



realtimepublishers.com<sup>™</sup>

*The Shortcut Guide<sup>™</sup> To*



# Rapid Windows Recovery

**Winternals**<sup>®</sup>

*Jeremy Moskowitz*

Chapter 4: Prescriptive Guidance and Best Practices .....	61
Preparing for and Averting Disaster .....	61
Multiple Domain Controllers .....	61
Multiple WINS Servers.....	62
Multiple DNS Servers.....	65
Setting up for Redundancy in AD.....	66
Setting up a Robust DNS .....	66
Multiple DHCP Servers .....	67
Ongoing Data Backup.....	68
Winternals Recovery Manager 2.0 .....	69
Microsoft System Center Data Protection Manager .....	71
DPM Nuts and Bolts .....	72
DPM Benefits.....	75
DPM Day-to-Day.....	75
Symantec Backup Exec 10D with “Retrieve” Software.....	76
Additional Preventative Maintenance: Backup of AD Support Structure .....	77
WINS Backup and Restore .....	77
DHCP Backup and Restore.....	80
DNS Backup and Restore .....	81
Understanding Tape Backup Types .....	82
Getting to the Backup Types.....	82
Understanding the Archive Bit .....	83
Understanding the Backup Types .....	83
Normal .....	83
Copy .....	83
Differential Backups .....	84
Incremental Backups.....	84
Daily Backup .....	84
Differential vs. Incremental .....	84
Differential.....	84
Incremental .....	85
Summary .....	85

## Copyright Statement

© 2006 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

---

## Chapter 4: Prescriptive Guidance and Best Practices

The previous chapter took a look at how to get back AD data if a specific domain controller goes belly up. The chapter also explored how to get back a specific user or group if the account is deleted. This final chapter will offer prescriptive guidance and review best practices that can prevent problems from becoming disasters. A little preventative maintenance here and a little forethought there can mean the difference between a bad day gone good, and a bad day gone really, really bad. Let's take a look at some things you can do to keep disasters at bay.

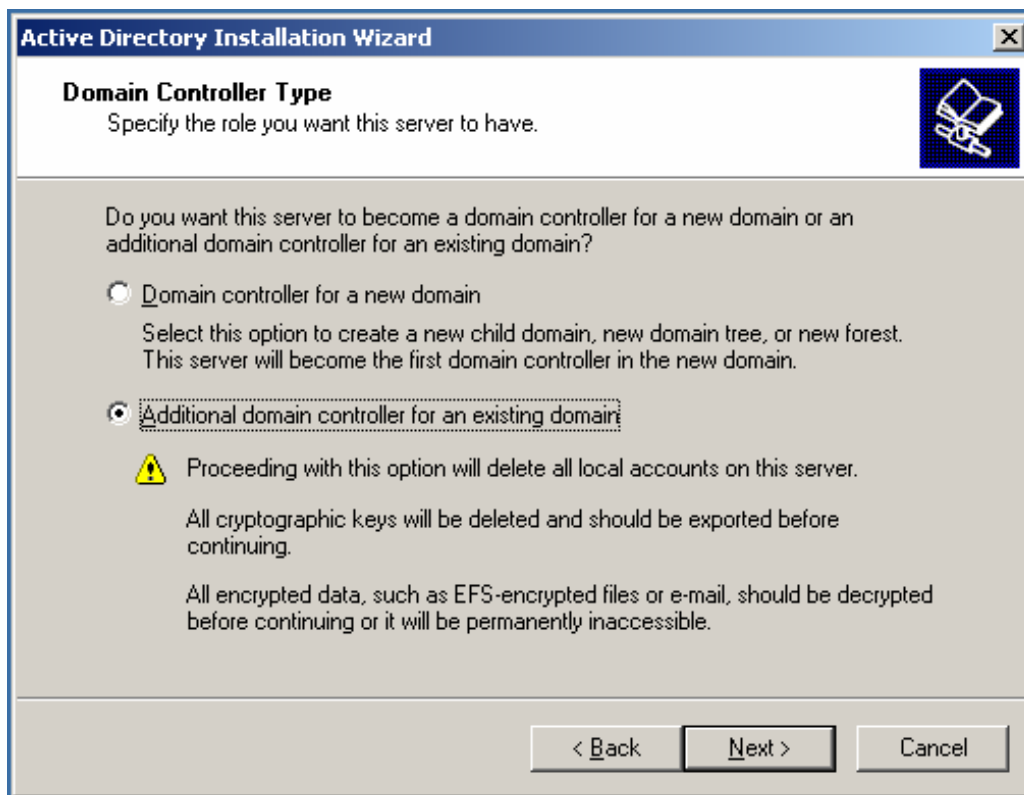
### Preparing for and Averting Disaster

One of the best parts of networking is that you can often just “create another copy” of what you need elsewhere. Garden variety backup and recovery is really only that: preserving a copy of what you need somewhere else in case disaster strikes. When it comes to the “moving parts” of your network, you can do something similar—even if you can't always easily make copies of your data. Let's examine some ways you can ensure that you have copies of your key moving parts online elsewhere on your network.

#### ***Multiple Domain Controllers***

The previous chapter touched on the subject of multiple domain controllers; this section dives into this topic a little deeper. Specifically, having other domain controllers to supplement your first domain controller is of paramount importance.

Employing more than one domain controller should be one of the very first things you do when you implement AD to ensure that if one domain controller goes down, at least one other domain controller contains a copy of the accounts database. The last chapter discussed how you can get out of a jam if your one and only domain controller should die—but, it's such an inexpensive proposition to get another domain controller for safety that the ROI is typically rapid. Many Small Business Servers (SBS) run with just one domain controller. However, you can add other domain controllers for additional protection (see Figure 4.1).



**Figure 4.1:** Use the `DCPROMO` command to bring up another domain controller from a member server.

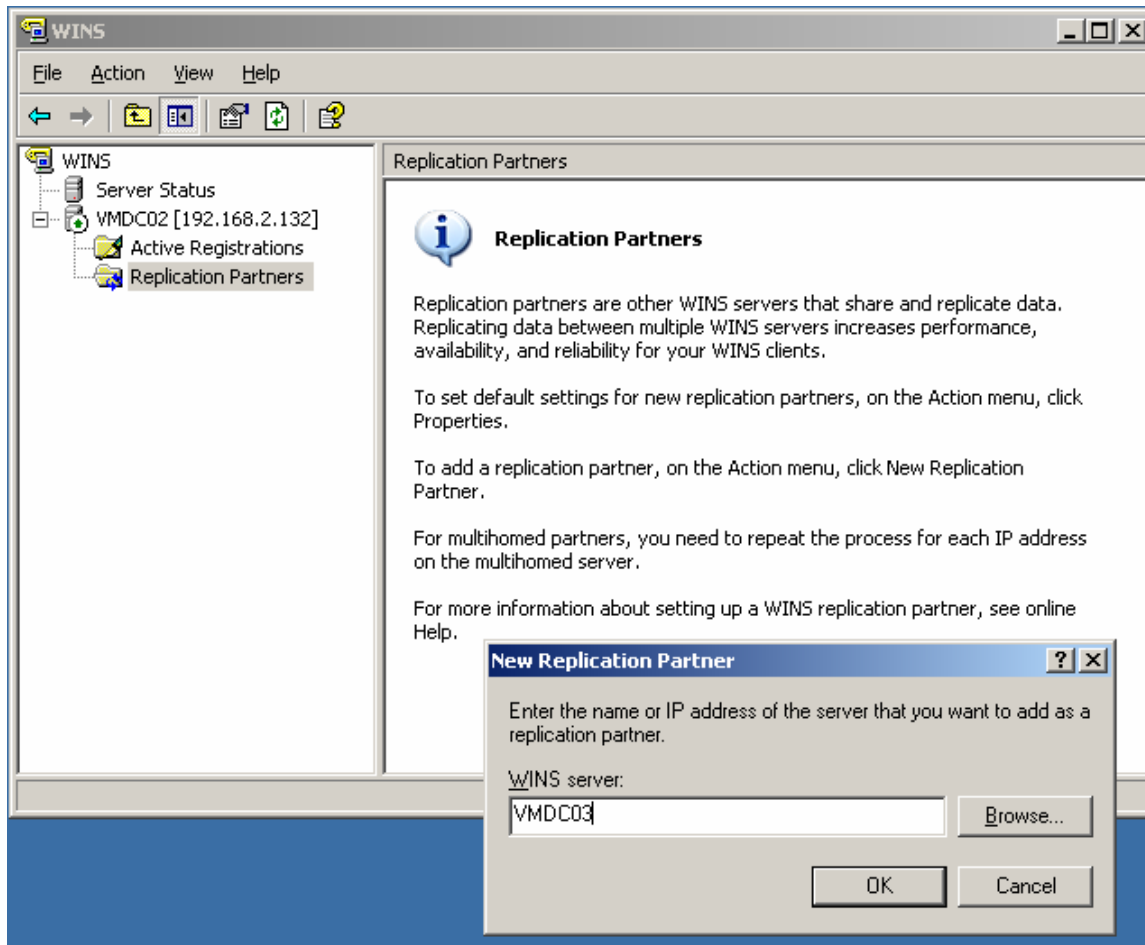
When you bring up your domain controller, the best approach is to put it in another physical site so that if the site with the first domain controller should burn down, get flooded, or otherwise be damaged, at least you didn't put both domain controller eggs in the same basket. In other words, you wouldn't want one site to be a single point of failure.

### **Multiple WINS Servers**

The Windows Internet Naming Service (WINS) helps your clients determine which computer's IP addresses belong to which computer's NETBIOS name. Although the industry is moving in that direction, WINS still can't be cast aside in favor of a pure DNS lookup. Too many applications still require WINS—both Microsoft and third-party applications rely on WINS to perform NETBIOS name resolutions.

