

# CHAPTER 6

## *Management*

### **In This Chapter:**

- Migrating a Windows Installation to a Similar Computer
- Modifying NTBACKUP Behavior
- Backing Up and Restoring the Remote Storage Database
- Backing Up and Restoring IIS Installations
- Recovering the ASR Floppy from an ASR Backup Set
- Increasing GPO Logon Performance
- Troubleshooting Global Policy Object Behavior Using Logging and Tools
- Upgrading Windows 2000 Group Policies for Windows XP Professional Clients
- Repairing a Missing Default Domain Controller Policy on a Windows 2000 Server
- Performing Scripted Administrative Tasks on GPOs
- Cleaning Up Temporary Files in User Accounts
- Reinstalling TCP/IP in Windows 2003

**M**anagement is one of those catchall terms for computers. Depending on who you talk to, the definition can vary quite a bit, so to avoid confusion, I'm going to take the time here to describe exactly what we mean by "management"—and to that end, what this chapter will cover.

The way I see it, "management" is everything you do to a PC that doesn't involve setting it up or using it. This includes backups, preventative maintenance, policy and password control, security, and some forms of repair (including repairs to the preceding functions). I've also decided to discuss migrating Windows in this chapter, partly because migration is often done as part of other management tasks.

Policies are a fairly major Windows administration subject. As per the general theme of this book, I haven't tried to explain what they are or how they work or how to use them. I've limited my discussion of policies to behaviors that are either undocumented or not well understood. I've also set aside pages to cover policies as they relate to mixed environments—where Windows 2000 and Windows XP Professional machines coexist.

Another major subject covered in this chapter is backup operations—specifically, enhancements and tips that involve undocumented features or behaviors of the NTBACKUP tool and System State Backup function. This includes backing up and restoring such things as the Remote Storage database, or making offline backups of the IIS configuration.

2000/2003

## Migrating a Windows Installation to a Similar Computer

High

Moderate

Low

Moving a Windows installation from one machine to another is slightly complex, but some of Microsoft's own tools, in conjunction with a little ingenuity, can cover the distance.

### Overview

Administrators do not tend to think of Windows as being portable. Once installed on a given piece of hardware, Windows stays there until it is upgraded or until the machine itself is decommissioned. But the reality is different for many Windows machines, workstations, and servers. Often, administrators face the prospect of upgrading a Windows machine while preserving the Windows installation on board.

Sometimes this is the best way to go. Most administrators would rather migrate an existing Windows server with all of its user accounts, software, and tweaks than go through the agony of reinstalling everything anew on a brand-new computer. Client workstations are another story, since they are usually reimaged using a utility like Ghost or DriveImage. Servers, however, tend to be tougher to deal with since they are not usually created from a central repository of images (and in the case of domain controllers, they can't be!).

## The Party Line

**Company X**

Windows is designed to stay put on one system the vast majority of the time. Microsoft does provide some details about cloning, but moving an intact system to another hardware setup—software, data, drivers, and all—is a step up from cloning.

### *The Undocumented Solution*

*Unfortunately, migrating a Windows installation from one machine to another isn't always a straightforward process. Like the proverbial cat-skinning, there's more than one way to do it.*

Here are three common methodologies for migrating Windows to new hardware:

- *Migration via system image.* This involves making an image of the contents of the system's hard drive—to tape, CD-R/W, DVD, a network repository, or directly to another hard drive—and using the image to re-create the system.

This approach is probably the slowest of the three, since it involves copying everything twice—once to the image media, and then a second time to the target system. One major advantage to this method is safety: the copied image serves as a system backup, and the original system disk remains untouched. Another advantage is that any number of other systems can be produced from the original image, and further copies of that image can also be made. Finally, the type of media used is totally up to the administrator, although the imaging software may restrict one's choices. The most commonly used imaging program, Symantec Ghost, has a broad range of media choices; everything from CD-R to a network repository is supported. There's also Microsoft's own SYSPREP, which is covered in some detail later in this segment.

- *Migration via direct copying.* The hard drive for the target system is installed in the same machine as the source system, and a utility is used to copy the contents of the source drive to the target drive. The target drive is then placed in the target system and booted.

This approach is slightly faster than system imaging—disk-to-disk copying is faster than copying to tape or another medium, because one, and only one, stage of copying is needed. The original disk also remains untouched, which is useful in the event the target drive turns out to be defective or some other disaster

rears its head. Because of the speed and the convenience, this method is my own personal favorite. A number of inexpensive-to-free utilities for doing disk-to-disk imaging are out there, such as BootIt Next Generation (free) and the Western Digital Data Lifeguard Tools (free, but only usable with Western Digital drives). Note that there is a timeout required to bring the system down and insert the other disc, but this is generally less than the timeout required to image the system using a non-Windows tool.

- *Direct migration.* The hard drive for the source system is placed directly into the target system and booted.

This is the fastest method, but it is also the riskiest. For one, if anything happens to the original drive or the Windows installation on it, the damage will be irreversible. However, there is a way to minimize the risk involved—by creating a separate hardware profile for the migration process.

Follow these steps to create a separate hardware profile:

1. Create a new hardware profile and boot into it. In both Windows 2000 and Windows 2003, right-click *My Computer*, select *Properties*, then the *Hardware* tab, then click the *Hardware Profiles* button to bring you to the window shown in Figure 6-1.

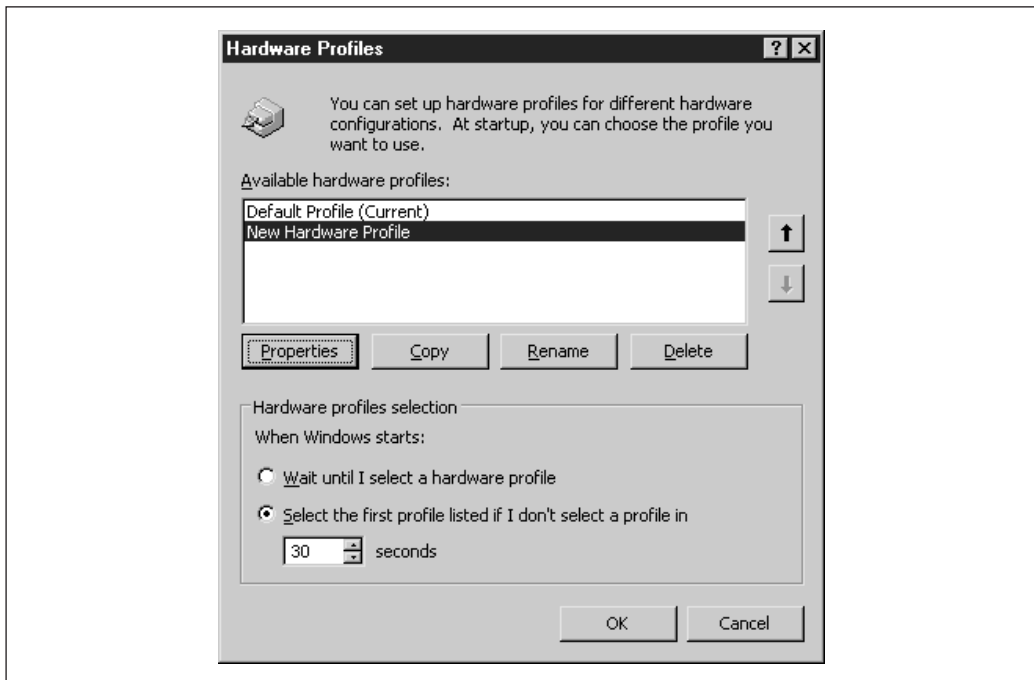


Figure 6-1. The Hardware Profiles menu in Windows 2000

2. Click Copy to create a new profile. Choose a name for it (it doesn't need to be unique, but it does need to identify the hardware profile for your sake), and then click OK on each window to close it out.
3. On your next reboot, you will be prompted to choose which hardware profile to use. Select the new one.
4. If the new system uses a different mass-storage controller driver than the one currently installed, install it using the manufacturer's installation procedure. This particular step can *sometimes* be omitted if the target system uses the default ATAPI/EIDE controller driver—for instance, if Windows is being moved to an IDE drive. If the existing system uses the same controller type, then you don't need to change this at all.

