Boot files, including system files
- System files under **Windows File Protection**

If the system is a domain controller in addition to the default system state data, system state will contain the following:

- **Active Directory** service
- **SYSVOL** directory

If you have installed clustering on the server, the system state data will contain the clustering services information.

If you have installed a certificate services server, the system state data will contain the certificate services database.

If you have installed IIS, the system state data will contain the IIS metadirectory.

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the backup wizard, in the Actions pane on the right, select Backup Schedule to create a regular backup task, or select Backup Once if you just want to perform an immediate backup. For this set of tasks, you will see the Backup Schedule choice.
3. Review the Getting Started screen, and click Next.
4. Select Custom, and click Next.
5. On the Select Items For Backup screen, click Add Items.
6. Click System State, click OK, and then click Next.
7. If presented with a scheduling window, set or modify your schedule, and click Next.
8. Select your destination type, and click Next.
9. Select the destination disk, and click Next.
10. If you are presented with a warning to format the disk and you are positive you want to use the selected disk, click Yes. Otherwise, click No, and select another drive to store your backup.
11. Review the Confirmation screen, and click Finish to create the scheduled task for backup and format the volume (if this is your first time using Windows Server Backup). If you chose Backup Once, you will click Backup to immediately perform the backup.
12. Review your Summary screen, and click Close.

Perform a Bare-Metal Backup

Another backup option that will provide you with a great option in case of a catastrophic failure is a bare-metal backup. The bare-metal backup will back up your system state, your system volume, and the system reserved data. This backup set is also unique in that you will need the Windows Server 2008 R2 installation media available during recovery.

This is a good time to use a USB drive or another portable media to store this backup. The main reason is because to perform the restore, you need to boot the system into the Windows Recovery Environment using a Windows Server 2008 R2 installation DVD.

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the backup wizard, in the Actions pane on the right, select Backup Schedule to create a regular backup task, or select Backup Once if you just want to perform an immediate backup. For this set of tasks, you will see the Backup Schedule choice.
3. Review the Getting Started screen, and click Next.
4. Select Custom, and click Next.
5. On the Select Items For Backup step, click Add Items.
6. Click Bare Metal Recovery, and click OK; then click Next.
7. If presented with a scheduling window, set or modify your schedule, and click Next.
8. Select your destination type, and click Next.
9. Select the destination disk, and click Next.
10. If you are presented with a warning to format the disk and you are positive you want to use the selected disk, click Yes. Otherwise, click No, and select another drive to store your backup.
11. Review the Confirmation screen, and click Finish to create the scheduled task for backup and format the volume (if this is your first time using Windows Server Backup). If you chose Backup Once, you will click Backup to immediately perform the backup.
12. Review your Summary screen, and click Close.

Look at the Scheduled Tasks

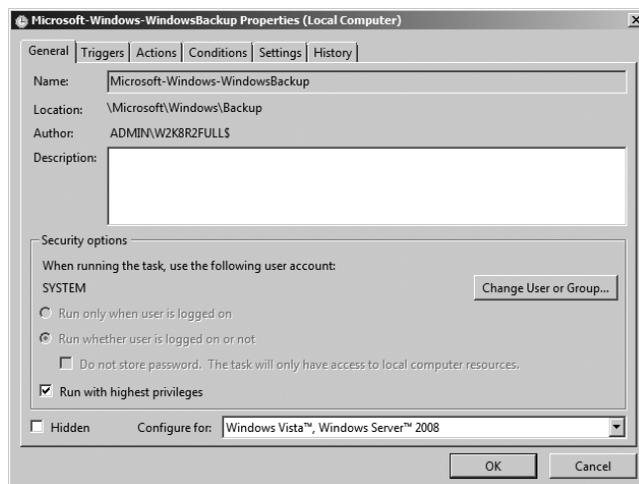
Whenever you create a backup schedule, you may be wondering where the task is stored. The task is stored in the Task Scheduler tool, and you can view your backup tasks there. You can also run the task directly from the Task Scheduler. The tasks in the Task Scheduler have several properties you can modify, as shown in Table 8.2.

Table 8.2: Task Property Tabs

Property Tab	Definition
General	Contains the description, author, and what account will be used to run the command.
Triggers	Determines when the task will be performed. In the case of a backup, the trigger is date and time.
Actions	Determines what programs or commands will be run.
Conditions	Specifies additional options, combined with the triggers, that determine whether the task should run.
Settings	Controls additional behaviors of the task. An important setting here is Allow Task To Be Run On Demand. If you want to be able to run your tasks directly from the Task Scheduler, you have to select this setting to turn it on.
History	Shows the past history of the task when it was run.