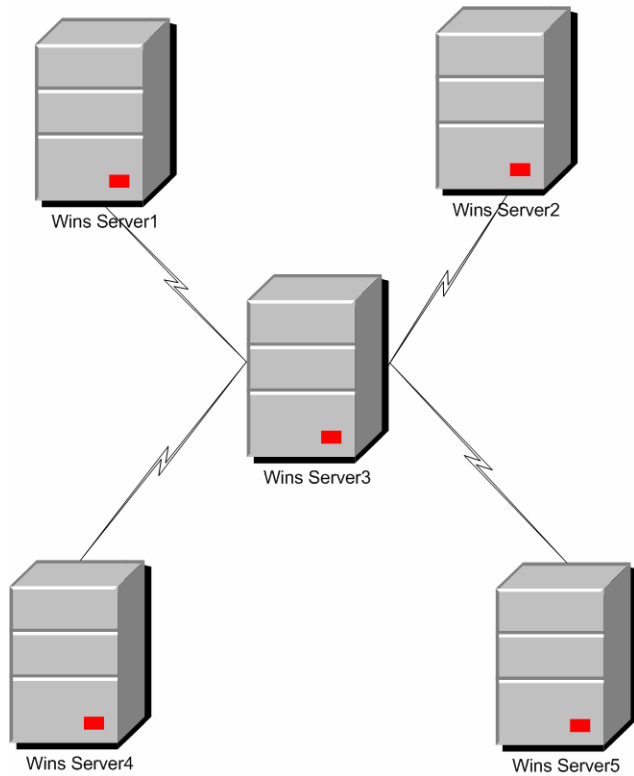
In other words, keeping WINS alive is important for the proper care and feeding of your network. With that in mind, having a second WINS server on the wire is smart, and fortunately quite easily done.

First, choose the machine that you want act as a WINS replication partner. Then use Add/Remove Programs on that computer to load the WINS software. Finally, on an existing WINS server, use the WINS manager, and right-click Replication Partners, then select New Replication Partner. The New Replication Partner dialog box will appear as Figure 4.2 shows.



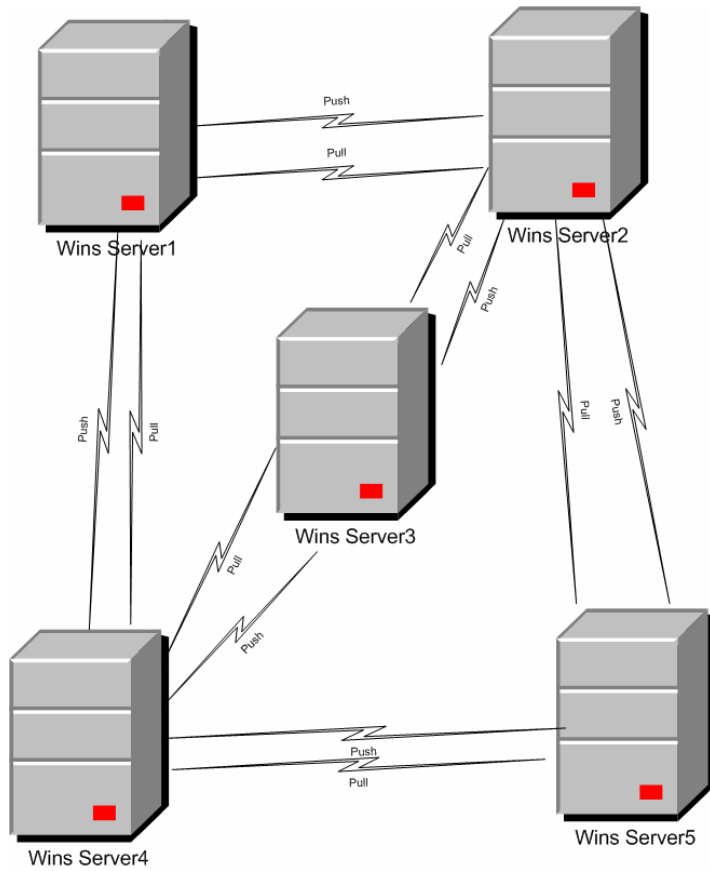
**Figure 4.2:** Set up your WINS replication partnerships for fault tolerance.

Next, provide the information about your new partner. That target machine will automatically be a push and pull partner of this machine. That is, it will accept any WINS updates that this server provides as well as inform this server about updates only it has. In Figure 4.3, you can see a WINS hub-and-spoke topology.



**Figure 4.3: A WINS hub-and-spoke topology.**

This design is common. However, it has one big drawback. That is, replication to the spokes will stop if the hub server (WINS server 3) should go down. Instead, consider a WINS ring topology, as seen in Figure 4.4.



**Figure 4.4: A WINS ring topology.**

In the configuration that Figure 4.4 shows, you are replicating all the spokes to each other. WINS Server 3, which was central to the replication partnerships in Figure 4.3 becomes less important.

### **Multiple DNS Servers**

AD and DNS are intrinsically linked. Without a healthy DNS, AD will fail to perform properly. It's a very, very good idea to ensure that you have multiple DNS servers in AD. Let's look at how this is done.

## Setting up for Redundancy in AD

The ideal way to have redundant DNS servers is to utilize AD to be the storage place for DNS data. To do so, you need to run your DNS servers on the domain controllers. Once you've loaded DNS, you can simply set the DNS server to use AD as the place to store the data through the settings on the Advanced tab of each domain controller running DNS (see Figure 4.5).

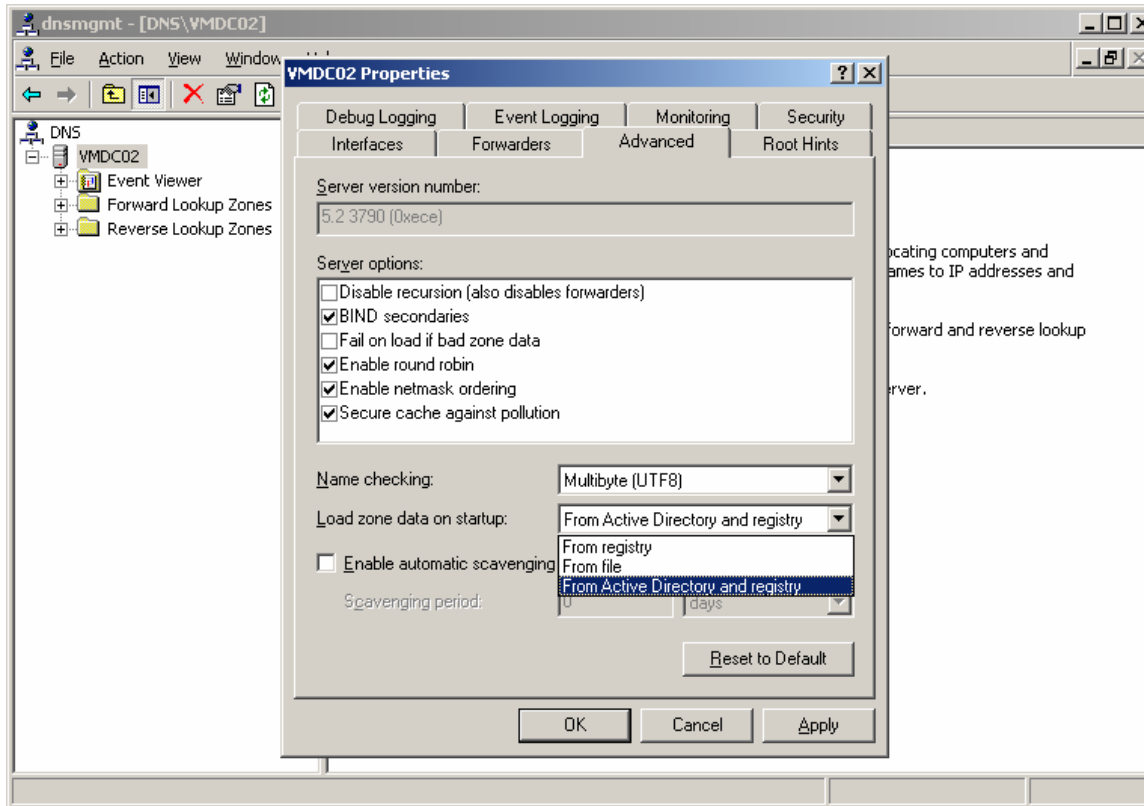
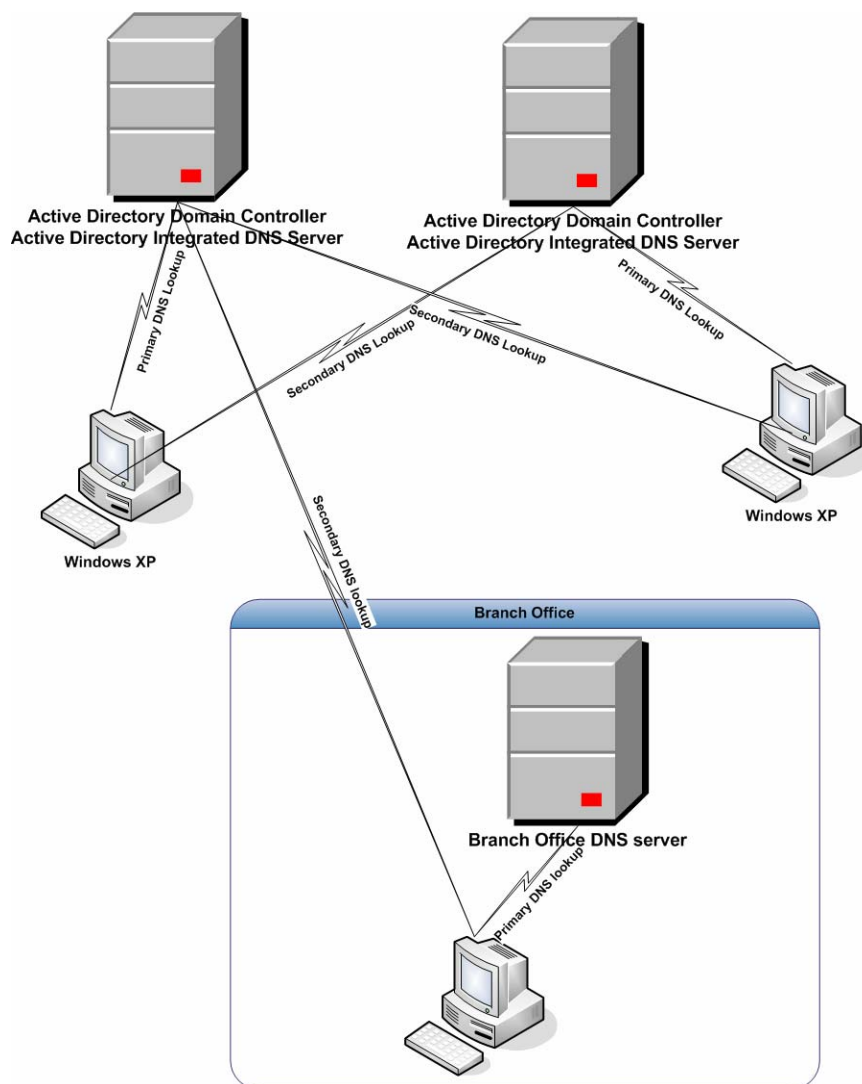


Figure 4.5: A domain controller running DNS can store its data in AD.