---

**NOTE** Not all ATAPI/EIDE controllers are created equal, and not all of them will work correctly with the default ATAPI.SYS driver installed by Windows. Some of them require their own custom controller driver (such as controllers by Promise Technologies or VIA). However, most of them will work well enough to get through the migration process. The default driver may simply not support the more advanced features of that controller—the controller may default to PIO (programmed I/O) mode rather than UDMA (Ultra DMA) and may run more slowly. If the system seems to be unusually sluggish after the migration process, this is the most likely reason why.

---

5. Move the Windows installation to the new drive, or transplant the drive into the new system if you are using that strategy.
6. Boot on the new system, using the new hardware profile. If something goes wrong during the migration, you can put the drive back into the old machine (if you've chosen to move drives) and boot using the original profile. Any hardware changes will be recorded only to the second hardware profile.
7. Once Windows is up and running again on the new computer, the old hardware profile can be deleted.

The reason for this is simple: by confining any detected hardware changes to the alternate profile, it becomes much easier to recover from problems. If the new system refuses to boot, or boots but experiences problems, the hard drive can be restored to the original system and then Windows can be rebooted using the original hardware profile with little or no problems.

---

**NOTE** Another suggested trick when performing this hardware-to-hardware migration is to switch the system HAL from ACPI to Standard PC, which ensures that it will work on a broader variety of hardware. When the migrated system is stable, it can be switched back to ACPI.

---

From what we've seen, all of these migration approaches have a common denominator. Windows often doesn't deal well with highly radical and sudden

changes in system configuration—doubly so now that Product Activation in Windows 2003 uses the hardware configuration as an indicator of whether or not the product has been licensed for that system.

To minimize the problems involved, the administrator doing the move should consider using the SYSPREP tool. SYSPREP is a Microsoft utility that prepares a Windows 2000 or 2003 system for cloning or imaging. Because of the way Windows 2000/2003 installations are uniquely identified, both in the software and the hardware, simply moving a Windows installation from one machine to another may not work. The main culprit is the system security ID, which cannot be easily replicated.

The system may become unbootable or may behave unpredictably. To make sure the transfer works, one way to handle it is by using SYSPREP to force Windows to redetect the hardware tree before physically moving the system. In other words, SYSPREP has to be run before any imaging, copying, or drive reinstallation takes place. Once it's run and the Windows installation is migrated to the new hardware, the system reboots, redetects the hardware in the system, re-activates if needed (in Windows 2003 only), and the administrator can continue where he left off.

---

**NOTE** SYSPREP cannot be used to clone domain controllers, either for Windows 2000 Server or Windows 2003 Server. A cloned system must be a stand-alone server, or must be demoted to being a stand-alone server beforehand. Because this is difficult to implement practically, there are a couple of approaches to moving a domain controller. One of the easiest is to set up a new server and add it to Active Directory as a domain controller, then move the Operation Master and Global Catalog roles to the new machine and remove or demote the old one. This does not migrate installed software, however, which is one of the main reasons to migrate the installation to new hardware. Another trick is to use the "Disaster Recovery of Active Directory on Dissimilar Hardware" trick described in Microsoft KnowledgeBase article 263532.

---

One of the things SYSPREP does is change the SID, or security identifier, of the computer. The SID is an internal serial number generated by Windows 2000/2003 when it is first installed, and uniquely identifies that particular installation of Windows. Thus, since it's used to distinguish copies of Windows on a network (among other things), it is a bad idea to have more than one machine with the same SID unless you have a very specific reason for doing so—for instance, if you have software that relies on the SID for security.

SYSPREP removes the SID and configures Windows so that when it is next booted it regenerates the SID from scratch. SYSPREP can also force Windows to redetect an entirely new hardware configuration (except for maybe the mass-storage controller—needed to boot the system), which is what makes it important for administrators trying to migrate Windows.

SYSPREP 1.1 for Windows 2000 is available as a download at [www.microsoft.com/windows2000/downloads/tools/sysprep/default.asp](http://www.microsoft.com/windows2000/downloads/tools/sysprep/default.asp). For Windows 2003, SYSPREP 2.0 is included on the Windows 2003 installation CD-ROM. It is stored in the DEPLOY.CAB archive, found in the \SUPPORT\TOOLS directory.

---

**NOTE** SYSPREP does not change access controls on Registry keys. If you try to view keys with accounts that were modified during SYSPREP, you may get an “Account unknown” error. If this happens, you may wind up breaking a lot of things unexpectedly, since many programs will fail if they are denied rights to certain Registry keys. The same applies to other objects with Registry referents such as printers and shares.

---

Even if the two machines are superficially identical, there are almost always enough differences between them that rebuilding the hardware tree is more or less mandatory when migrating to new hardware. For instance, if you are moving from a non-ACPI-compliant computer to one that is ACPI-compliant, the device tree has to be completely reconstructed. Non-ACPI machines don’t enumerate devices the same way ACPI machines do. This re-enumeration is called a *mini-setup*, since it is essentially a stripped-down version of the setup process.

---

**NOTE** Make sure absolutely nothing else is running before activating SYSPREP. This includes programs that are normally “idle” in the system tray. To be on the safe side, deactivate automatic startup for any programs that don’t need it and reboot before imaging.

---

Here is a quick breakdown of the command-line options used with SYSPREP.

- **-pnp** Used to force the redetection of hardware. Because this requires drivers being present, you’ll need to have the CD-ROM handy on the target system, or modify the config files to point to a network share.
- **-reboot** Automatically reboot after you’re done. This is a good way to save time, but omitting it allows you the freedom to shut down the PC manually before migration.
- **-nosidgen** Don’t generate a SID. If you have software preloaded that depends on the SID for security, or you’re having trouble with the cloning process, you may want to enable this.
- **-quiet** No confirmation dialogs. Another speed option.
- **-factory** (only in SYSPREP 2.0) Specifying the **-factory** switch will cause the system to reboot in a network-enabled state, adding customer data and new drivers specified in the answer file `Winbom.ini`. After the changes are made, SYSPREP is run again with the **-reseal** option. These two command-line options are normally only used for people working with mass-imaged machines rather than a single machine being moved, but they can be useful for other manually-added changes.
- **-activated** (only in SYSPREP 2.0) This preserves a successful activation of the Windows installation.

---

**NOTE** You *cannot* use the `-activated` switch to activate a Windows 2003 installation and then move it to another machine. Windows 2003 *must* be re-activated on the target machine when it is moved. Also, you can only use SYSPREP three times on any given installation with the `-activated` switch. Finally, you can only store a prepped image of Windows 2003 for 30 days before the activation clock expires. These limitations make SYSPREP useless for pre-activating an installation. If you want to do that, you're better off obtaining a volume-licensed version of Windows 2003.