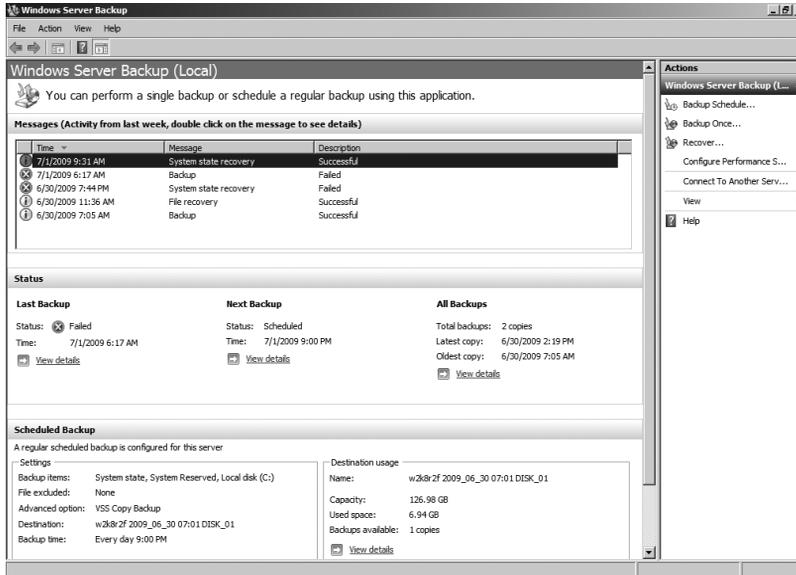
1. Click Start ⇨ Administrative Tools ⇨ Task Scheduler.
2. Expand the tree to view the backup tasks. Click the + to expand Task Scheduler Library ⇨ Microsoft ⇨ Windows, and then click Backup.
3. Double-click the task to view the properties of the backup task, and you will see a screen similar to Figure 8.13.

Figure 8.13: Backup task



You can also view the status of your backups and get more details on the main console page of the Windows Server Backup window, as shown in Figure 8.14.

Figure 8.14: Windows Server Backup



From the main console window, you can view the details, status, and next schedule for your backups and recovery processes. The Windows Server Backup Tool will show all the events with your backups and restores in this main console window.

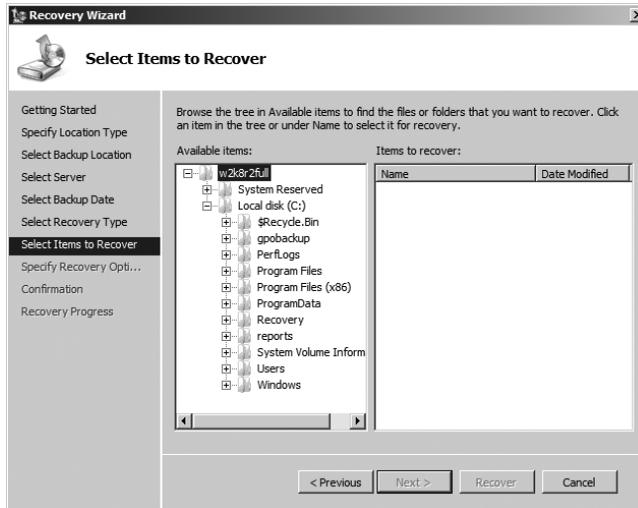
Recover Your Data

I hope recovering your data is not a daily task. However, you should know how to recover data just in case. Fortunately, the recovery tool is straightforward to use presuming you have performed a proper backup. The method used to back up your data will always determine what recovery method you will need to perform. Your desired outcome will impact what and how you need to perform your recovery.

Restore Specific Files or a Full Volume

If the time comes that you need to recover the files, it is just a matter of knowing what files and what time frame you need to restore.

1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the recovery wizard, in the Actions pane on the right, select Recover.
3. Select where you have stored the backup, and click Next. If the backup is stored locally on an internal hard drive, verify This Server is selected, click Next, and proceed to step 7. If the backup is stored elsewhere, select A Backup Stored On Another Location, and click Next.
4. Depending on the location of the backup, click Local Drives or Remote Shared Folder, and click Next. If you specified Remote Shared Folder, you will need to type in the UNC name for the backup in the form of \\servername\sharename.
5. On the Select Backup Location screen, verify your backup set, and click Next.
6. Select the server data you want to recover, and click Next.
7. On the Select Backup Date screen, select the date and possible time for the backup set you want to recover from, and click Next.
8. On the Select Recovery Type page, select what you want to recover.
 - Select Specific Files Or Folders if you trying to recover a specific file or folder. When you select this option and click Next, you will see a screen similar to Figure 8.15, allowing you to expand the tree to recover the file from.
 - Select Volumes if you need to recover the entire volume from a backup set. When you select this option and click Next, you will be provided with a list of volumes to select from.
 - Select System State if you want to recover system state.