## Setting up a Robust DNS

Another way to ensure that your DNS will always be available is to ensure that you have multiple DNS servers at both the central office and the branch offices. One way to approach a robust DNS is to have each client machine have both primary and secondary DNS lookups as seen in Figure 4.6.



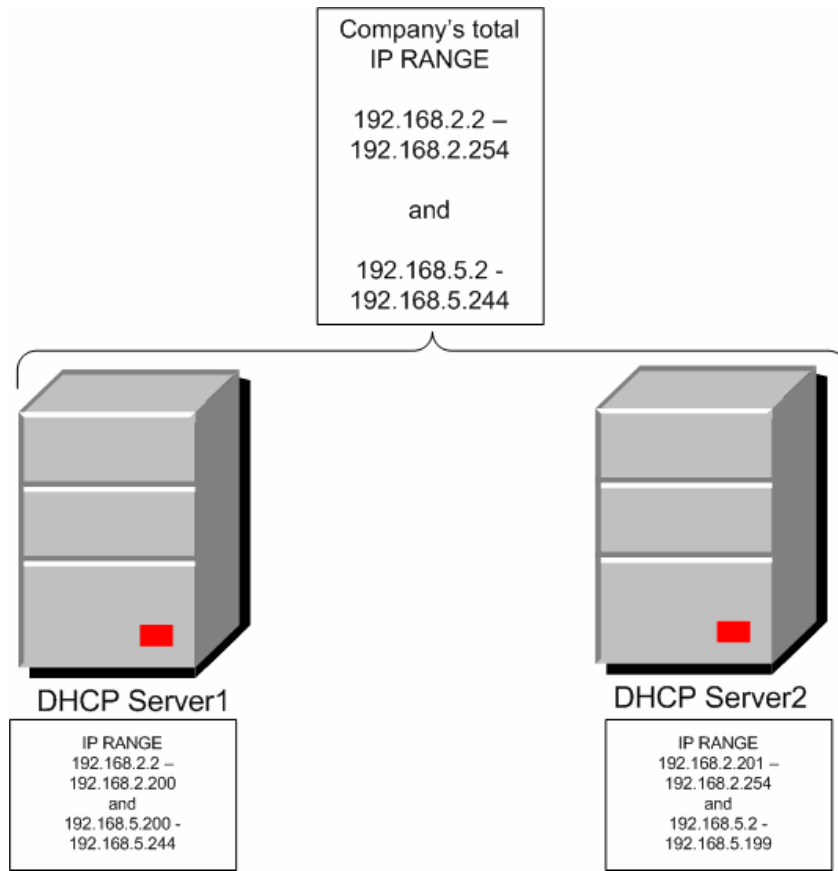
**Figure 4.6:** An effective DNS design deals with both main offices and branch offices.

In Figure 4.6, you can see that both the home office and branch office clients have both primary and backup DNS servers. Therefore, if any one DNS server should go down, DNS lookups can continue.

### **Multiple DHCP Servers**

Running multiple Dynamic Host Configuration Protocol (DHCP) servers on an enterprise network can be tricky. However, if you get it right, having multiple DHCP servers can be a lifesaver.

The best procedure for maximum uptime when it comes to DHCP servers is to spread your distributable IP address range among your servers. That way, if one server should fall ill, your distributable IP addresses can continue to function for at least a little while.



**Figure 4.7:** Use the “split” DHCP technique to have multiple DHCP servers share the IP range to distribute.

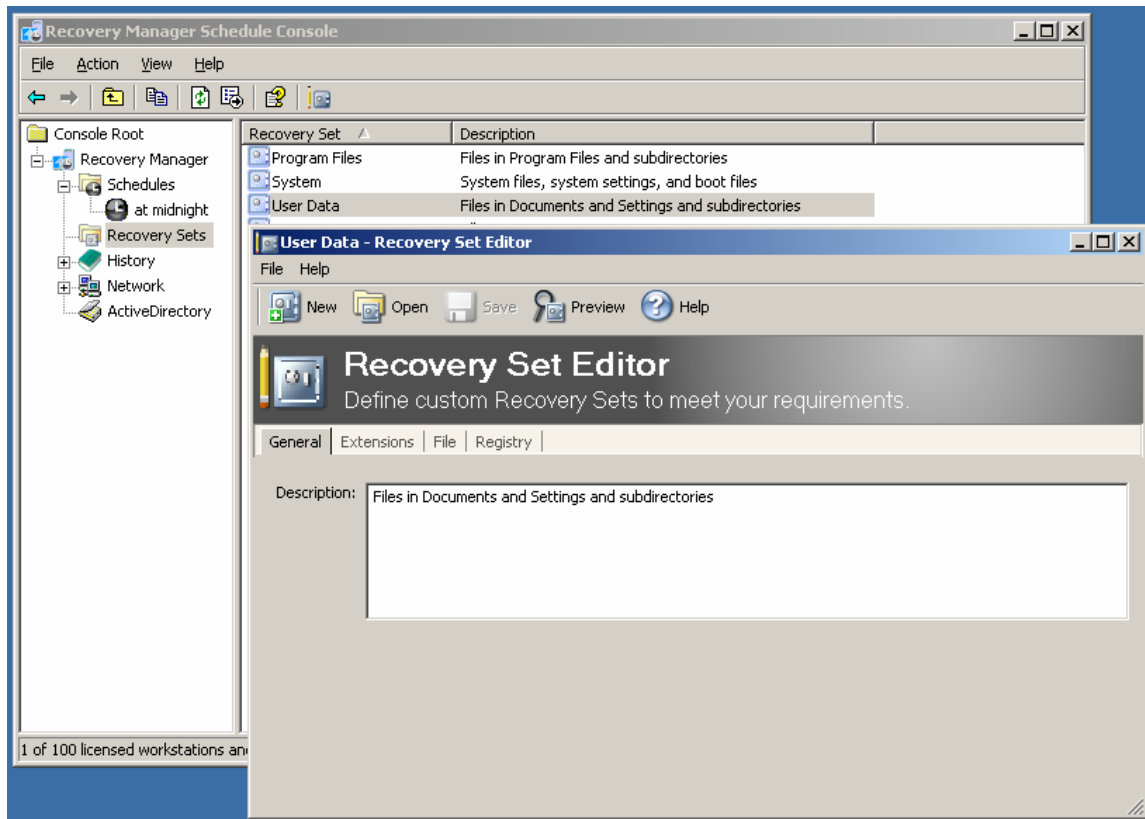
If you set up your DHCP servers in this fashion, you’ll be able to continue to give out a percentage of IP addresses in both ranges even though one server is currently down. Note that servers never “share” IP addresses; that is, there is no overlap. If you overlap IP ranges between servers, you’ll have a difficult time helping clients who try to register with the same IP address.

## Ongoing Data Backup

As we’ve explored multiple times in this book, protecting workstation data is a key component to ensure that you are able to get back in case of failure. To that end, this section will explore a handful of ways you can provide the ability to perform “ongoing data backup” to your users, to ensure that you can always help them get data back if need be. In addition to protecting the OS, you can back up data.

## Winternals Recovery Manager 2.0

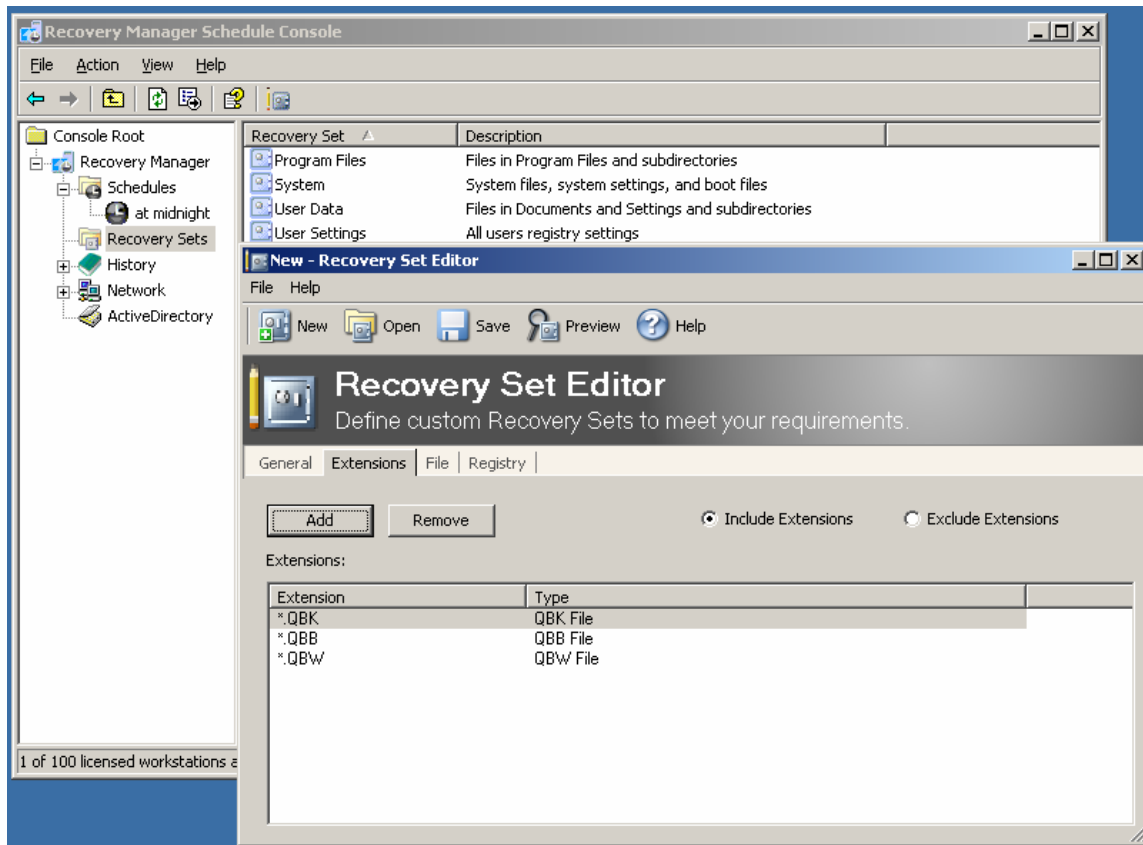
In addition to protecting the OS as discussed in previous chapters, Winternals Recovery Manager 2.0 provides ongoing data backup. Recall how Recovery Manager uses Recovery Sets. The idea is to dictate which directories and which files within those directories you want to frequently back up. Out of the box, Recovery Manager 2.0 will back up the user's Documents and Settings directory, as Figure 4.8 shows.