---

There are many more SYSPREP options available beyond the command line. For instance, if you are restoring the image on a system that has no local copy of the Windows 2000 drivers and want to point to a network share where drivers are located, you need to configure this manually. The administrator will need to create a SYSPREP.INF file—a plain text file with options in it—and place it in the directory with the SYSPREP executable before you run it. When you unpack SYSPREP, there is a sample SYSPREP file, named `BothSysprep.ini`, which you can customize as needed. Listed next are many of the common options (and the sections they are found in) that you may need to customize in order to use SYSPREP in a migration.

---

**NOTE** If you don't see any of these options in the file, you can simply add them manually using Notepad, one to a line.

---

### [Unattended]

- **InstallFilePath** Lets you specify a local drive or a network share where the Windows 2000 install files can be found.
- **OemPnPDriversPath** Lets you specify a local drive or a network share where you have your OEM Plug-and-Play drivers.

---

**NOTE** As I hinted here, these two options are important if you're cloning out systems that need to detect new hardware, and you don't have local copies of the OS. If you're connecting to a network share that needs credentials, there's a way to specify them automatically in the following file.

---

- **OemSkipEula** Set this to "Yes" to skip the license agreement screen. Most administrators will want to do this.
- **ExtendOemPartition** Set this to 1 and it automatically extends the system partition to the size of the disk during reboot.

### [GUIUnattended]

- **OEMSkipWelcome** Set to 1 to skip the welcome screen.
- **OEMSkipRegional** Set to 1 to skip the regional options screen, such as which language locale to use.

## [Identification]

- **DomainAdmin** Set this to the domain\username of an account with permission to add a computer account to a domain, such as household\w2kadmin. Use this only if you're reconnecting the machine to a domain.
- **DomainAdminPassword** The password for the preceding account.
- **JoinDomain** The domain to join (if any).

## [ProductKey]

- **ProductKey** This lets you specify the Windows product key, to avoid having to retype this information on reboot, in the format **ProductKey = "12345-ABCDE-12345-ABCDE-12345"** This will allow Product Activation to be performed automatically, provided the machine in question has network connectivity.

## [SysprepMassStorage]

The SysprepMassStorage area allows you to identify mass storage device drivers that will be set up on the destination computer automatically. This is a convenient way to deposit mass-storage device drivers that will not be found on the source system. The syntax, however, is a little tricky, and setting up the entries for this section requires a little legwork.

## What You'll Need

- The device's .INF file, usually packaged with the driver
- A text editor, like Notepad, to make the appropriate changes to SYSPREP.INF

Here's how to add entries to SysprepMassStorage:

1. Find the hardware ID of the device in question from the .INF (*not* .INI!) file for the device driver. The hardware ID usually looks like this:

```
PCI\VEN_1022&DEV_7007
```

The corresponding line in the .INF file will look like this:

```
%PCI\VEN_1022&DEV_7007.DeviceDesc%=AMDXP_Install,PCI\  
VEN_1022&DEV_7007
```

2. Copy the hardware ID and insert it into SYSPREP.INF with the following syntax:

```
<hardware ID> = "<path to driver inf>","<disk directory>","<disk  
description>","<disk tag>"
```

The <path to driver inf> is the full path and filename to the .INF file. This can be a subdirectory of the SYSPREP folder you've unpacked on that system.

The <disk directory> item is the name of the directory on the floppy disk provided by the third party that contains the copy of the mass-storage driver. This is important, since you may be prompted for a floppy-disk copy of the driver during setup. The <disk description> section is the description of the floppy disk as described in the TXTSETUP.OEM file provided by the third party, and <disk tag> is the disk tag for the floppy, again described in the TXTSETUP.OEM file.

A fully filled-in mass-storage reference would look something like this:

```
PCI\VEN_1077&DEV_1080 = "C:\Sysprep\qlogic\qlogic.inf",  
"\nt", "Qlogic Software Disk", "\qlogic"
```

3. Save the SYSPREP.INF file and make sure the appropriate drivers are available on the system itself. In Step 2, I noted that the drivers could be made available in a subsidiary of the SYSPREP folder, which is probably the easiest way to do it.

The \$OEM\$ directory can contain a file named cmdlines.txt, which allows you to specify additional commands to run at the conclusion of minisetup. These are all command-line commands, so you can run batch files, install additional applications after the image has been deployed, or whatever you like. You can gain a great deal of flexibility through creative use of \$OEM\$—if you’ve got drivers that need to be deployed on specific systems, for instance.

A full breakdown of the options and commands for SYSPREP is found in the REF.CHM file also included in the DEPLOY.CAB archive.

Finally, for some additional perspective, you may want to take a look at this article, “Using the System Preparation Tool on Dissimilar Computers” (Microsoft KnowledgeBase article 216915).

## 2000/2003 Modifying NTBACKUP Behavior

High

Moderate

Low

An administrator who relies on NTBACKUP for backup functions in Windows will want to know how to modify many of its apparently hard-wired behaviors.

### Overview

NTBACKUP, Windows 2000/2003’s built-in backup program, is widely used by many administrators simply because it’s free, easy to work with, and for the most part gets the job done. That said, it’s also limited in its functionality, although it has some functions which are not directly documented and which can make working with the program a little easier.

## The Party Line

**Company X**

Since NTBACKUP is actually a stripped-down and rebranded version of a third-party product, Arcada/Veritas' Backup Exec, there are a number of undocumented extensions to the program that are not described by Microsoft in their documentation or their KnowledgeBase. This is not likely to change, either.

## The Undocumented Solution

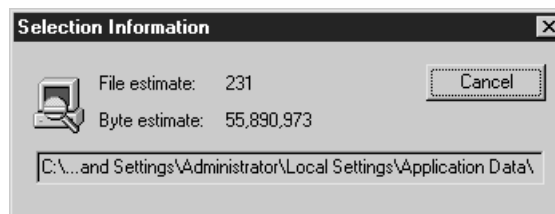
*Many of NTBACKUP's default behaviors can be modified through a series of Registry edits that are not widely circulated.*

### What You'll Need

- A Registry editor
- The NTBACKUP tool, which should have been run at least once to set up its initial options in the Registry

To modify many of NTBACKUP's default behaviors:

1. Open the Registry and navigate to HKEY\_CURRENT\_USER\Software\Microsoft\NTBackup\User Interface. (This affects the current user's settings only; the program cannot be modified on a global basis.)
2. Edit the REG\_SZ value named Estimate Byte Count. Set this to 0 for faster backup starts; this disables NTBACKUP's enumeration of the total byte count for the backup, as shown here:



3. Edit the REG\_SZ value named "Backup files inuse" (note that "inuse" is one word, exactly as printed). Set this to 1 to force NTBACKUP to use shadow

copying to back up files that are flagged as being in use, but are not themselves system files (such as open documents).

4. Edit the REG\_SZ value named Remote Drive Backup. Set this to **1** to allow NTBACKUP to make backups of remote drives—drives exposed through a network share or mapped network path. Normally, this is not allowed.
5. Edit the REG\_SZ value named Backup Catalogs. Set this to **1** to force NTBACKUP to back up all catalog files from your TEMP directory on each backup operation. (The catalog files will still be deleted when the backup operation is closed, but they will be saved to tape first.)
6. Edit the REG\_SZ value named Skip Open Files. NTBACKUP attempts to open any non-system file for 30 seconds if it's being held open by another process. Change this value to **1** to force NTBACKUP to skip non-system files that are being held open.