Figure 8.15: Recovering a specific file

NOTE You may also notice a choice called Applications. Depending what applications you have installed on your server, some may have registered with Windows Server Backup. If they have, you have the ability to recover those applications as well.

9. After you make your selection for the recovery of files, click Next.
10. The Specify Recovery Options screen will look like Figure 8.16. This screen gives you a few options on how you want to recover the file. You can recover to the original location or an alternative location. You can also control whether you create a copy of the file to make sure you have both versions, overwrite any existing version of the file, or do not recover the file if one already exists. You can also bring back any security permissions on the file. After you make your selection, click Next.
11. Review the Confirmation screen, and click Recover.
12. After the recovery process is complete, review the results, and click Close.

Figure 8.16: Recovery options



Perform a System State Restore

When you want to recover system state data, you need to take an extra bit of precaution and planning when recovering this data. Because of the nature of the data being recovered, you have the potential to render your system unbootable. Specifically, when this restore process is started, it cannot be stopped or interrupted. If it is, this process could render your server unbootable. In other words, use caution when recovering the system state. Of course, if you are using this process, chances are you are not too far from having to rebuild your server anyway.

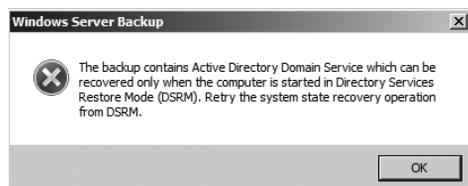
1. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
2. To launch the recovery wizard, in the Actions pane on the right, select Recover.
3. Select where you have stored the backup, and click Next. If the backup is stored locally on an internal hard drive, verify that This Server is selected, click Next, and proceed to step 7. If the backup is stored elsewhere, select A Backup Stored On Another Location, and click Next.

4. Depending on the location of the backup, click Local Drives or Remote Shared Folder, and click Next. If you specified Remote Shared Folder, you will need to type in the UNC name for the backup in the form of \\servername\sharename.
5. On the backup location screen, verify your backup set, and click Next.
6. Select the server data you want to recover, and click Next.
7. On the Select Backup Date screen, select the date and possible time for the backup set you want to recover from, and click Next.
8. On the Select Recovery Type screen, select System State to recover the system state information, and click Next.
9. Select the area you would like to recover your system state data to, either the original location or an alternate location. If you are trying to recover, make your selection, and click Next.
10. On the Summary screen, review your selections, and then click Recover.
11. After the recovery process is complete, review the results, and click Close.

Recover System State Data Containing Active Directory Data

If your system state backup contains Active Directory information, you will not be able to recover the data via the recovery wizard unless you specify an alternate location to recover to. If you try to recover the data in the Windows Server Backup tool, you will see an error message similar to the one shown in Figure 8.17.

Figure 8.17: System state with Active Directory data error

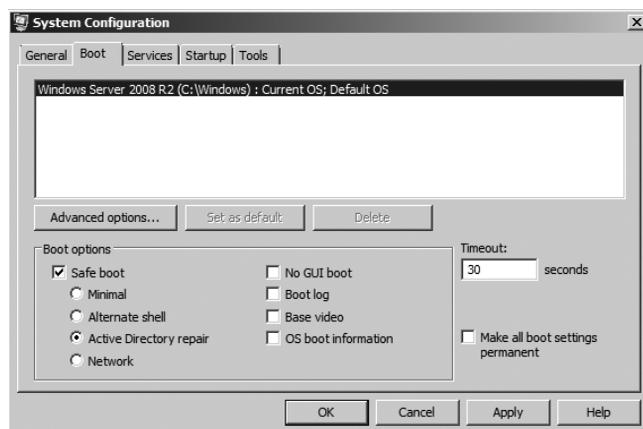


To perform a system state recovery of your Windows Server 2008 R2 server containing Active Directory information, you need to boot the operating system into Directory Services Restore Mode (DSRM). Specifically, you will be performing an authoritative restore.