**Figure 4.8:** Recovery Manager 2.0 will back up users' Documents and Settings folders.

However, user data can be anywhere on the PC, so it might be a better bet to know which file types you want to back up. Perhaps the entire Office suite's file types, or AutoCAD file types, QuickBooks file types, and so on.

To that end, you should create new Recovery Sets for each of these designations. In Figure 4.9, you can see the creation of a new Recovery Set for QuickBooks file types: QBW, QBB, and QBK.



**Figure 4.9: Creating a Recovery Set for the files you want to back up.**

Then, simply capture these changed files from anywhere on the user's hard drive.

#### **On the Cheap: Offline Data Backups**

Not all companies back up all of a workstation's information. Yet, that is precisely where much company data is stored. If you don't want to invest in a third-party tool that can help back up desktops, you can take a more low-tech approach.

Specifically, you can set up offline CD-writing stations. That is, you can set up one or multiple PCs with CD-Rs or DVD-Rs attached. Users can copy their workstation data onto this removable media to ensure that they always have a copy of their data. However, there is the conundrum of how users will actually transport their data from their workstations over to these offline CD-writing stations. USB thumb drives are a perfect way to transport midsized chunks of data. A 512MB thumb drive can hold 73 percent of what a CD-ROM can hold. Thus, it can be an effective transport mechanism to get data off the user's workstation and on to the offline CD-writing stations.

However, it should be noted that this practice could be in violation of security policy. With that in mind, be sure to contact your internal security folks to make sure this method is an acceptable practice within your organization.

### Microsoft System Center Data Protection Manager

Microsoft has a new product, System Center Data Protection Manager (DPM), that is the company's first tool to help administrators make continuous backups of data on servers. Additionally, users are given the power to restore data themselves via "self-service." This functionality is part of the Shadow Copies feature that earlier chapters explored. In other words, if users need to get to a previous version of a file, they can do so themselves.

The idea of DPM is to aggregate data that already exists on file servers and ensure that the data is constantly backed up. Then, via third-party products that hook in to DPM, the data is archived in a permanent fashion (see Figure 4.10).

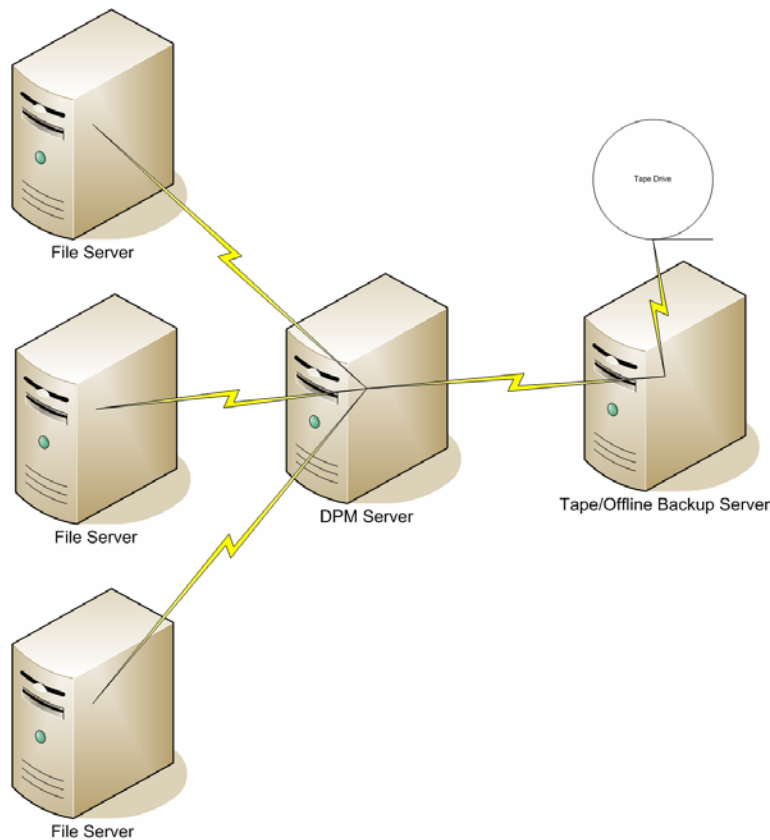


Figure 4.10: The Microsoft DPM server architecture.

The DPM server doesn't actually perform archives to tape. That's where either NTBACKUP or third-party products come in. The following list highlights how DPM and the tape backup server interact:

- Imagine on File Server 1, Joe creates a 50MB Word file on Monday.
- On Tuesday, Joe changes 10 words and saves the file. With traditional backup software, the entire 50MB file would be saved to tape.
- Instead, DPM copies only the differences in the file—perhaps only 1MB or 2 MB of changes, and stores those changes in the database.
- Finally, a tape backup program (NTBACKUP or a third-party tool) hooks into DPM and pulls only the changed files and saves them to tape. NTBACKUP backs up the entire changed file. Third-party tools may be able to back up just the changed data.

This strategy has an extra benefit. That is, organizations that are in a time crunch to get the entire backup performed within 24 hours now have a reduced strain. That is, because you're only backing up the changed bytes in a file, the entire backup operation is more efficient.

When data needs to be recovered—it can be recovered quickly via the DPM server, which pushes the data back to the appropriate file server. DPM has several ways to back up data on servers: full, incremental, snapshot, or a mix.

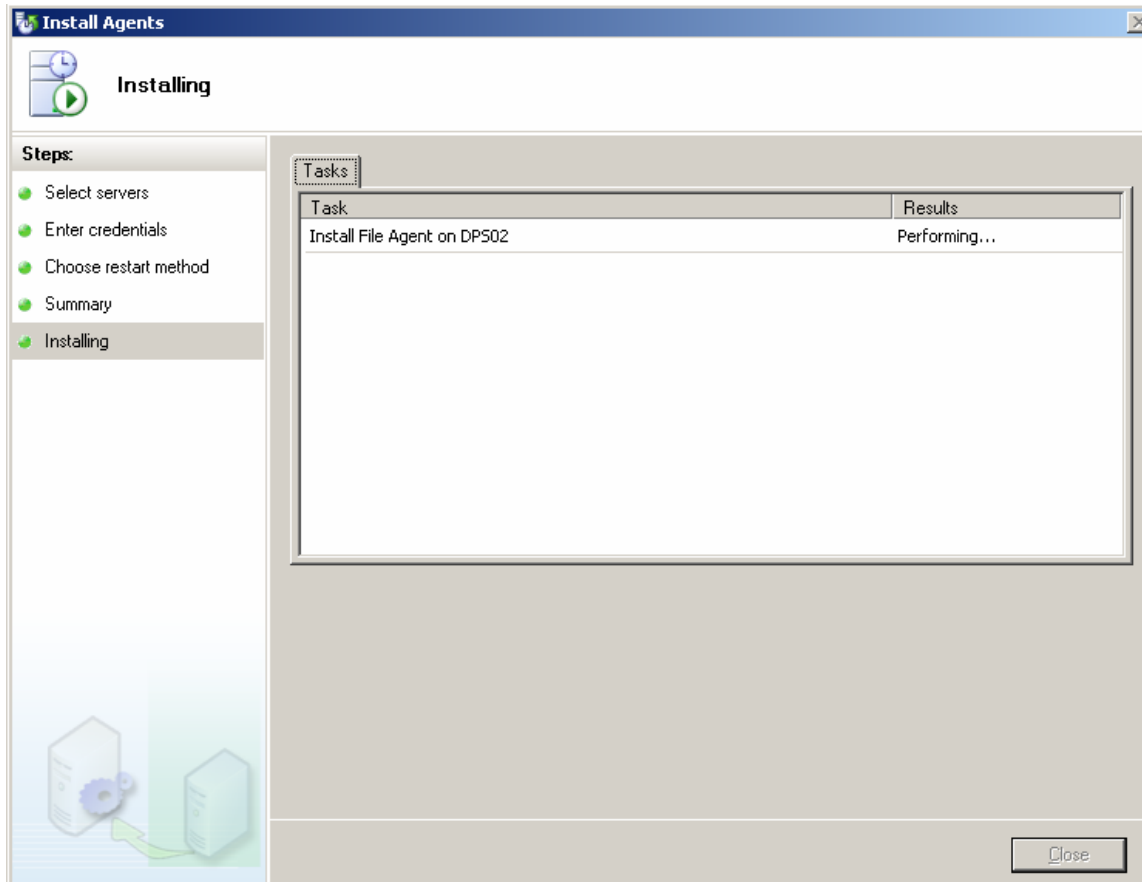
### DPM Nuts and Bolts

DPM resides on a dedicated Windows Server 2003 (WS2K3) machine. Additionally, that machine must have SQL 2000 (or the provided SQL 2000 trial). Finally, the DPM setup wizard installs the application and the required prerequisite software.

You also need a suggested 1GB of RAM on this server, as it's got a lot to do: backup and restore files and manage a huge database. Finally, you need a disk big enough to hold your backup. Then triple it. The idea is that you need a disk 2 to 3 times the size of your current data set. That way, previous versions of a file can be recovered at a moment's notice. Of course, having a SAN here is most helpful, though not required.