---

**NOTE** System files are, by default, copied using the shadow copy function, whenever a System State backup is being made.

---

7. Navigate to HKEY\_CURRENT\_USER\Software\Microsoft\NTBackup\Hardware.
8. Add or edit the REG\_SZ value Drive Settling Time (that's "settling", not "setting") as a type REG\_SZ. The default value is 60 (seconds). Try setting it to 120 if the program times out waiting on your tape drives.

---

**NOTE** Windows 2003 uses a different tape format for backup than Windows 2000 or Windows XP Professional. The Windows Server 2003 edition of NTBACKUP can allocate tape block sizes up to 64KB. NTBackup in Windows 2000 and Windows XP can only allocate block sizes of up to 32KB for tape. If Windows 2000 or Windows XP Professional try to read a tape with 64KB block sizes, they will report an error. There is no known way to force Windows 2003 to use 32KB block sizes on tape, but Microsoft has documented the problem in KnowledgeBase Article 821588 and should have a fix shortly.

---

## 2000/2003 Backing Up and Restoring the Remote Storage Database

High

Moderate

Low

The Remote Storage Service database contains information about remotely stored data. If you are setting up an entirely new Windows 2000 installation and you want remotely stored data to be available on the new system, you must restore the Remote Storage Service database on the new machine.

---

**NOTE** Migrating or cloning a system will bring the database over automatically, so you don't need to do this on a machine that's been migrated or cloned.

---

## Overview

The Remote Storage database is one of the more esoteric components of Windows and yet it isn't discussed very widely. All metadata about data that has migrated into Remote Storage is kept here, but it is not generally accessible to the end user or administrator. This is apparently by design, since tampering with the Remote Storage database could make all remotely stored data unavailable.

### The Party Line

**Company X**

Normally, if you make a System State backup or some other full-system image, the Remote Storage database is preserved. However, Microsoft doesn't describe how to back up the Remote Storage database independent of everything else.

### *The Undocumented Solution*

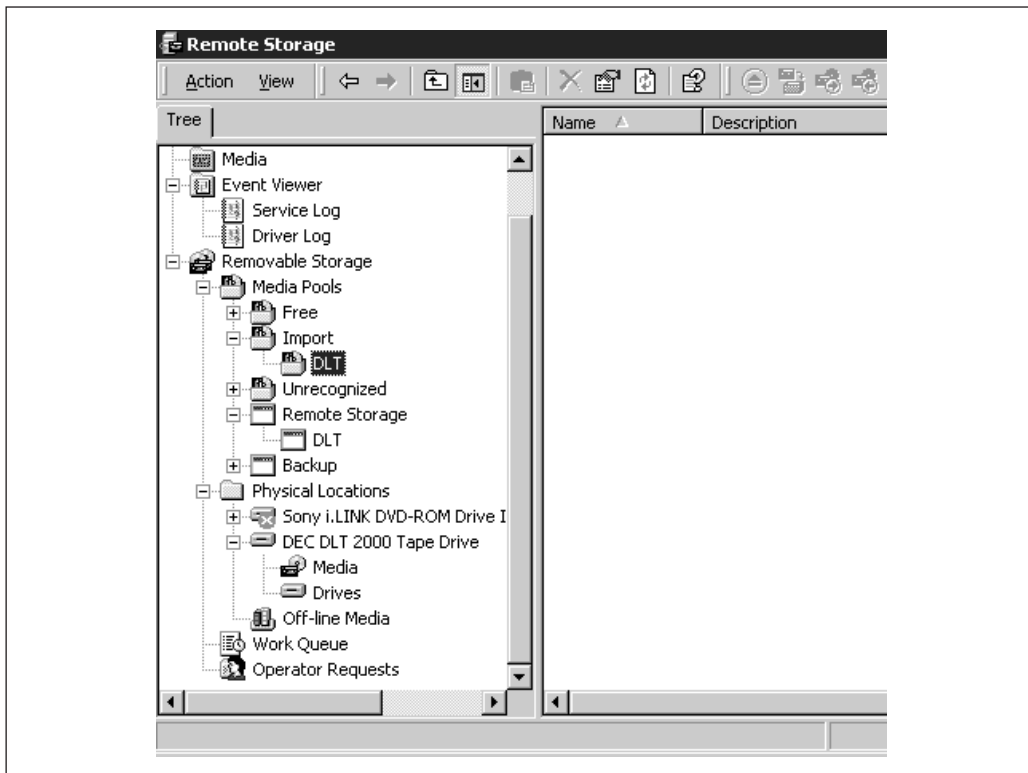
*As it turns out, the Remote Storage database can be manually restored, although it requires some work and isn't a simple one- or two-step process. Plan for some downtime when doing this, if you haven't done so already.*

## What You'll Need

- The Remote Storage Service, which should already be installed and running
- A tape drive or some other RSS-supported media
- A copy of the most recent backup media used for a Remote Storage action

To restore a copy of the Remote Storage database:

1. Right-click My Computer, select Manage, and open the Removable Storage snap-in. Under Media Pools, look in the Import Pool, which should be empty. If it isn't, don't panic; it simply means that there is a catalog there that does not reflect what you are going to restore. See Figure 6-2 for an example of where to look for the Import Pool.



**Figure 6-2.** The Import Pool in the Media Catalog, which here shows the presence of a DLT folder (which is empty)

2. Insert the most recent tape (or other media) used for remote storage. If the backup is on more than one piece of media (in other words, it spans two or more tapes or discs), catalog the media by moving them temporarily into the NTBackup media pool and checking the dates.
3. Move the media into the NTBackup media pool (usually named "Backup"). If there is no such pool, you can create one automatically by simply running NTBACKUP.
4. Launch NTBACKUP and catalog the media to find the last copy of the RSS database, which is stored in the `%systemroot%\System32\RemoteStorage` folder. Make sure you are getting the most up-to-date copies. This is critical; if you work from a less-than-recent piece of media, you'll have an incomplete database and you won't be able to get to everything in Remote Storage.
5. Select the most recent folders labeled NTMSData and RemoteStorage.

6. In the Restore Files To: box, select a new location and point to the drive that contains the *%systemroot%* folder.
7. Select Start Restore | Advanced, and then choose Restore Removable Storage Database. Click OK to go through each prompt.
8. Once the restore operation is finished, reboot.
9. Look in the Removable Storage Manager after rebooting and make sure all the databases have been restored. All the earlier media pools should exist, with all of their attendant media inside.
10. Check the Services snap-in to see that Remote Storage Engine, Remote Storage File, and Remote Storage Media are all stopped.
11. Look in the *%systemroot%\system32\RemoteStorage\engdb* folder (make sure you have Show Hidden Files/Folders and Show System Files turned on in Explorer, or you won't see anything). If there is anything in there, move it to another, temporary folder.
12. From the command line, type **RSTORE %systemroot%\system32\Remote Storage\engdb.bak**. This runs the RSTORE tool, which comes with the Remote Storage service to repair the Remote Storage database.
13. Restart the Remote Storage Engine, Remote Storage File, and Remote Storage Media services. Look in Remote Storage to make sure all the managed volumes listed there show up correctly. Then, test things out by restoring a few migrated files.

2000/2003

## Backing Up and Restoring IIS Installations

High

Moderate

Low

Internet Information Server's internal configuration can be backed up and restored locally, but it can also be backed up offline.