Before you can boot into DSRM, you need to configure your boot process:

1. Click Start, type **msconfig**, and click the Msconfig program under Programs.
2. Click the Boot tab.
3. In the Boot Options section, select the Safe Boot check box, and select the Active Directory Repair option. Click OK. Your screen should look like Figure 8.18.

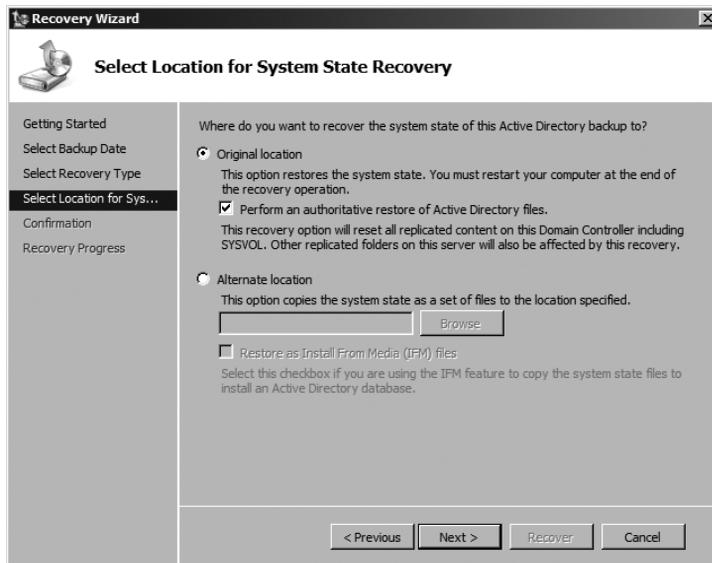
Figure 8.18: Booting into DSRM



4. Restart the server.
5. Log on to the server with the local administrator ID and the DSRM password you created while installing the server.
6. Start Windows Server Backup by selecting Start ⇨ Administrative Tools ⇨ Windows Server Backup.
7. To launch the recovery wizard, in the Actions pane on the right, select Recover.

8. Select where you have stored the backup, and click Next. If the backup is stored locally on an internal hard drive, verify that This Server is selected, click Next, and proceed to step 12. If the backup is stored elsewhere, select A Backup Stored On Another Location, and click Next.
9. Depending on the location of the backup, click Local Drives or Remote Shared Folder, and click Next. If you specified Remote Shared Folder, you will need to type in the UNC name for the backup in the form of \\servername\sharename.
10. On the Specify Backup Location screen, verify your backup set, and click Next.
11. Select the server's data you want to recover, and click Next.
12. On the Select Backup Date screen, select the date and possible time for the backup set you want to recover from, and click Next.
13. On the Select Recovery Type screen, select System State to recover the system state information, and click Next.
14. Select Original Location, and select Perform An Authoritative Restore Of Active Directory files, as shown in Figure 8.19.

Figure 8.19: Authoritative restore



15. You will receive a warning noting that all replicated content on the server will be resynchronized and that this can cause potential latency on your server and network. Acknowledge the message by clicking OK.
16. On the Summary screen, review your selections, and then click Recover.
17. You will receive another warning message stating that system state recovery cannot be paused or canceled once it has started. Click Yes to proceed with the recovery, or click No to complete the recovery at a later time.
18. After the recovery process is complete, review the results, and click Close.
19. Before you restart the server, you need to turn off DSRM.
20. Click Start, type **msconfig**, and click the Msconfig program under Programs.
21. Click the Boot tab.
22. In the Boot Options section, deselect the Safe Boot check box. Click OK.
23. Restart the server, and log on with your normal domain credentials.
24. If you see a command prompt window notifying you the status of your recovery, review the message, and press the Enter key.

Perform a Bare-Metal Restore

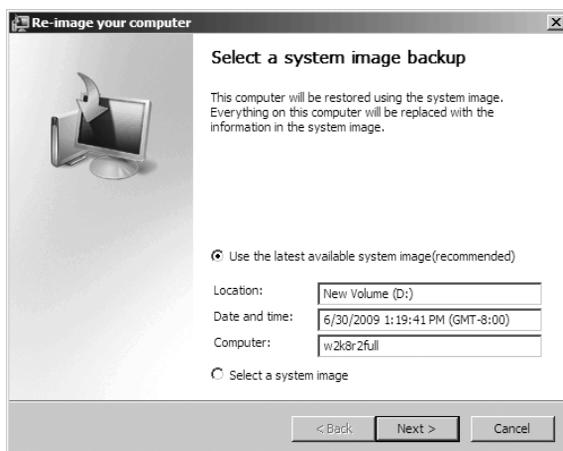
Sometimes you run into problems that a simple file restore or a system state recovery cannot fix. If you have created a bare-metal recovery image, then you can recover your full server using the recovery process. This recovery process is different from recovering just files or the system state. The bare-metal recovery process is part of the Windows Recovery Environment, and to get to it, you need a Windows Server 2008 R2 DVD to boot the operating system to, and you need access to the drive containing the bare-metal backup. Typical USB drives can work really well in this scenario presuming your BIOS supports USB at boot.