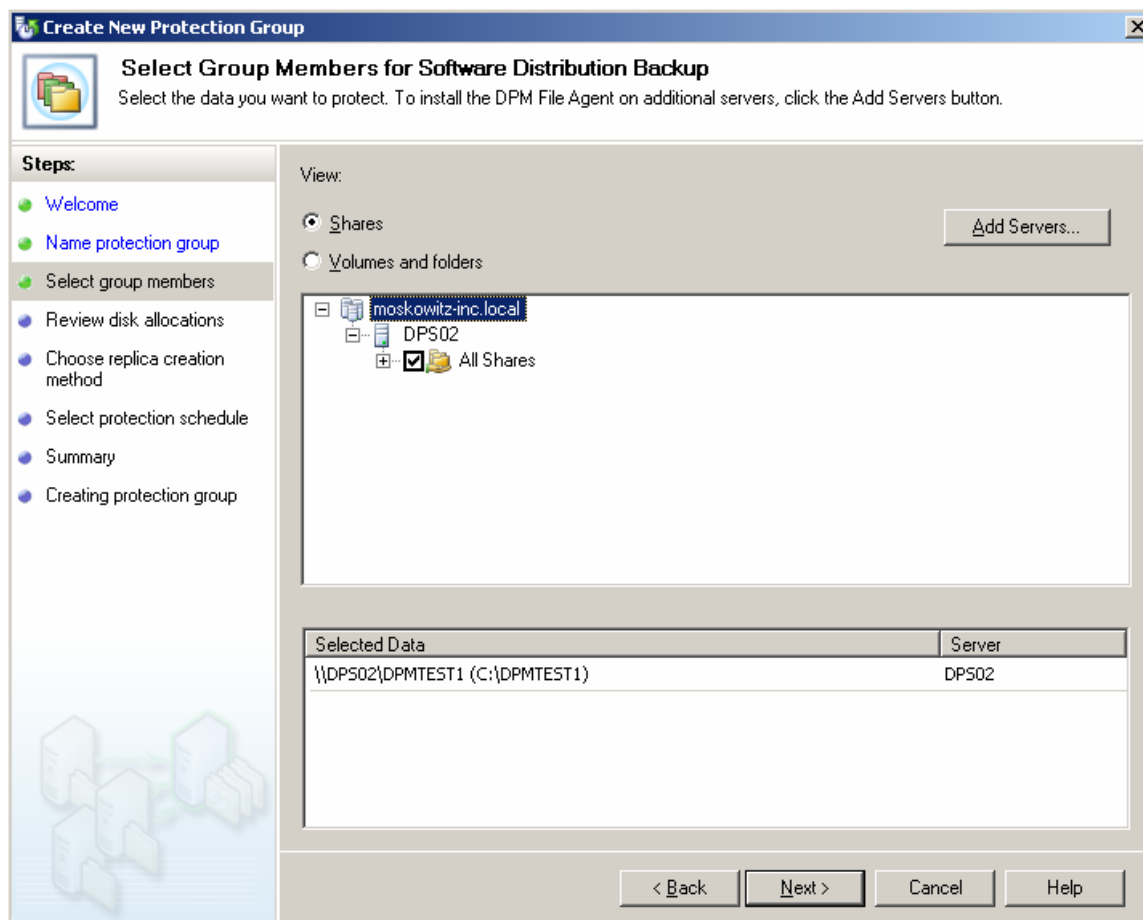
👉 Upon installation, DPM looks for an "unused" or unformatted disk to store the data. It uses its own "disk type" and automatically formats and utilizes the unused disk.

Once the DPM server is installed, you need to put the agents on the file servers. The DPM administrator console performs this task for you and is handled nearly automatically as Figure 4.11 shows.



**Figure 4.11:** You can remotely deploy the agents to your file servers.

After agents are installed, you have the ability to specify which shares on those servers you want to back up. Figure 4.12 shows how to specify to backup All Shares on a server named DPS02.



**Figure 4.12:** You tell the DPM server which shares on which file servers you want backed up.

Additionally, you can specify how often the DPM server should grab the data from each protected server and create shadow copies, as seen in Figure 4.13.

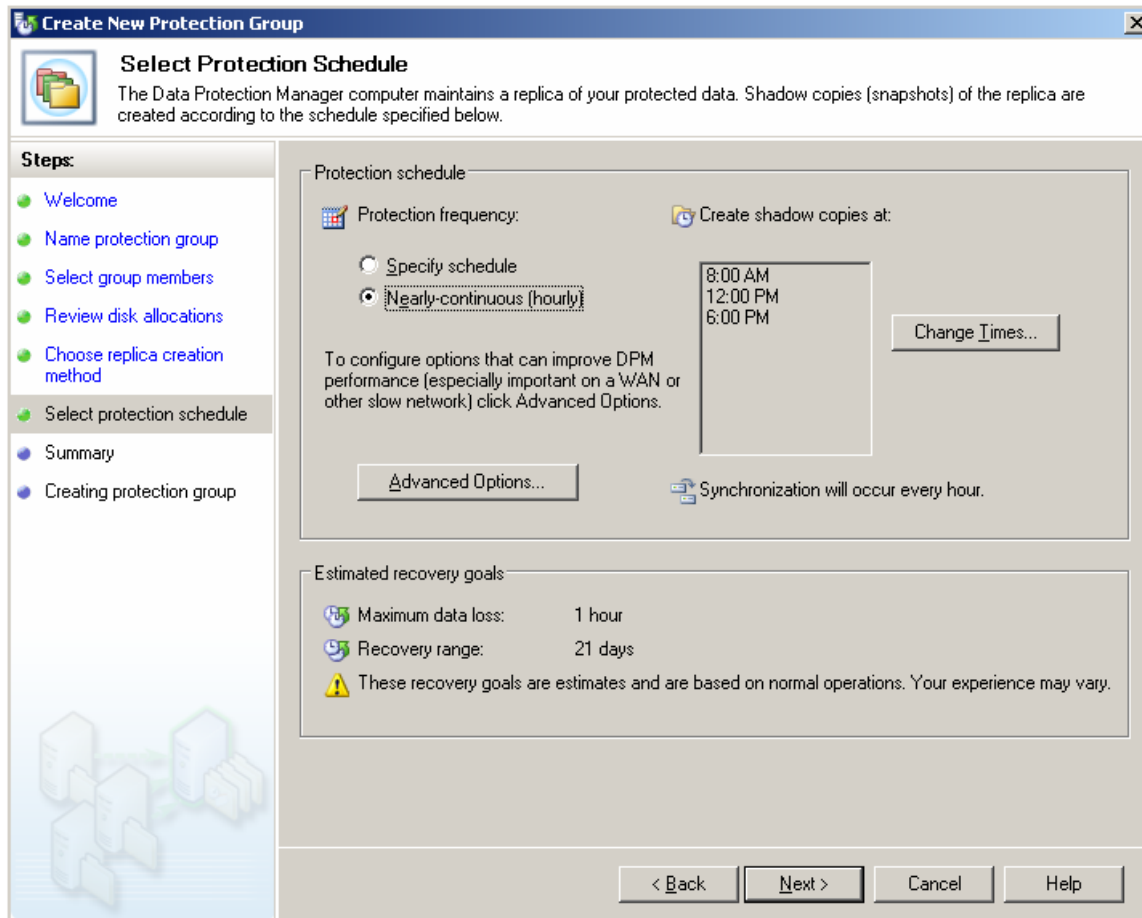


Figure 4.13: You can tell DPM how often to take snapshots of files on protected servers.

## DPM Benefits

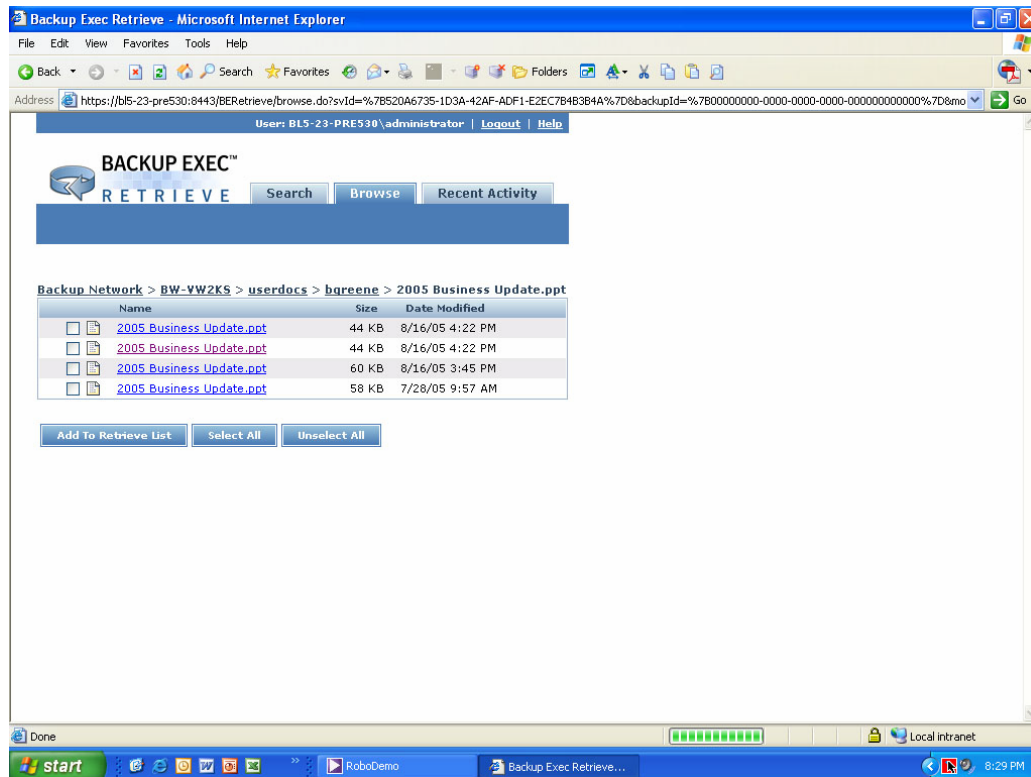
One of the key benefits is that users can restore their own files. Recall in earlier chapters how we saw users restore their own files with the Shadow Copies client. The best news is that there is a shadow copies client update that hooks into DPM. In other words, users can continue to use the same procedure to restore files. The update is available at <http://support.microsoft.com/default.aspx?scid=kb:en-us:903234>.