### Overview

When setting up Internet Information Server (IIS), an administrator will usually take great pains to tweak IIS so it runs just the way it's needed. This is true not only if there are a great many sites and virtual directories that need to be set up by hand, but also if IIS needs to be modified under the hood to run a certain way. If the IIS installation is lost and needs to be reconfigured from scratch, having a backup copy of the whole thing comes in handy.

## The Party Line

**Company X**

Microsoft has thoughtfully built into IIS a tool for backing up the current IIS configuration. The entire IIS configuration, including the Metabase (the Registry-like repository for data used by IIS), can be backed up and restored in this fashion. What's more, multiple backups can be made, so that an administrator can experiment with different configurations easily. What Microsoft didn't do, however, is provide the user with a direct way to back up that information *offline*.

### *The Undocumented Solution*

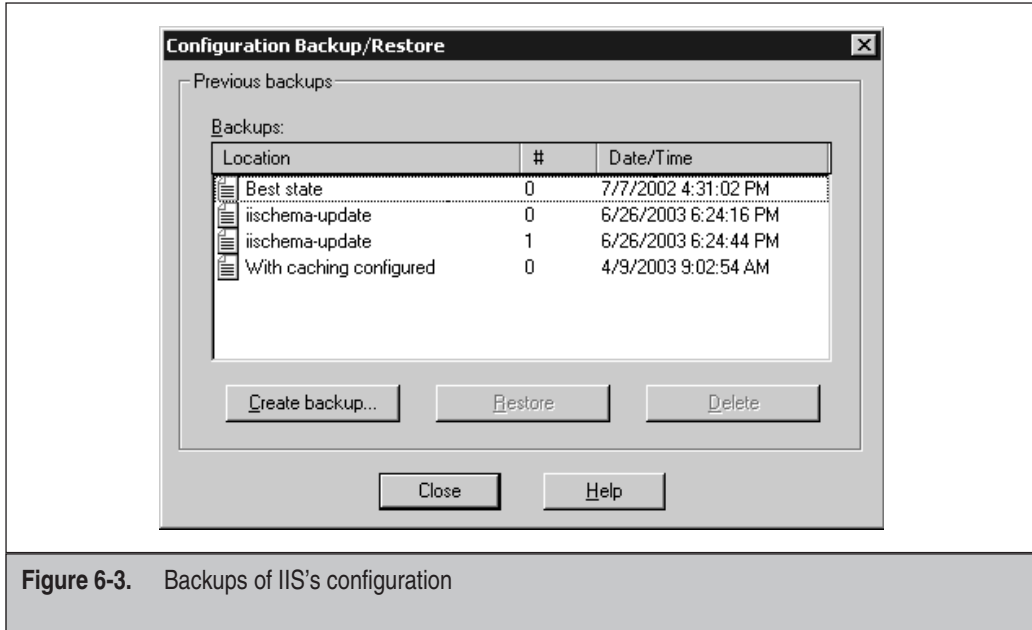
*Happily, saving IIS backup information offline isn't difficult. The data in the Metabase is saved to a file that can either be copied out by hand or copied using a backup utility of your choice.*

## What You'll Need

- The Internet Service Manager
- A safe place to back up the IIS directory data

To save the IIS backup information:

1. Back up the data directories for IIS themselves. This can be done in any manner you choose, and you usually don't have to take the site offline to do this, unless the contents of one of the directories in your web site are modified by the site's users. The reason for this is that it hardly helps to have a copy of the IIS site configuration information without also having a copy of the sites themselves, and the standard IIS config backup process doesn't back up site data.
2. Launch the Internet Service Manager.
3. Right-click the computer in question in the left-hand pane and select Backup/Restore Configuration to produce the image shown in Figure 6-3.
4. Choose a descriptive name for the backup set. If you are performing a series of progressive changes on the site to see which work the best, make a small note



**Figure 6-3.** Backups of IIS's configuration

here about what changes have been made, for instance. You don't need to specify the time and date since those are backed up automatically. Click OK.

**NOTE** With IIS6, you can encrypt the contents of the backup by checking the box marked Encrypt Backup Using Password and then typing a password.

5. Shut down IIS. (This step is optional.)
6. Look in the `%systemroot%\system32\inetsrv\MetaBack` directory for a file with the name you chose and the extension `.MD0`. Copy that file and save it along with the backup of your site. In Windows 2003, there will be two files, one with the extension `.MD0` and another with the extension `.SC0`; copy them both.

**NOTE** These Metabase backups will only work on the same installation of Windows. They cannot be moved to another installation.

## 2003 Recovering the ASR Floppy from an ASR Backup Set

High

Moderate

Low

In Windows 2003 and Windows XP, the Automated System Recovery process creates a floppy disk that holds important system information, including Plug-and-Play device enumeration that may be needed to access the data in the accompanying backup setup.

### Overview

When an administrator runs NTBACKUP and creates an ASR (Automated System Recovery) backup set, the floppy disk that gets produced along with it is often the weakest link, so to speak. The floppy can be easily damaged, erased, or lost, and without it the ASR process cannot continue.

### The Party Line

**Company X**

Microsoft's standard dictate about the ASR floppy is that it should be guarded carefully, but one of the things they don't mention is that the contents of the floppy can in fact be regenerated from the ASR backup set without a great deal of work.

### *The Undocumented Solution*

*If you lose the ASR floppy, but still have the ASR backup set, you can mount the backup set on another computer and re-create the ASR disk without too much difficulty.*

### What You'll Need

- A newly formatted, blank floppy
- The ASR backup set
- The NTBACKUP utility

The steps to recover the floppy disk from an ASR backup set are as follows:

1. Start the NTBACKUP utility by typing **NTBACKUP** in the Run dialog from the Start button.

2. Insert your ASR backup media.
3. Select the Restore and Manage Media tab in NTBACKUP.
4. Select the media that contains your ASR backup from the media tree and expand it.

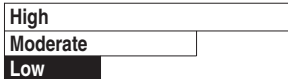
---

**NOTE** If the media isn't present in the tree—in other words, if the media was backed up on a different system and this system's Media Manager does not have it—you will need to mount the media manually.

---

5. Open the *second instance* of the drive letter that contains the system files, and navigate down to the `%systemroot%\Repair` folder.
6. Select the files ASR.SIF and ASRPNP.SIF.
7. Set the Restore Files to: option to Single Folder and the Alternate Location option to the A: drive.
8. Click Start Restore. The ASR files should be copied out.

## 2003 Increasing GPO Logon Performance



One common complaint about Windows 2000 is that it can take a long time to start up or log in, especially on a domain that has Group Policies. Windows 2003 and XP Professional doesn't have this slowness, and a big part of the reason for that is the way the OSs behave by default when handling policies.

### Overview

Windows 2000 uses *synchronous* policy behavior at logon, meaning that each step of the policy is applied one at a time, with the server waiting for separate confirmation about each step.

Windows XP Professional, on the other hand, uses *asynchronous* policy behavior at logon. All steps of the policy are run at the same time, and the server doesn't hang around waiting for individual confirmation for each. This logs the user in much faster.

The downside of this behavior is that events are not processed in the order you might expect them to be, such as folder redirection and software installation. Folder redirection, for instance, might be critical to a program that runs later in the logon. What's more, a user may have to restart or log on up to *three* times to effect changes that require synchronous policies.

## The Party Line

**Company X**

Microsoft has several suggestions for reducing the time it takes to process GPOs. One is to combine as many GPOs as possible, or to filter their application by user group. Another, which is documented but little-discussed, is to make Windows 2000 behave the same way as Windows XP Professional when it comes to processing group policies: asynchronously.