Additionally, this recovery process is destructive, meaning when you run a bare-metal recovery all the data on your drives will be replaced with data from the system image. You also have the potential during

the recovery process to partition and format the drives, in other words, restoring the server completely to a previous working state.

1. Make sure your backup media is attached to the server, and insert and boot to your Windows Server 2008 R2 DVD.
2. Select your language preferences, and click Next.
3. In the Install Now window, click the Repair Your Computer option located in the lower left of the installation window.
4. To recover from your bare-metal backup, select the Restore System Using A System Image You Created Earlier radio option, and click Next. You can also get to the image via the Recovery Tools option.
5. The system image will scan your system's drives for an image for you to restore from; you will see a screen similar to Figure 8.20. You can select the image provided to, usually the most current, or you can select a different image by selecting Select A System Image. When you have the proper image selected, click Next.

Figure 8.20: Bare-metal image selection



6. On the Choose Additional Restore Options screen, you have the ability to control how your drives and partitions are handled, as shown in Figure 8.21. You can repartition and format the drives. You can also exclude drives from the partition, which is particularly useful when you want to keep other drives intact. By clicking

Advanced, you will see a window similar to Figure 8.22. This window allows you to control whether you want restart upon completion. It will also allow you to perform a hard disk scan to check and possibly repair errors. After you're done, select your options, and click Next.

7. Review your selections, and click Finish to begin the bare-metal restoration.

Figure 8.21: Bare-metal recovery options

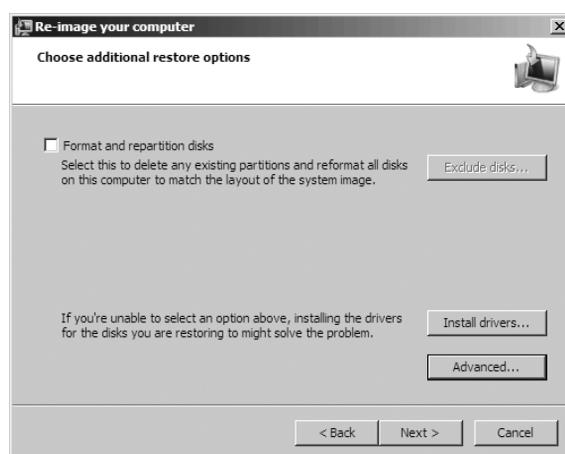
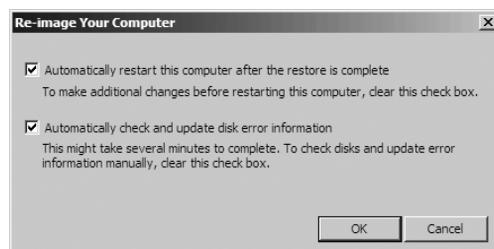


Figure 8.22: Advanced options



8. You will be presented with a warning reminding you that the process will replace existing data from the bare-metal backup image. If this is what you want to do, click Yes to finalize the restoration

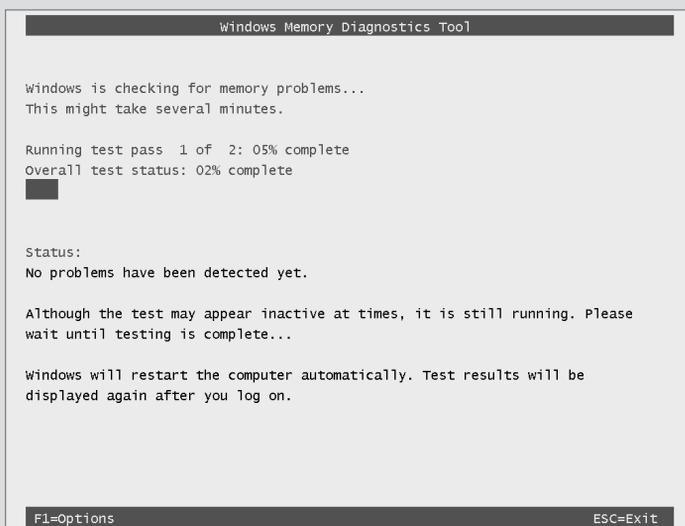
process. This process could take a long time to complete based on how much data you need to recover.