## DPM Day-to-Day

The Microsoft DPM solution is a good solution, but could still use further development. For instance, today, it's only a really viable option for file servers. Application servers, such as Exchange, SQL, or any custom applications aren't good candidates as DPM clients. These kinds of machines typically keep their data not in straight files, but rather, as databases or open files that DPM doesn't handle at all.

## Symantec Backup Exec 10D with “Retrieve” Software

A well-known player in the backup and recovery game is Symantec, who now owns VERITAS. The Backup Exec family of products is popular with archiving data to tape. However, the newest Backup Exec 10D has the ability, like Microsoft’s DPM, to also make snapshot backups and keep them available for quick recovery. One of the major benefits of Backup Exec 10D is the ability to perform self-service restores via a Web-interface, as Figure 4.14 shows.



**Figure 4.14:** BackupExec 10D has a Web-based restore feature for users.

Backup Exec Retrieve, has a simple Google-like Web-based retrieval system that lets user retrieve their own files. Because Backup Exec Retrieve is Web-based, there is nothing to load on the client.

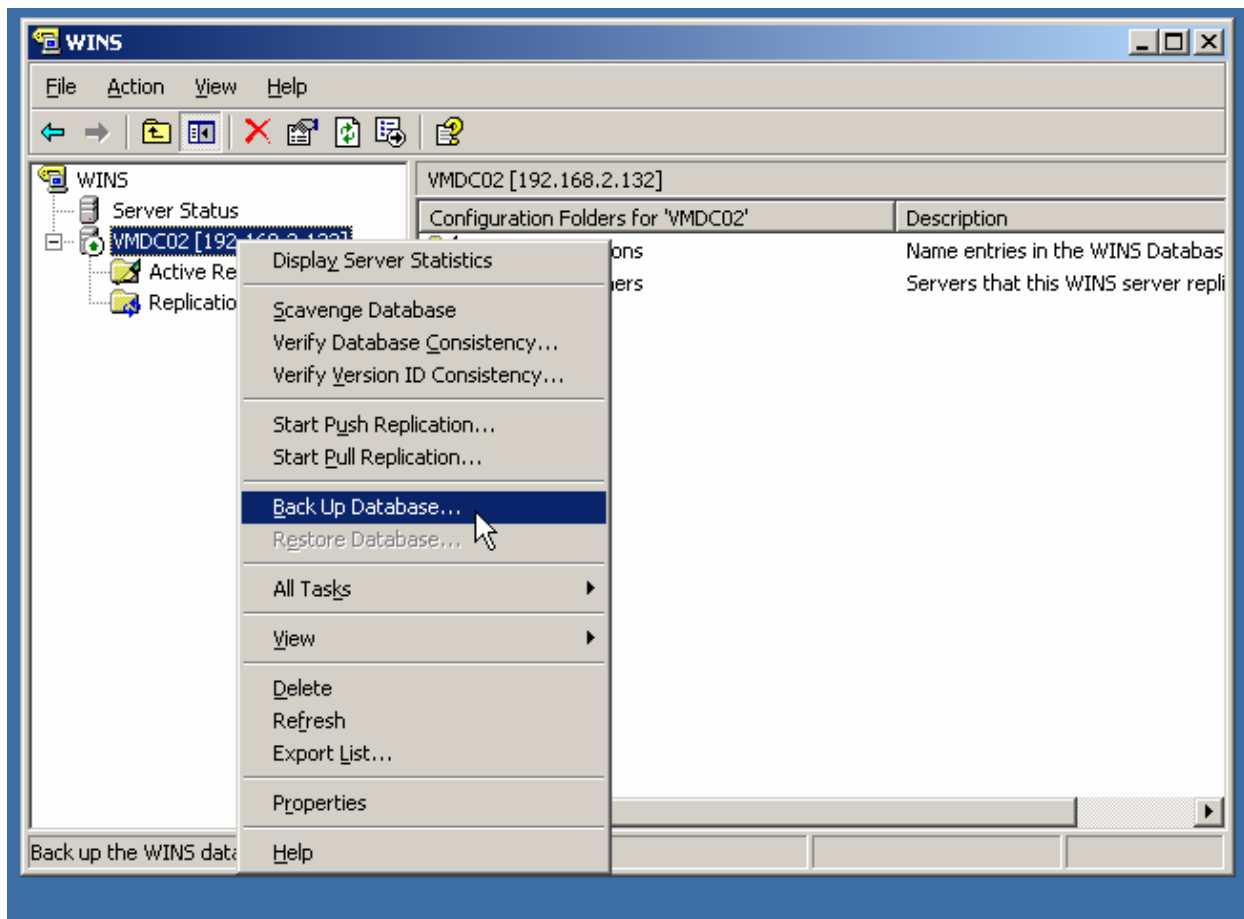
## Additional Preventative Maintenance: Backup of AD Support Structure

Earlier, this chapter talked about best practices to ensure that the key components of AD are redundant. However, redundancy isn't enough. You need to also back up this data in case of a major failure of some kind.

### ***WINS Backup and Restore***

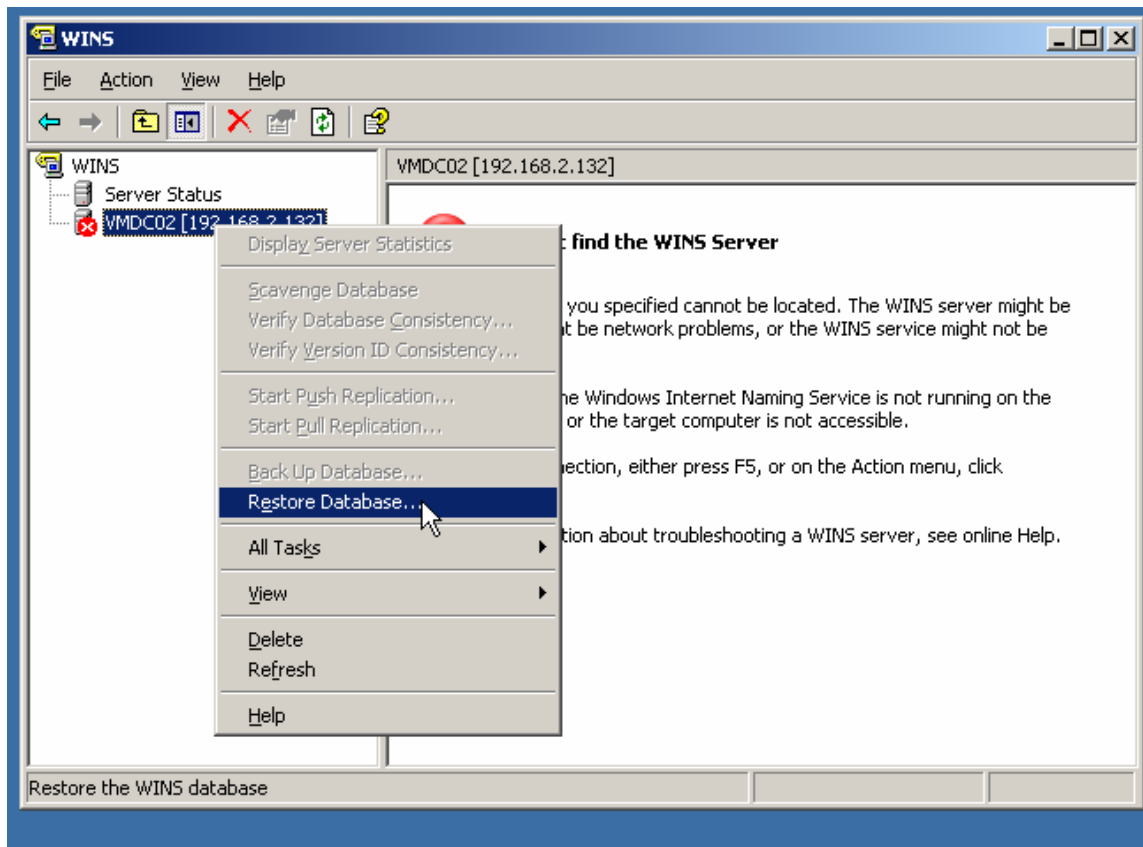
As we explored earlier in the chapter, having redundant WINS servers is useful in case any one WINS server should go down. However, if the data itself becomes corrupted and is replicated to all the partners, you'll have problems.

To that end, WINS is easy to backup. Simply right-click the WINS server name in the WINS manager, and click Back Up Database as Figure 4.15 shows.



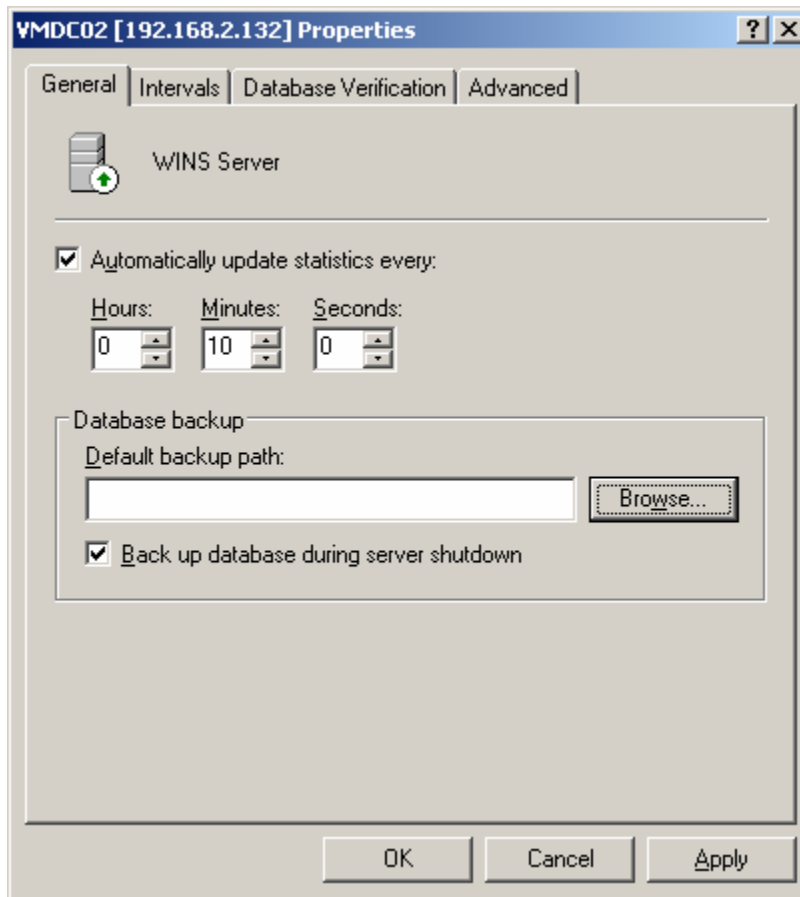
**Figure 4.15:** You can back up the WINS data using the built-in backup tool.