### *The Undocumented Solution*

*The trick to changing Windows 2000's logon behavior is easy enough: asynchronous (and synchronous) behavior is controlled through a policy itself. However, there are side effects. If your workstations require logon event processing to take place in a certain order, you will not want to do this. The same goes for any servers, of course, that are affected by this policy.*

*If, however, the order of logon events is not critical (for instance, if you don't do much drive mapping, or if you use UNC names for remote drives rather than rely on drive mappings), you ought to try this, since you will get a significant improvement in logon time and startup time for Windows 2000 without any real tradeoffs.*

### What You'll Need

- The Windows 2000 server where the policies are managed
- The Active Directory Management Console (which is included by default)

Here are the steps to follow to change to asynchronous GPO behavior for Windows 2000:

1. Open the management console for Active Directory Users and Computers.
2. Right-click your domain, and then click Properties.
3. Under the Group Policy tab, select the GPO you want to edit and then select Configure.

4. Expand the tree to Computer Configuration | Administrative Templates | System | Group Policy.
5. In the Policy pane, double-click Apply Group Policy For Computers Asynchronously During Startup. Select Enabled.
6. Click Apply, and then click OK.
7. Double-click Apply Group Policy For Computers Asynchronously During Logon, and click Enabled.
8. Click Apply, and then click OK.

2000/2003 **Troubleshooting Global Policy Object Behavior Using Logging and Tools**

High	<input type="checkbox"/>
Moderate	<input type="checkbox"/>
Low	<input checked="" type="checkbox"/>

---

**NOTE** Thanks to Darren Mar-Elia for the information in this section.

---

Global Policy Objects, or GPOs, are one way for administrators to constrain user and system behavior. Debugging and modifying them can be more complicated than it might initially appear.

### Overview

Microsoft provides a few tools for evaluating policies. The Resulting Set of Policy (RSoP) or GPO Results tool in Windows 2000, Windows XP Professional, and Windows Server 2003 is a good way to judge what effects a policy will have.

RSoP uses WMI to report what policy settings would be applied to a given workstation or user. If there are problems when an application of policy takes place, they're logged either to the Application Event Log on the target client or a log file on the server (in `%systemroot%\debug\usermode\userenv.log`). You can change the verbosity of these logs by editing the Registry key `\HKLM\Software\Microsoft\Windows NT\Diagnostics\RunDiagnosticLoggingGroupPolicy`, a `DWORD`, and setting it to 1 for maximum verbosity.

---

**NOTE** If for some reason you have disabled the WMI service on the target workstation or server (or something else has disabled it or is interfering with it), RSoP will not work for that machine.

---

## The Party Line

**Company X**

However, aside from using RSoP as a way to debug problems, there are some behaviors of GPOs that are not always spelled out by Microsoft, and which may have an impact on how well your system deals with policies.

### *The Undocumented Solution*

*Here are some additional reasons why GPOs may not be processed correctly, and some suggested ways to deal with them.*

*The way GPOs are processed* can be tricky and deceptive. GPOs are processed at boot time and when a user logs on. They are also processed at random intervals within 90-minute spans on member servers and workstations, and every five minutes on domain controllers.

What takes precedence over all of this, however, is whether or not something has *changed*. If a processing cycle listed earlier comes up for a particular GPO, but that GPO has not been changed, then nothing happens. Changes, not time elapsed, are what really trigger the processing of a GPO. You *can* force the processing of an unchanged GPO through an Administrative Template policy, but administrators shouldn't rely on this mechanism, since it also depends on whether or not the Active Directory-based GPO changes as well.

Because of this behavior, one good way to deal with GPOs that seem to be out of sync is to change an insignificant setting and then change it back again, which may force a refresh.

Another advantage to using this method is that the log will indicate if a *slow link* has been detected. Slow network links—dial-ups or even highly congested LANs—can foul up Policy processing, since certain policies are not processed by default if slow links are detected. This can also trip people up, since while the Event Log may report the policy was in fact processed, it doesn't seem to have taken effect.

To get around this, an administrator can edit the default slow-link threshold in the Local Computer Policy snap-in, in Computer Configuration | Administrative Templates | System | Group Policy, shown as Group Policy Slow Link Detection. This setting is calibrated in kilobits per second.

*Problems with DNS* can also cause GPO policy processing to go awry. GPO processing requires the SRV records used by LDAP (Active Directory is an implementation of LDAP, remember?). Try stopping and restarting the Netlogon service on your domain

controllers to determine if SRV registration is taking place. If it still isn't working, something may be wrong with DNS.

## 2000 Upgrading Windows 2000 Group Policies for Windows XP Professional Clients

High

Moderate

Low

An out-of-the-box installation of Windows 2000 Server needs to be modified to use Windows XP Group Policies, which are not available in Windows 2000 by default.

### Overview

With Windows XP Professional starting to replace earlier versions of Windows in the workplace, many administrators have found that Windows XP Professional has a host of policies which don't exist in Windows 2000 Server and can't be administered.

### The Party Line

**Company X**

Microsoft is aware of this, and in fact has discussed the problem (and a possible solution) in KnowledgeBase article 307900. The trick is to use the Windows XP policy settings to upgrade the policies on the Windows 2000 server (described next).

### *The Undocumented Solution*

*The exact process is simple enough, and is reproduced next, with some additional things an administrator needs to be aware of that Microsoft doesn't cover in their article.*

### What You'll Need

- A Windows XP Professional machine that has been joined to the Windows 2000 Server domain you are upgrading
- The domain administrator's logon information

Here's the process to upgrade the policy objects:

1. Log on to the Windows XP Professional workstation using the domain administrator's credentials. This particular (and previously undocumented) step is important, because it allows the XP user to traverse directories on the 2000 server.
2. From the Start | Run dialog, type **mmc** to open the Microsoft Management Console (MMC).
3. From the File menu in MMC, select Add/Remove Snap-In and add the stand-alone Group Policy Object, as shown in Figure 6-4.
4. When you are prompted to select a Group Policy Object, the local machine will initially be selected as the target object, as shown in Figure 6-5.
5. Click Browse and navigate to the server whose GPOs you want to upgrade.
6. Click Close and then OK to commit the changes.
7. Use a Windows XP Professional system with the domain administrator logon to manipulate the policy changes, since Windows 2000 will not be able to display the changed GPO objects. Windows 2003, on the other hand, is able to do so natively and doesn't need to be tweaked in this fashion.