9. When the recovery is complete, you will be prompted to restart, or the system will restart automatically (the default option).

Windows System Recovery Tools

During the bare-metal restore process, you saw an option to load the Windows system recovery tools. The Windows system recovery tools provide you with three options to further troubleshoot your environment:

- **System Image Recovery** will take you to the bare-metal recovery wizard to allow you to fully recover your system.
- **Windows Memory Diagnostics** will perform diagnostic checks on the memory of your system to see whether faulty memory is to blame for any system errors. When you select this option, you will be asked to either restart the system immediately to check for problems or schedule the memory check for the next time you restart the system. Pressing F1 will allow you to control the types and number of memory tests you can perform. When the test is running, you will see a screen similar to this one.



- **Command Prompt** will load a command prompt to allow you to perform a variety of command prompt actions.

Recover via Shadow Copy

Recovering files via a shadow copied shared volume is something you can teach your users to do. It is very straightforward to work with when it is enabled and as easy to access as right-clicking the file or folder you want to perform the recover. To access the shadow copies on your Windows Server 2008 R2 server, the users must be running an operating system that supports the Shadow Copy Client. Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 all have built-in support for the Shadow Copy Client. For Windows XP or Windows Server 2000 SP3 or later, you need to download the client located from this location:

<http://support.microsoft.com/kb/832217>

Using the Shadow Copy Client to recover a file is just a matter of knowing where the file is located and knowing how you want to recover the file. Shadow copies are great if a user has accidentally deleted a file or folder or inadvertently overwritten a file, such as by choosing Save instead of Save As. You can work with the shadow copy files or folders just like you would any regular file or folder.

When restoring with shadow copies, you have three options, as listed in Table 8.3.

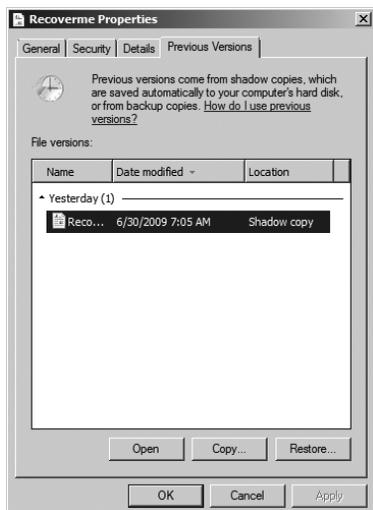
Table 8.3: Shadow Copy Options

Option	Usage
Open	Allows you to open a shadow copy of the file or folder to view any changes. You can copy and paste between the shadow copy and the original file or folder. This method is very useful when you want only to recover a file from a folder instead of the whole folder.
Copy	This will make a copy of the shadow copy and store it in a different location. This is also useful when you want to compare files or folders side by side.
Restore	This will restore the file in the original location. Be careful if you restore a folder with this method because it will restore all the contents of the folder.

You can access the shadow copies either locally if the shadow copy has been enabled on your local volume or via a network share after you have opened the folder or share where you want to recover data from.

1. Right-click the file or folder you want to restore with the shadow copy. You can also right-click the whitespace of an opened folder.
2. Select Properties.
3. Click the Previous Versions tab; your screen will look similar to Figure 8.23.

Figure 8.23: Shadow copy restore



4. Select the shadow copy you want to use; they are stored by date and time.
5. Select Open, Copy, or Restore.
6. When you are finished, click OK.

NOTE If you do not see any shadow copies listed, the most likely cause is that the file has not changed. Remember, shadow copies store only the changes for the files, and if there are no copies listed, the file is the original.

It is important you also know that shadow copy is not retroactive. The feature will not protect you until the feature is enabled. In other words, if a user makes changes to files or deletes a file prior to enabling shadow copy, the act of enabling shadow copy will not allow you to retroactively make copies of files and folders.

Perform Backup and Recovery with Command Tools

You may choose to back up and recover your systems with command-line tools. Specifically, in the case of a Windows Server 2008 R2 Server Core installation, two options are available to you; they are the command-line tool `wbadmin.exe` (the command-line equivalent of the Windows Server Backup GUI) and PowerShell cmdlets.

Regardless of which tool you use, the techniques, terminology, and processes in this chapter still apply. These tools provide the same capabilities as the GUI for Windows Server Backup. Therefore, you do not need to relearn all the previously mentioned information—the command-line versions are just an alternative way to access the tools.