However, should it become necessary to restore the WINS server database, it should be noted that the WINS server needs to be stopped. Once the WINS server is stopped, you can opt to choose Restore Database option as Figure 4.16 shows.



**Figure 4.16:** When WINS is stopped, use the WINS manager to restore the database if necessary.

You can also tell WINS to automatically back up the database. To do so, right-click the WINS server name, and select Properties. On the General tab, select the *Back up database during server shutdown* check box (see Figure 4.17).

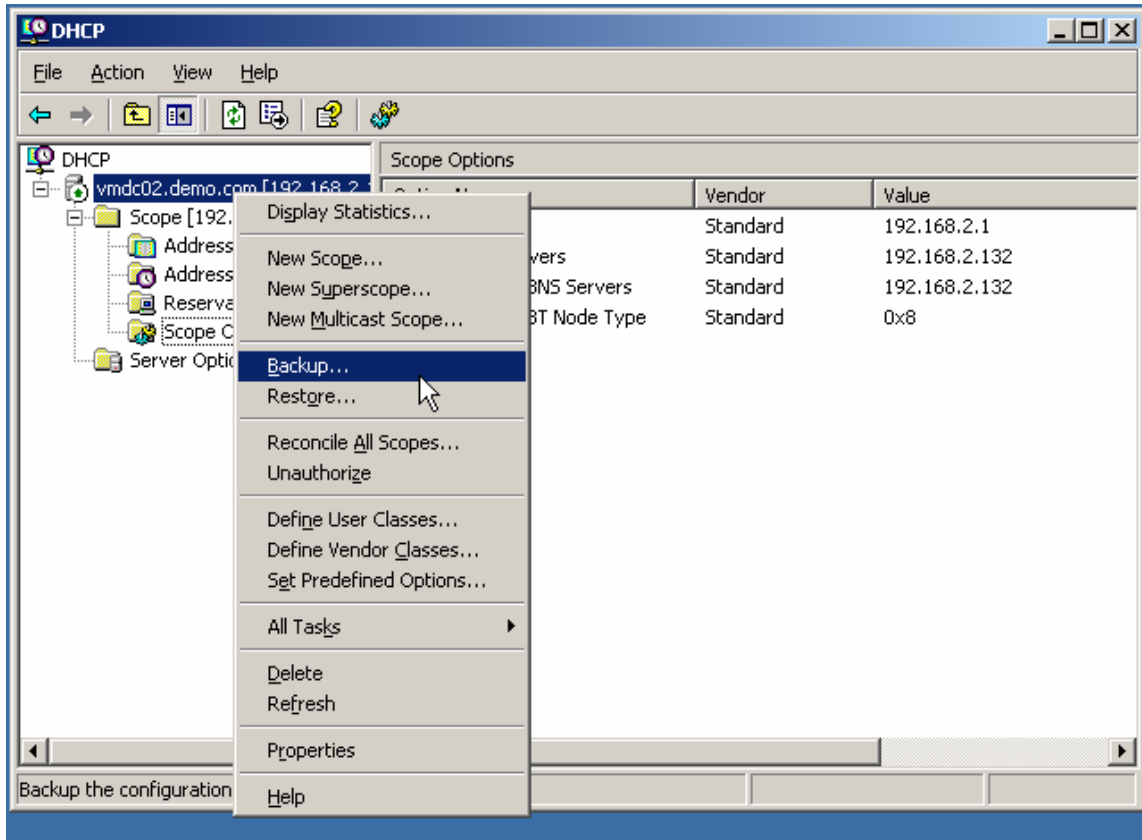


**Figure 4.17:** The WINS properties on the General tab holds key WINS settings.

Be aware that this *Back up database during server shutdown* check box is a bit misleading. Although it implies it performs the backup only during a server shutdown, it also performs the task every 3 hours. The resulting files are found in `\Windows\system32\WINS`.

### DHCP Backup and Restore

Backing up and restoring any DHCP server is similar to backing up and restoring WINS. That is, the facility is built-in to the DHCP manager. Simply right-click the server name, and select Backup, as Figure 4.18 shows.

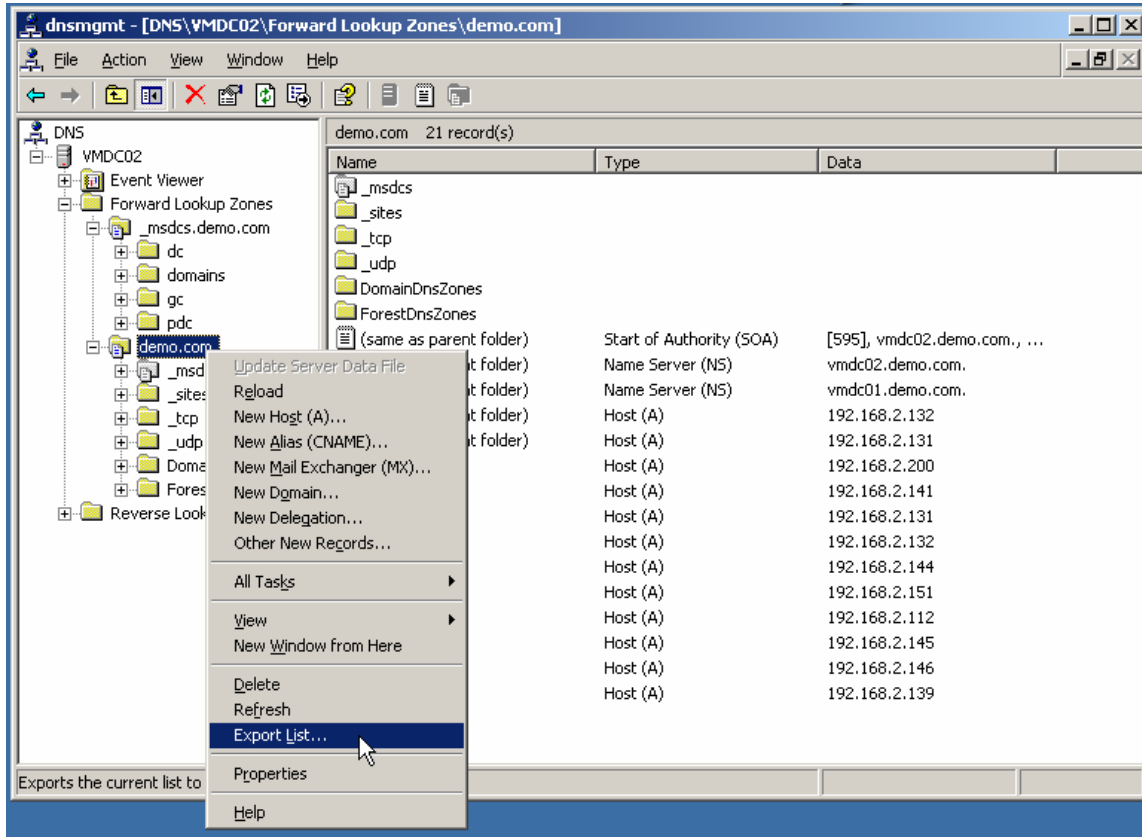


**Figure 4.18:** The backup and restore facility for DHCP is built-in to the DHCP manager.

If you need to perform a restore of the DHCP database, the procedure is slightly different than, say, restoring WINS. Specifically, the service doesn't need to be stopped manually in order to utilize the restore function. The restore function will automatically stop the service, restore the database, and restart the service.

## DNS Backup and Restore

Producing a proper backup of a DNS server can be a little bit of a chore. In the DNS manager itself, you can, if desired, right-click a specific zone, and select the Export List (see Figure 4.19).



**Figure 4.19:** You can export any DNS zone to a flat text file.

However, the only problem with this method is that you need to do so once for every zone you have in AD. Some AD implementations have one or two zones, so this requirement isn't a big deal. However, multiple-domain AD implementations will see multiple zones, making this process a tedious task.

## Understanding Tape Backup Types

Which way is the best way to perform tape backups? There is no “best” way to perform tape backups. However, with a little education, you can make your own decisions about how to best perform your backup. Let’s start with a rundown to help you understand the various backup types available out of the box.

### Getting to the Backup Types

To discover your potential backup types, you must first fire up NTBACKUP. Once up and running, select a gaggle of files to backup and click Start Backup. When you do so, the Backup Job Information appears; click Advanced to access the Advanced Backup Options properties page (see Figure 4.20). Once here, you can see the various backup types available.