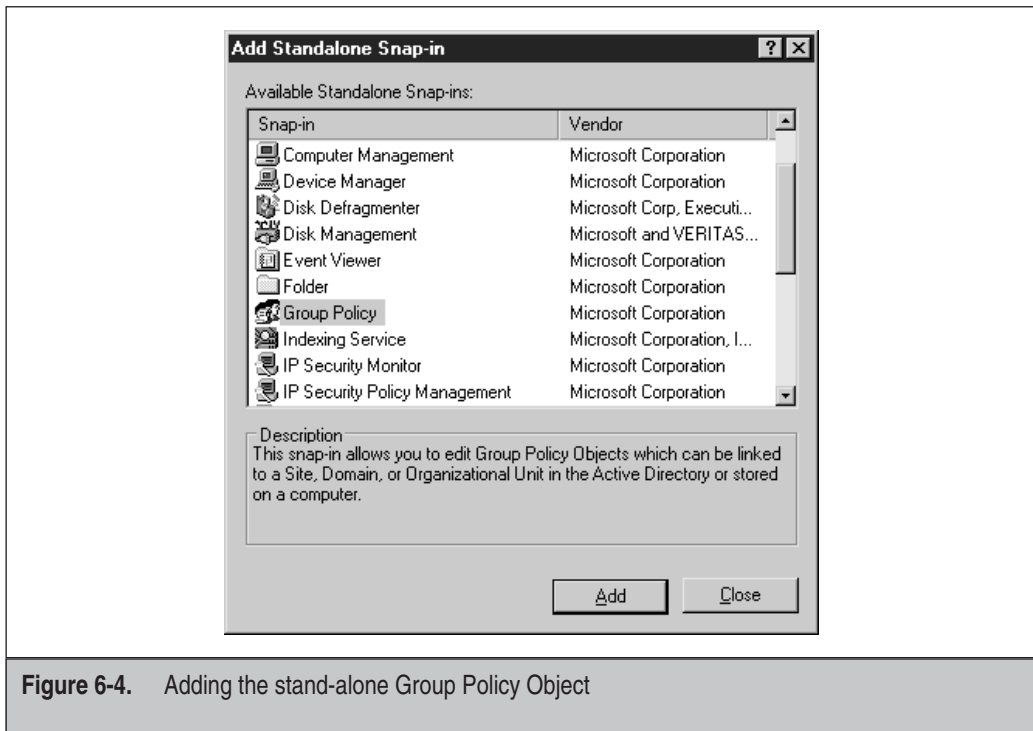
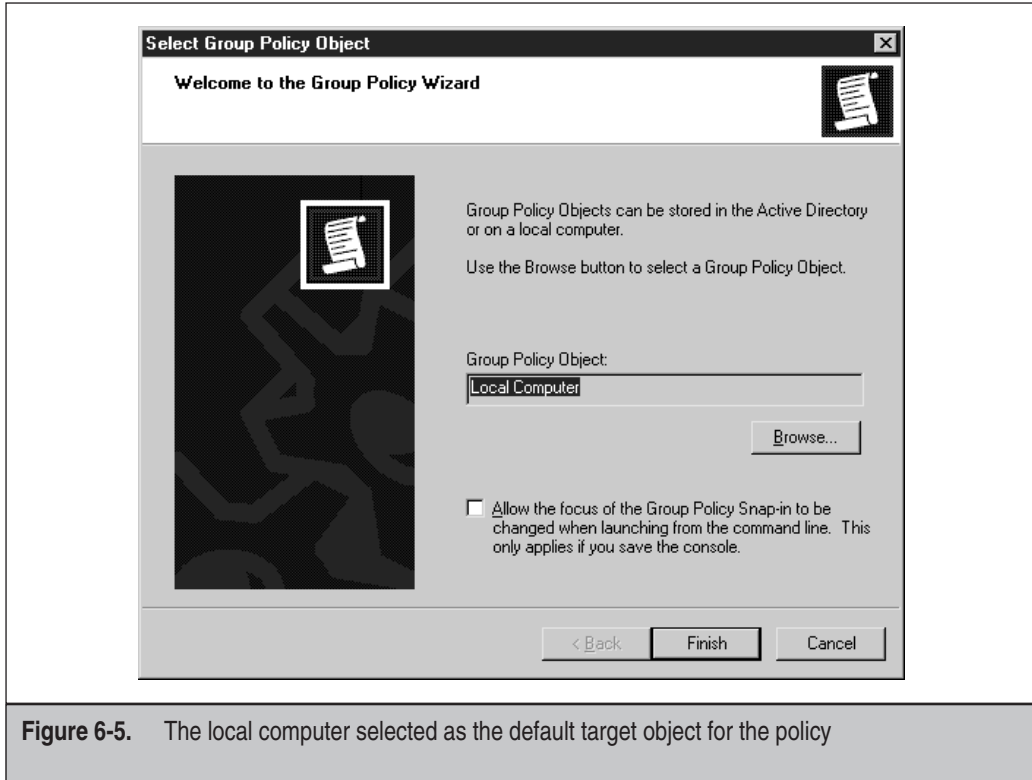


Figure 6-4. Adding the stand-alone Group Policy Object



**Figure 6-5.** The local computer selected as the default target object for the policy

## 2000/2003 Repairing a Missing Default Domain Controller Policy on a Windows 2000 Server

High

Moderate

Low

If a domain controller delivers errors whenever an administrator tries to edit or configure the domain policy, there is a good chance the domain policy has been destroyed, possibly by mistake.

### Overview

Missing policies can create a whole slew of bizarre behaviors. To find out if the default domain controller policy is in fact missing, look in the folder `%systemroot%\SYSVOL\domain\policies` (where `<domaincontroller>` is the network name for your domain controller). Within that folder should be a directory starting with `{31b2` (note the curly

brace as part of the name), which indicates a GUID used to refer to the policy in question. If that folder is missing, then the default domain policy is also missing.

Another possible form of damage is a missing domain controller security policy, which is stored in the same location using a folder that begins with {6AC1. (Again, note the curly brace as part of the name.)

## The Party Line

**Company X**

Microsoft's typical solution for a problem this deep-rooted is to reinstall Windows, or to restore from a working System State backup.

## *The Undocumented Solution*

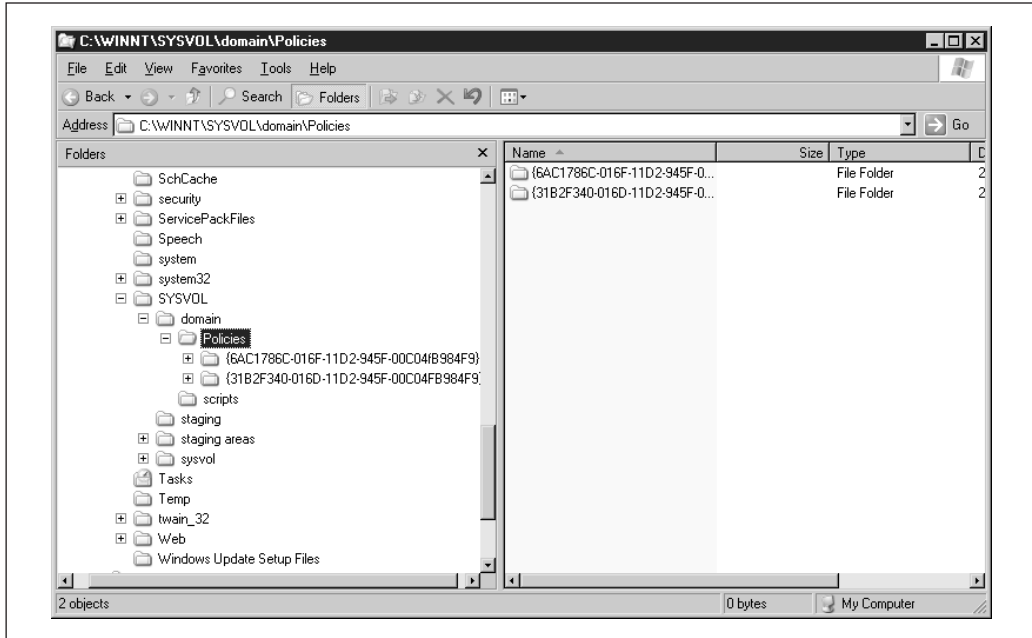
*There is a roundabout way to reinstall the default domain policy, although it requires the presence of another domain controller from which to borrow the policy settings.*

## What You'll Need

- Another Windows Server that can be promoted to the status of a domain controller, or...
- Another existing stand-alone Windows domain controller

To rebuild the domain policies:

1. Obtain access to or set up another Windows Server in the network.
2. If you haven't already, run DCPRMO on that computer to promote it to the status of a domain controller. For the best results, make it a stand-alone domain.
3. Once the new domain controller is up and running, go to the %systemroot%\SYSVOL\domain\policies directory on *that* machine, and look for the directory that begins with the GUID {31b2. (If you are repairing the domain controller security policy, look for {6AC1.)) You can see an example of this in Figure 6-6.
4. Make a copy of that directory and keep it somewhere safe.
5. Demote the domain controller you just created.