In this section, you will see how to back up and recover your systems with the command-line tools.

Use `wbadmin.exe`

Using the command-line tool `wbadmin.exe` provides you with a method to create scripts for backup as well as a method to back up servers like Server Core installations where there is no GUI present. Table 8.4 describes some of the common switches for the `wbadmin.exe` backup. For more information on how to use `wbadmin.exe`, in a command prompt, type the following command and hit Enter:

```
wbadmin /?
```

Table 8.4: `wbadmin.exe` Common Switches

Switch	Explanation
<code>enable backup</code>	Allows you to modify or create a backup schedule
<code>start backup</code>	Performs a one-time backup
<code>get disks</code>	Lists the current disks available and online
<code>start systemstatebackup</code>	Allows you create a system state backup
<code>start recovery</code>	Begins the recovery process from an existing backup

wbadmin.exe Examples

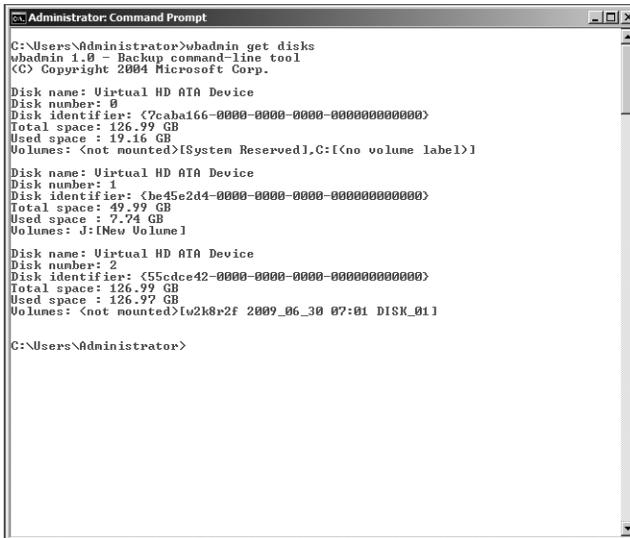
Here are some examples on how you can use `wbadmin.exe` to perform the various tasks of backup and recovery.

Before you back up the systems, you will need to see what drives are available on the system. When you create a backup, you can use the drive letter if one exists, or you will need the disk identifier. To see what drives are available, run the following command:

```
wbadmin get disks
```

Your output will look similar to Figure 8.24.

Figure 8.24: Available online disks



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

Disk name: Virtual HD ATA Device
Disk number: 0
Disk identifier: {7caba166-0000-0000-0000-000000000000}
Total space: 126.99 GB
Used space: 19.16 GB
Volumes: <not mounted>[System Reserved],C:[no volume label]

Disk name: Virtual HD ATA Device
Disk number: 1
Disk identifier: {be45e2d4-0000-0000-0000-000000000000}
Total space: 49.99 GB
Used space: 7.74 GB
Volumes: J:[New Volume]

Disk name: Virtual HD ATA Device
Disk number: 2
Disk identifier: {55cdce42-0000-0000-0000-000000000000}
Total space: 126.99 GB
Used space: 126.97 GB
Volumes: <not mounted>[v2]kRr2f 2009_06_30 07:01 DISK_01

C:\Users\Administrator>
```

The following command will create a backup of the C and D drives and would occur daily at 4 a.m. and 10 p.m. The backup would be stored on the disk {7caba166-0000-0000-0000-000000000000}.

```
wbadmin enable backup
-addtarget:{7caba166-0000-0000-0000-000000000000}
-schedule:04:00,22:00 -include:c:,d:
```

If you wanted the backup to occur just once, the command would look like this:

```
wbadmin start backup
-backuptarget:{7caba166-0000-0000-0000-000000000000}
-include:c:,d:
```

The following command would back up the system state to the disk {7caba166-0000-0000-0000-000000000000}:

```
wbadmin start systemstatebackup
-backuptarget:{7caba166-0000-0000-0000-000000000000}
```

To be able to restore items with `wbadmin.exe`, you need to know two things: the backup version identifier and what items are stored in the backup. You use `wbadmin get versions` to find out what backups you currently have available. Specifically, you are looking for the version identifier, which is formatted as a date and timestamp. You would run the following command to see the items backed up on June 30, 2009, at 2:05 p.m.