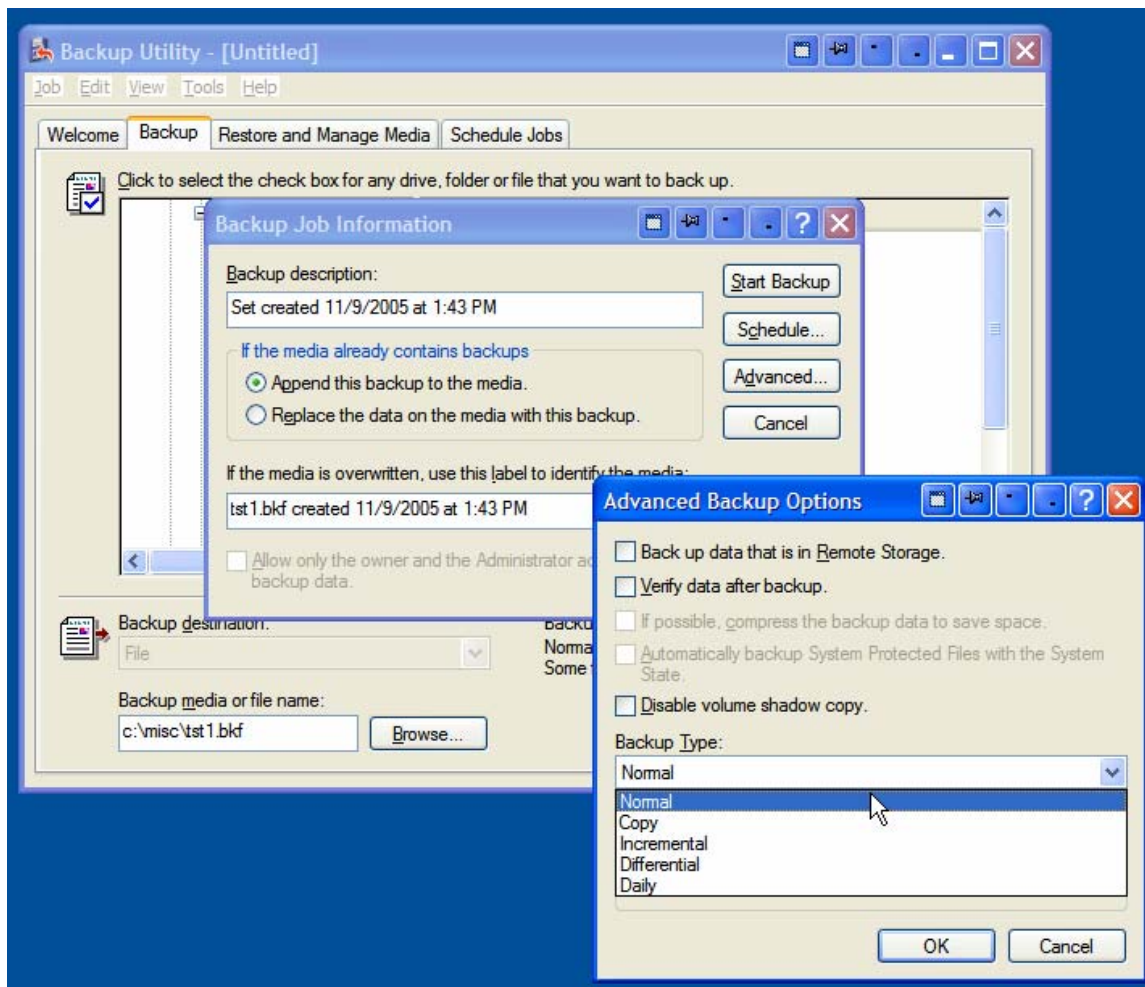


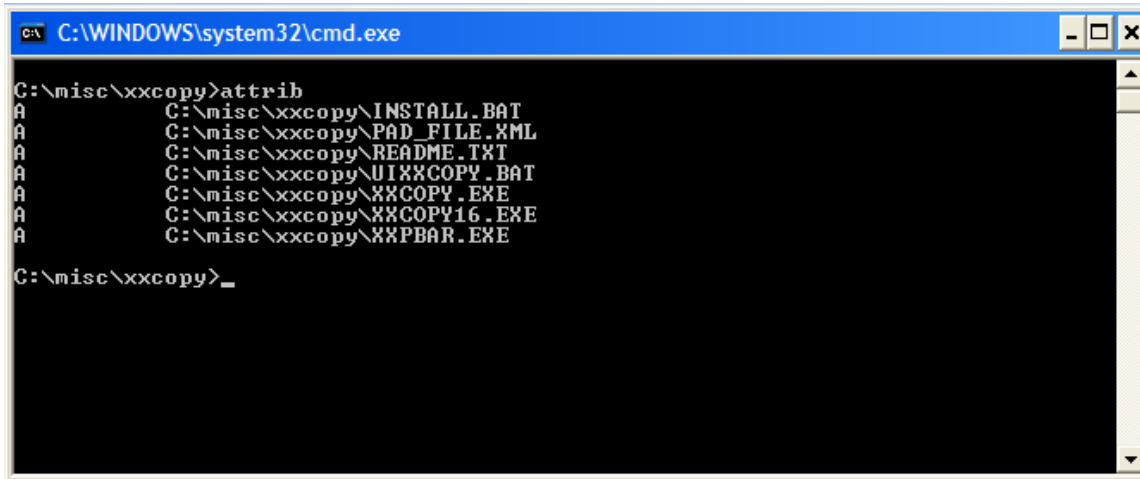
Figure 4.20: NT Backup has several backup types.

### Understanding the Archive Bit

Windows has a rudimentary way to keep track of which files need to be backed up. To do so, it uses what is called the Archive bit, or “A” bit. You can see this by using the command prompt, traversing into your favorite directory, and typing

```
attrib
```

When you do, you’ll see that some (or all) files have the A attribute set as seen in Figure 4.21.



```
C:\WINDOWS\system32\cmd.exe
C:\misc\xxcopy>attrib
A          C:\misc\xxcopy\INSTALL.BAT
A          C:\misc\xxcopy\PAD_FILE.XML
A          C:\misc\xxcopy\README.TXT
A          C:\misc\xxcopy\UIXXCOPY.BAT
A          C:\misc\xxcopy\XXCOPY.EXE
A          C:\misc\xxcopy\XXCOPY16.EXE
A          C:\misc\xxcopy\XXPBAR.EXE
C:\misc\xxcopy>_
```

Figure 4.21: Any new files written to the disk will automatically get the [A]rchive bit set.

If the A bit is set, the file still needs to be backed up. This information is helpful as you try to understand the types of backup options available.

### Understanding the Backup Types

As you can see in Figure 4.20, there are many backup types available. The reason there are many backup types is so that you can finely tune how you perform backups. Let’s take a minute to explore each of these options.

#### Normal

Normal backups produce a full backup of all the files selected. It doesn’t matter when those files were last backed up; this backup type will ensure that they are on the tape. The downside to this option is that if you backed up the file yesterday, and the file hasn’t changed today, you now have two exact backups of the same file. In doing so, you wasted time, space on your tape, and the percentage cost of that tape that you used. Once a file is backed up the [A]rchive bit is cleared, meaning that it no longer needs to be backed up.

#### Copy

A copy backup is like a Normal backup, except the [A]rchive bit is never cleared. This allows you to take, perhaps, an interim backup during the day, which won’t disturb the normal backup cycles that differential or incremental backup types would need.

## Differential Backups

Instead of backing up every file every day with the Normal backup, consider a differential backup. The idea is that because a Normal backup clears the [A]rchive bit, only files that still have the [A]rchive bit set need to be backed up. With a differential backup, the files that have the [A]rchive bit set will be backed up but the files keep their [A]rchive bit even though they've been backed up so that the next Normal backup will also include these files.

## Incremental Backups

An incremental backup finds the files with the [A]rchive bit set and backs them up. It then clears the [A]rchive bits on the files it backed up.

## Daily Backup

Daily backups take a look at the file modification dates on a file. If the modification date is today, the file is backed up.

### *Differential vs. Incremental*

Clearly, a differential and incremental backup can help squeeze more efficiency in your backup. But which one should you use, and when? Let's examine both cases to see where they're each useful. In all cases, let's assume you backed up all your data on a Monday. Therefore, the archive bit will be cleared.

## Differential

Let's assume you decide to back up Tuesday and Wednesday and Thursday:

- When you do so on Tuesday, you're backing up what has changed between Monday and Tuesday.
- When you do so on Wednesday, you're backing up what has changed between Monday and Wednesday (this includes Tuesday).
- When you do so on Thursday, you're backing up what has changed between Monday and Thursday (this includes Tuesday and Wednesday).

Thus, each day, it will take longer and longer to back up your environment, because, presumably, each day more data has changed since Monday. When it comes time to perform a full restore, however, you'll need two tapes: Monday (the full backup) and the day you want to recover. That's because you're restoring the full "baseline" and then what has changed on that one tape.

## Incremental

Let's again assume you decide to back up Tuesday and Wednesday and Thursday:

- When you do so on Tuesday, you're backing up what has changed between Monday and Tuesday.
- When you do so on Wednesday, you're backing up what has changed between Tuesday and Wednesday.
- When you do so on Thursday, you're backing up what has changed between Wednesday and Thursday.

Thus, each day it will take a pretty short time to back up your environment because, presumably, each day you're changing about the same amount of data. However, when it comes time to perform a full restore, you'll need *all* the tapes leading up to the disaster. If your disaster happens on a Friday, and you want to restore back to Thursday, you'll need: Monday (full), Tuesday (incremental), Wednesday (incremental), and Thursday (incremental). Without all the tapes, you won't have a full record and won't be able to fully restore.

## Summary

Let's take a quick review of the key points you should have learned in each chapter of this guide:

Chapter 1:

- Use NTBACKUP. It's in the box, and it works.
- Automate your backups. You're only as protected as your last backup.
- Use ASR to take a live "snapshot" of your system.
- Use System Restore, ERDisk, or another tool to help return a system to health.
- Use a tool such as Winternals Recovery Manager to roll back specific files.

Chapter 2:

- Use Volume Shadow Copy to maintain copies of users' data files.
- Use the Previous Versions Client to enable users to get to their Shadow Copies.
- Use a Password Recovery tool if you need to.
- Use an Account Password recovery tool if you need to.
- Understand your Windows repair options: Last Known Good, Safe Mode, Recovery Console, and SFC.

Chapter 3:

- Back up the System State to get the “nucleus” of the system.
- Use Non-Authoritative and Authoritative restores to recover domain controllers and accounts contained within domain controllers.
- Remember that tombstone reanimation doesn’t recover all attributes from a deleted user.
- An AD Lag Site might help you recover accounts quicker.

Chapter 4:

- Plan for disaster by having redundancy built-in to your network.
- Keep an ongoing backup of your data; doing so reduces your required backup window and allows you to recover quickly.
- Back up your AD support structure such as WINS, DNS, and DHCP.
- Know which backup type to use: Normal, Copy, Differential, Incremental, or Daily.

Be vigilant and plan for disaster and consider all the possibilities to ensure that you have the best backup possible—and above all test your plan!