**Figure 6-6.** The Policies directory with copies of the default domain and domain security policies

6. Copy the {31b2 (or {6AC1) directory into the Policies directory for your existing domain controller—whichever GUID matches the Object ID of the policy.
7. Reboot the domain controller.

**NOTE** While this will provide you with a newly minted domain policy, a great many of the key policies in it will not be there and will not be correct. Take the time to walk through the default policy and set things up as they should be.

## 2000/2003 Performing Scripted Administrative Tasks on GPOs

High

Moderate

Low

Group policies can be arcane and abstruse. Thus, sometimes the best way to explore them is outside the context of the Group Policy Management Console.

### Overview

The Microsoft Management Console application tends to be a one-size-fits-all approach to things, whether for Group Policies or just about anything else. It's designed mostly for top-down viewing, not allowing for advanced filtering and searching. For this reason it can be hard to analyze multiple group policies. There is also a great deal that

the console doesn't do, or doesn't support directly—or maybe there are specific tasks you want to automate rather than do manually.

## The Party Line

**Company X**

Believe it or not, Microsoft has a solution for all of this, albeit an enormously underreported one. After you install the Group Policy Management Console, a whole slew of administrative scripts are installed in the %programfiles%\gpmc\scripts directory (where %programfiles% is the Program Files directory for your system).

## The Undocumented Solution

*There are 32 sample scripts in the \scripts directory, which cover a broad variety of tasks: backing up an individual GPO, backing up the GPO in a domain, creating a copy of a GPO, creating a new GPO, creating a policy environment using an XML file, creating a GPO file that represents a policy environment, listing GPOs orphaned in SYSVOL, and many more. A full breakdown of the script samples can be found in the MSDN library, at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gpmc/gpmc/group\\_policy\\_management\\_console\\_scripting\\_samples.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gpmc/gpmc/group_policy_management_console_scripting_samples.asp).*

2000/2003

## Cleaning Up Temporary Files in User Accounts

High

Moderate

Low

On both workstations and servers, the TEMP directories for user accounts and the Windows installation can become cluttered with files that can cause program installations to fail, or create other bizarre behaviors.

### Overview

Windows maintains several folders for temporary files. One is a system-level folder, located in %systemroot%\TEMP. The other is in each user's Documents and Settings

folder, in the path \Documents and Settings\<>user>\Local Settings\Temp. Local Settings is a hidden folder, which makes this TEMP directory harder to find than normal.

Many different programs use the TEMP directories as dumping grounds for all sorts of digital trash. Installer applications usually unpack compressed files into these directories, for instance, and one of the common reasons an application install can fail is if files from another, totally unrelated program have left similarly named temp files there. The installer may balk at overwriting, and may instead fail, or even copy out the wrong information. For this reason, the TEMP directories need to be kept clear.

There's also the simple fact that, over time, this sort of accumulation becomes burdensome. While repairing a friend's computer, I found *over two gigabytes* of files in that user's TEMP folder. Deleting that mess cleared up almost all of the bizarre behaviors her machine had been exhibiting.

## The Party Line

**Company X**

About the only acknowledgement Microsoft makes regarding the TEMP directory problem is through the use of one of their tools—the Disk Cleanup tool, which purges temporary files from many folders, but doesn't do the most consistent job of cleaning out the TEMP directory. The best way to do it, it seems, is by hand.

## *The Undocumented Solution*

*Many of the files in a given user's TEMP directory will be locked for exclusive access when that user is logged on. To get around this, use another account—one whose sole purpose is to purge other accounts.*

## What You'll Need

Administrative access on the computer in question

Here's the process for purging user's TEMP directories:

1. Create a new user account, preferably with a name and password that cannot be easily guessed, and give this account administrative privileges. I'll refer to this account as the "purge" account, henceforth.

2. Log off all other users and log on as the “purge” user.
3. Implement the following batch file command for each user whose directories you want to purge:  
**rd "<drive>:\Documents and Settings\<user>\Local Settings\TEMP" /S /Q  
md "<drive>:\Documents and Settings\<user>\Local Settings\TEMP"**  
For <drive>, substitute the drive letter where Documents and Settings is located; for <user> substitute the username. (You can look in the Documents and Settings folder to determine the exact name syntax.) Repeat this command as many times as needed in the batch file for each user.
4. You can now do one of two things. If you are inclined to do the purging manually, add this batch file into the “purge” user’s Startup folder. If you wish, you can append a LOGOFF command to the file, so that the “purge” user is automatically logged back off when the command has finished running. This way, you can simply log in as the “purge” user periodically when you want to perform maintenance.

If you would rather perform the cleanups automatically, create a Scheduled Task for that batch file and run it in the context of the “purge” user account. Any logged-in user who has those files open will simply have them skipped over at the time of the purge. For that reason, you may want to schedule such cleanups to take place more than once a day.

## 2003 Reinstalling TCP/IP in Windows 2003

High

Moderate

Low

Because of changes to the way TCP/IP is handled in Windows 2003, it cannot be uninstalled and reinstalled in the conventional manner.

### Overview

Windows NT 4.0 and Windows 2000 listed TCP/IP as one protocol among many—it could be deinstalled and reinstalled like any other network component. In Windows 2003, however, that all changed: a curious administrator will find that the Uninstall button for TCP/IP in the Network Connection Properties window is dimmed and cannot be clicked. A surprising number of administrators attempt to deal with bizarre network problems by simply deinstalling and reinstalling all network components, without realizing that that doesn’t always fix everything either for reasons described further in this section.

## The Party Line

**Company X**

Microsoft rewrote the way TCP/IP works in Windows 2003 to be a core system component. Part of this was apparently for the sake of speed, since more network components are now handled through kernel-level drivers, but also to reflect a change in the philosophy behind the use of TCP/IP: it's not just a network component but *the* network component. If TCP/IP malfunctions in Windows 2003, an administrator may attempt to reinstall TCP/IP, only to find he can't.

### *The Undocumented Solution*

*The answer, as it turns out, is to use the NETSH tool to reconfigure the network stack. NETSH deletes and rewrites all IP-related Registry entries and refreshes the network stack as if it had been newly installed. (The affected keys, if you're curious, are HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters and HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DHCP\Parameters.) Simply deinstalling network components does not always reset this information.*

To rebuild the network stack, issue the command,

```
netsh int ip reset <logfile>
```

where <logfile> is the path to a text file that will contain the results of the operation. The changes that take place will depend largely on what changes, if any, have been made to the TCP/IP stack. The machine will need to be rebooted after this change, however.

This technique also works for Windows 2000, and is in fact preferred to deinstalling and reinstalling TCP/IP "by hand."

---

**NOTE:** If you've applied any of the tweaks or optimizations listed in this chapter, running this command will undo them and they will need to be recreated from scratch.

---