```
wbadmin get items -version:06/30/2009-14:05
```

The results would look similar to Figure 8.25.

Figure 8.25: `wbadmin.exe get items`

```
Administrator: Command Prompt
C:\Users\Administrator>wbadmin get items -version:06/30/2009-14:05
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Volume ID = {71f9e6d2-3847-11de-87ee-806e6f6e6963}
Volume 'System Reserved', mounted at <not mounted> 'System Reserved', mounted at
<not mounted> at the
time the backup was created)
Volume size = 100.00 MB
Can recover = Full volume

Volume ID = {71f9e6d3-3847-11de-87ee-806e6f6e6963}
Volume '<Unlabeled Volume>', mounted at C:
Volume size = 126.89 GB
Can recover = Full volume

Application = FRS
Component = AADF2A0B-705E-4549-9A7E-3FF0BEC2ED48-20B856F4-F07A-455C-9363-BC53E79
EB2DD {SYSVOL\AADF2A0B-705E-4549-9A7E-3FF0BEC2ED48-20B856F4-F07A-455C-9363-BC53E
79EB2DD}

Application = AD
Component = ntds <C:\Windows\NTDS\ntds>

Application = Registry
Component = Registry <\Registry>

C:\Users\Administrator>
```

The following command would restore the C volume from the backup taken on June 30, 2009, at 2:05 p.m.:

```
wbadmin start recovery -version:06/30/2009-14:05
-itemType:Volume -items:c:
```

Use PowerShell

Using the backup and recover cmdlets for Windows Server 2008 R2 follow the same syntax and language from Chapter 3. These cmdlets provide another tool to perform your server recovery. If you choose to install the command-line tools for Windows Server Backup, you will have access to the PowerShell backup and restore cmdlets as well. Before you can run these tools, you have to verify the PowerShell snap-in for backing up has been loaded.

To verify the tools have been loaded, run the following command from a PowerShell window. Then verify you see `Windows.ServerBackup` as the loaded snap-in.

```
Get-PSSnapin
```

If you do not see Windows Server Backup in your loaded snap-ins, you will need to run this command:

```
Add-PSSnapin windows.serverbackup
```

Working with the PowerShell is quite a bit more complex than working with `wbadmin.exe` to perform backup tasks. You need to create a PowerShell script to accomplish your tasks. Although PowerShell can be more complex, it does offer some nice flexibility to performing backups. All the capabilities of PowerShell are determined by what backup policy you set. The backup policy for PowerShell is stored in an object called `WBPolicy`. The `WBPolicy` object contains all the settings for the backup, including the schedule, backup types, backup targets, and so on.

Working with PowerShell and backup, you need to understand how to set the values for the `WBPolicy` object. Table 8.5 describes some of the common PowerShell commands used for backup and recovery and how to set the parameters for `WBPolicy`. For a full listing of the PowerShell cmdlets for backing up the system, run the following cmdlet:

```
Get-Command *wb* -CommandType cmdlet
```

Table 8.5: PowerShell Backup Cmdlets

cmdlets	Explanation
Get-WBPolicy	Displays the current settings for the WBPolicy object on the server
Set-WBPolicy	Allows you to set the parameters for the WBPolicy
Add-WBVolume	Adds a volume to the WBPolicy object to be backed up
Add-WBSystemState	Adds the system state to the WBPolicy object to be backed up
Set-WBSchedule	Sets the time for your daily backup schedule
Start-WBBackup	Starts a one-time backup
Get-WBJob	Shows the current status of a running backup job

PowerShell Examples

As you can see in Table 8.5, only a few of the commands are available to work with PowerShell in Group Policy. This section gives a couple of examples to allow you to get used to using PowerShell.

The following two lines will back up your system with your current backup policy settings. You can create a PowerShell script to run these commands, or you can run each line separately by hitting Enter after each line:

```
$policy = Get-WBPolicy
Start-WBBackup -Policy $policy
```

This first line sets the `$policy` variable to the current settings in WBPolicy. The second line starts the backup process with settings currently in the `WPObjct` object's `$policy` variable.

The following script will back up the C, D, and system state on your system to your Z drive. Notice you will be using a variety of the Add cmdlets to modify the value of the variable `$policy`, as well as variables for target and paths:

```
$policy = New-WBPolicy
$volume = Get-WBVolume -VolumePath c:
Add-WBVolume -Policy $policy -volume $volume
$volume1 = Get-WBVolume -VolumePath d:
```

```
Add-WBVolume -Policy $policy -volume $volume1
Add-WBSystemState -Policy $policy
$target = New-WBBackupTarget -VolumePath Z:
Add-WBBackuptarget -Policy $policy -target $target
Start-WBBackup -Policy $policy
```